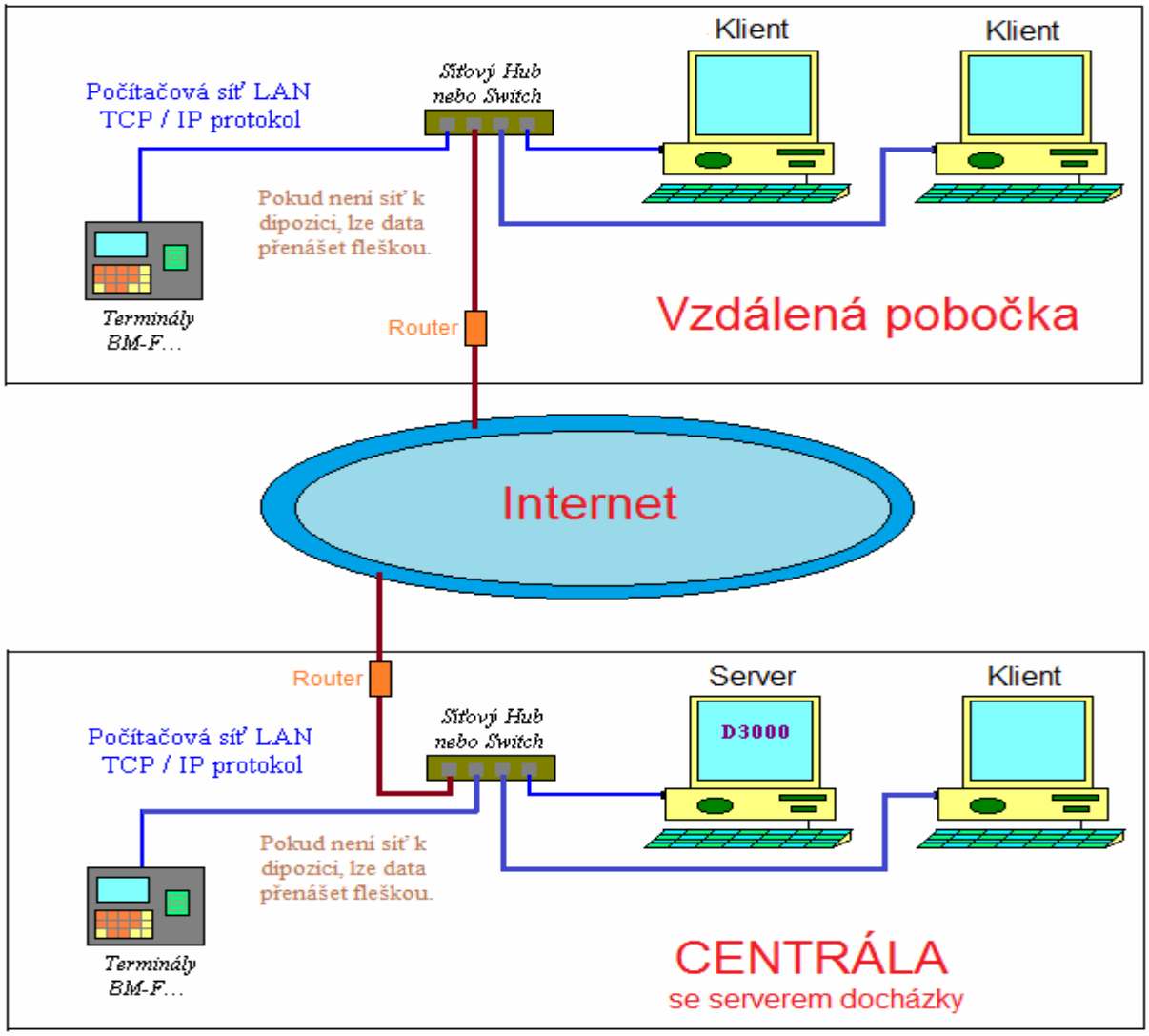
Docházka 3000 – propojení terminálů mezi pobočkami a centrálou

Tato příručka popisuje 5 možností, jak řešit situaci připojení více terminálů BM-Finger v případě, kdy máte jednu nebo více vzdálených poboček a potřebujete zajistit, aby se data z terminálů na nich umístěných dostala do instalace programu Docházka 3000 na serveru (hlavním PC docházky) v centrále.

Tedy například tato situace:



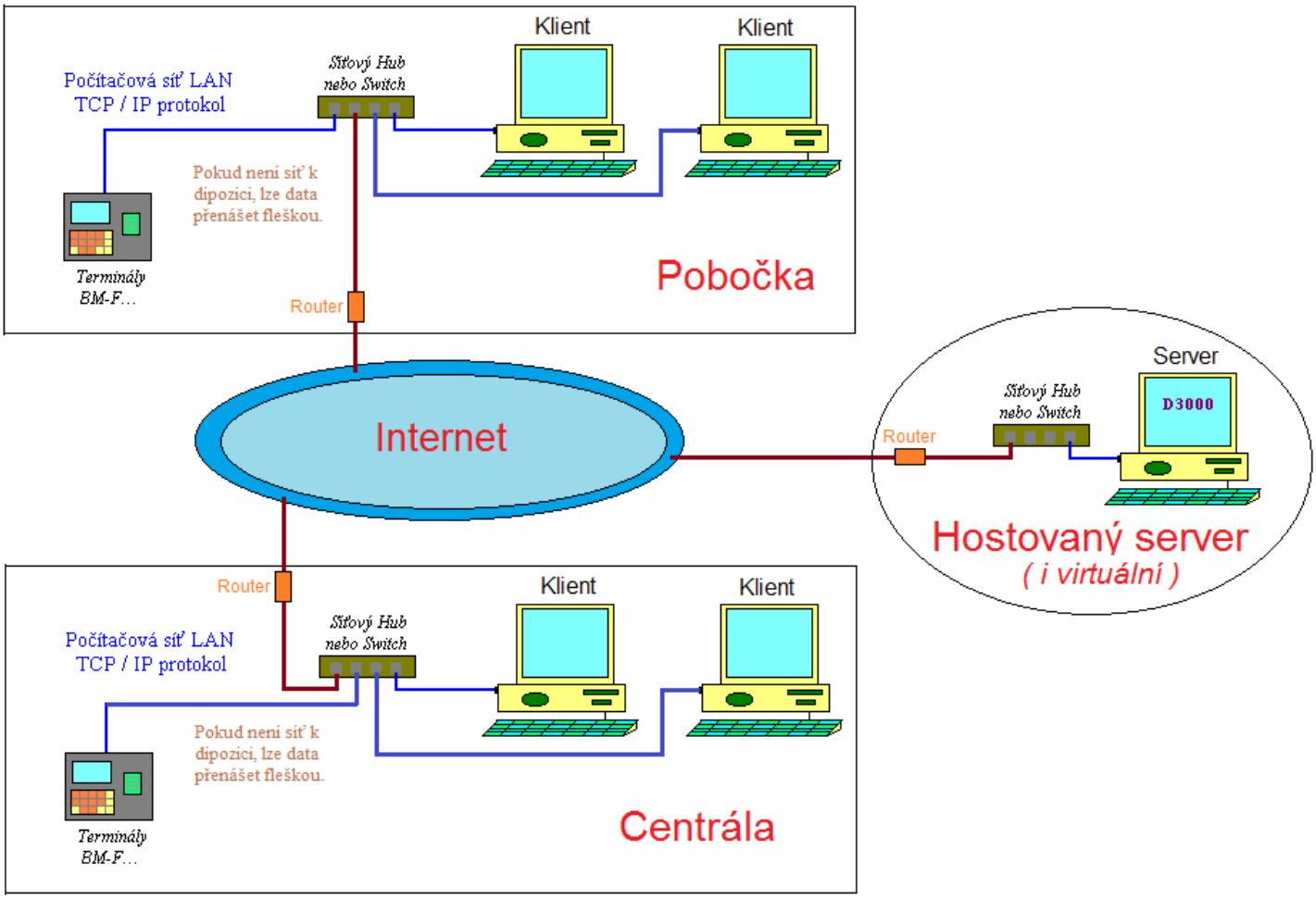
Na výše uvedeném obrázku je příklad, kdy má firma centrálu a vzdálenou pobočku. Na centrále je umístěné hlavní PC docházky na obrázku označené jako **Server.** Tento docházkový server napřímo komunikuje s terminálem umístěným na centrále, ale s druhým terminálem, umístěným na pobočce nemůže komunikovat přímo, jelikož se jedná a jinou fyzickou počítačovou síť.

Tato příručka shrnuje jak lze zajistit, aby i přes toto oddělení sítí dokázal server docházky stahovat data z terminálu na pobočce. A to buď použitím VPN (virtuální privátní sítě) nebo proroutováním portů 4370 a 3001 na TCP i UDP protokolu, tedy takzvaný port-forwarding či port-proxy.

Komunikace klientských PC s docházkou je opět napřímo uvnitř sítě centrály, kde se klienti připojují pomocí lokální sítě centrály přímo k serveru http protokolem (port 80, nebo port 443 u https protokolu). Klienti na vzdálené pobočce opět mohou bez problému s docházkou pracovat ze svých počítačů, pokud se používá VPN, kdy počítače ani nepoznají, že datové spojení prochází přes veřejnou síť – internet.

Uvedené obrázky ukazují situaci s centrálou a jednou pobočkou, princip je ale stejný i když je poboček více.

Popsané metody přenosu dat z terminálu do programu Docházka 3000 pomocí VPN nebo port-forwardingu (port proxy) jsou použitelné i v případě, kdy server docházky není umístěný na centrále ani na pobočce, ale jedná se o Windows Server umístěný u poskytovatele služeb v nějakém datacentru providera. Viz následující obrázek:



A to ať je u providera váš pronajatý Windows server dedikovaný (skutečný HW), nebo pouze virtuální. K serveru se při jeho obecné administraci tedy připojujete vzdáleně např. přes vzdálenou plochu (RDP protokol). Princip přenosu dat docházky je ale stále stejný. Tedy tento vzdálený server musí mít možnost připojit se IP protokolem do terminálů centrály i pobočky a stahovat z nich data. Klienti na centrále i pobočce zase potřebují přes webové prohlížeče (http nebo https protokolem) pracovat s docházkou běžící na vzdáleném serveru. Někdy se toto řešení označuje jako cloudové („*server je v cloudu*“). Důležité stále je, že na serveru běží OS Windows a je v něm nainstalovaný program Docházka 3000. Opět je možné mezi všemi třemi stanovišti zřídit buď šifrované datové spojení a emulovat tak lokální síť pomocí VPN. Nebo alespoň na pobočkách, pokud jejich vstupní routery (přes které jsou připojeny k internetu) mají pevnou veřejnou IP adresu, lze použít proroutování portů 4370 a 3001 na TCP i UDP protokolech pro komunikaci serveru s terminály a v opačném směru pro komunikaci klientských PC s docházkou běžící na serveru pak proroutovat TCP port 80 při používání http protokolu nebo 443 pro https.

Dostupná řešení:

1. řešení - VPN

Tato metoda s použitím VPN je z pohledu nastavení docházky úplně nejjednodušší, protože terminály ani klienti ani server nepotřebují žádnou úpravu konfigurace programu docházky, jelikož se zde vše jeví jako jedna velká lokální síť. Celá síť například používá IP adresy 192.168.x.x nebo 10.x.x.x a o šifrování dat, jejich tunelování internetem se starají routery či VPN servery. Pro docházku a terminály i klienty je toto „skryto“ a pro ně se celá komunikace jeví jako v lokální síti.

Například pokud používáte IP adresy 192.168.1.x (maska /24), tak například terminálům přidělíte adresy 192.168.1.201 a 192.168.1.202. Server má například IP adresu 192.168.1.200. Pak do Docházky 3000 v menu *„Firma / Terminály BM-Finger“* zadáte přímo IP adresy terminálů (tedy 192.168.1.201 pro první terminál a 192.168.1.202 pro druhý terminál). Tlačítkem *„Spusť přenos hned“* ověříte, zda se server s terminály úspěšně spojil a pokud opravdu mají terminály ve svém menu nastaveny tyto IP adresy, VPN je nastavena správně a přenos neblokuje žádný další firewall či jiný systém, bude vše fungovat v pořádku.

Klienti, kteří budou ze svých počítačů pracovat s docházkou přes webový prohlížeč budou do adresního řádku prohlížeče jednoduše přímo zadávat IP adresu serveru, tedy 192.168.1.200 a tím se dostanou na úvodní obrazovku docházky, kde se přihlásí a mohou dle svých práv normálně s programem pracovat.

Při použití VPN je tedy nastavení docházky nejjednodušší a neliší se od nastavení v malé lokální síti. O nastavení VPN, která zajisti protunelování lokálního provozu přes internet, se postará váš správce IT či správce sítě či poskytovatel internetové datové konektivity. Ten správně nastaví routování i pokud lokální síť centrály bude používat např. IP 192.168.1.x a pobočka pak 192.168.2.x a podobně.

2. řešení – port-forwarding (*port proxy*)

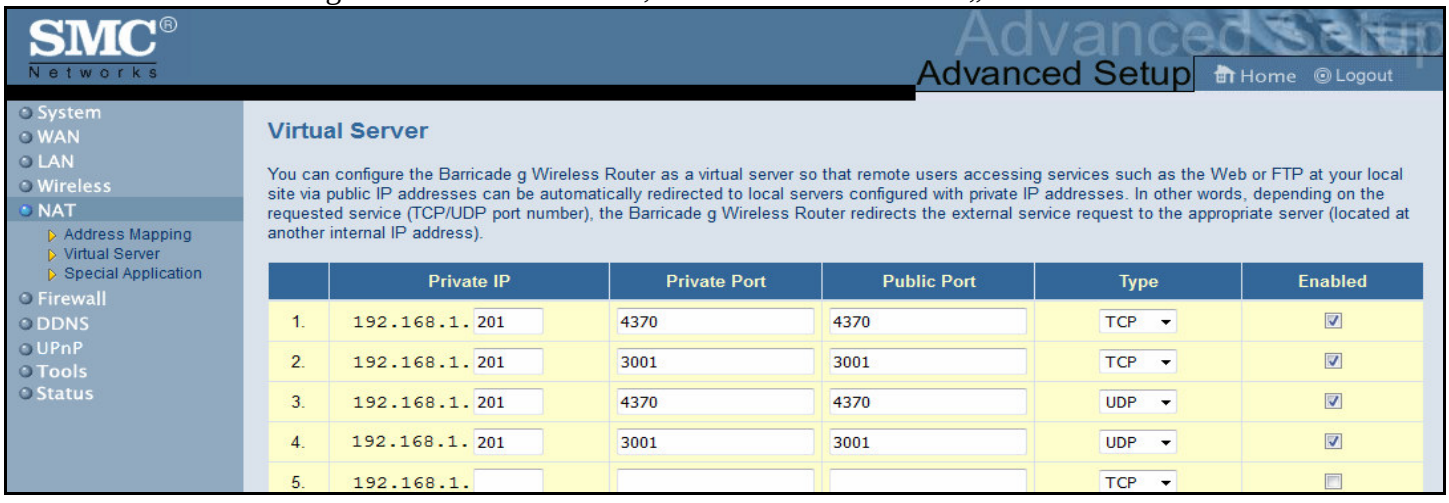
Pokud z nějakého důvodu nechcete zřizovat VPN, je možné situaci vyřešit pomocí proroutování portů používaných docházkou pro přenos dat z terminálů. Zde je třeba myslet na to, že přenos dat do programu iniciuje server, který spouští komunikaci tak, že se snaží připojit do terminálů na jejich porty 4370 a 3001 na TCP i UDP protokolu při použití terminálů BM-F201, BM-F630, BM-F702 a BM-F900 (protokol *Zkem*). U terminálu BM-F108 se používá protokol *FP-Clock*, který komunikuje na portu 5005. Dále ale budeme uvádět příklad řešení pro většinu terminálů používajících *Zkem* protokol.

V tomto případě tedy musíte znát IP adresy routerů přes které jsou pobočky připojeny do internetu (a při cloudovém serveru u providera také IP adresu routeru centrály). V těchto routerech se nastaví 4 pravidla, která zajistí přenos dat z internetu do terminálu. Tedy že když přijde na vstupu routeru z internetu požadavek na datový přenos na porty 4370 a 3001 na TCP i UDP protokolech, aby byly tyto datové pakety předány do vnitřní sítě na IP adresu terminálu. V menu terminálu v jeho konfiguraci sítě pak musí být nastavena síťová maska a brána tak, aby odpovědi terminál směroval na router této pobočky.

Například pokud má router pevnou veřejnou IP adresu, přes kterou je dostupný z internetu, nastavenou od poskytovatele připojení na 77.78.147.145 a vnitřní síť této pobočky bude používat IP adresy 192.168.1.x kde adresa vnitřního rozhraní routeru bude 192.168.1.1 a vnitřní adresa terminálu bude 192.168.1.201, pak bude port-forwarding na routeru nastavený na toto směrování:

port **4370 TCP** pro rozhraní s IP 77.78.147.145 přeroutovat na **4370 TCP** vnitřního rozhraní na IP 192.168.1.201
port **3001 TCP** pro rozhraní s IP 77.78.147.145 přeroutovat na **3001 TCP** vnitřního rozhraní na IP 192.168.1.201
port **4370 UDP** pro rozhraní s IP 77.78.147.145 přeroutovat na **4370 UDP** vnitřního rozhraní na IP 192.168.1.201
port **3001 UDP** pro rozhraní s IP 77.78.147.145 přeroutovat na **3001 UDP** vnitřního rozhraní na IP 192.168.1.201

Většina routerů má konfigurační webové rozhraní, ve kterém lze nastavení „naklikat“:



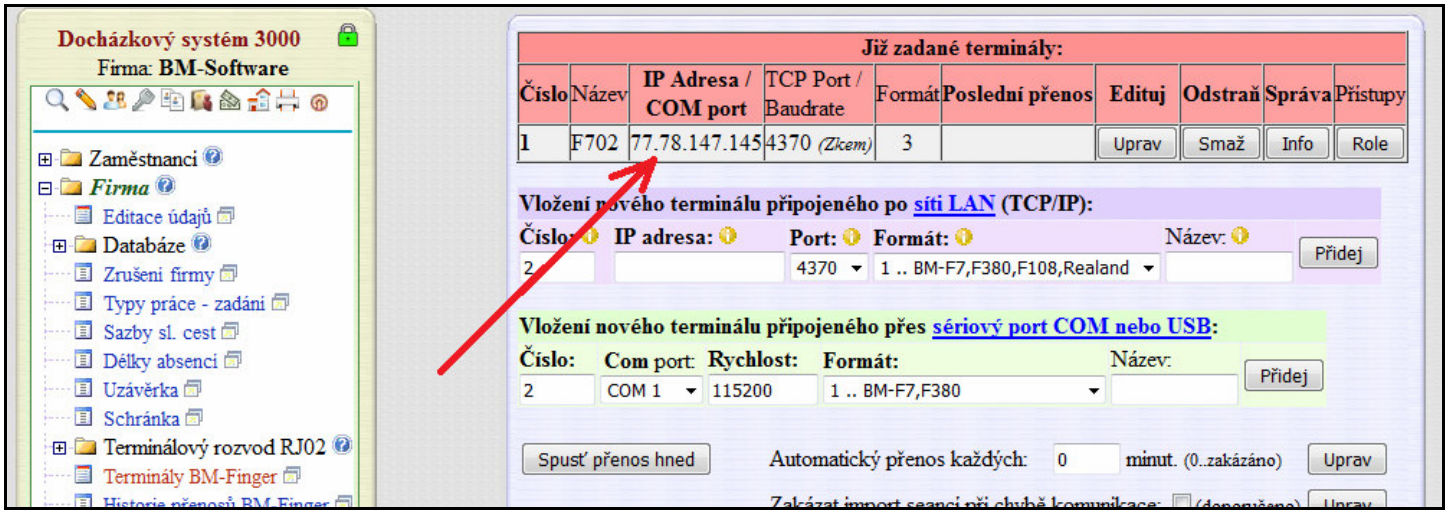
Pokud jako router používáte počítač se dvěma síťovými kartami a například operačním systémem Linux, lze nastavení routovacích tabulek provést pomocí příkazu *iptables* například na Centosu 6 těmito příkazy:

```
/bin/echo 1 > /proc/sys/net/ipv4/ip_forward
/sbin/iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
/sbin/iptables -I FORWARD -p tcp -i eth0 -o eth1 -s 192.168.1.201 -m state --state NEW,ESTABLISHED,RELATED --match multiport --ports 4370,3001 -j ACCEPT
/sbin/iptables -I FORWARD -p udp -i eth0 -o eth1 -s 192.168.1.201 -m state --state NEW,ESTABLISHED,RELATED --match multiport --ports 4370,3001 -j ACCEPT
/sbin/iptables -t nat -I PREROUTING -p tcp -i eth1 --dport 4370 -j DNAT --to-destination 192.168.1.201:4370
/sbin/iptables -t nat -I PREROUTING -p udp -i eth1 --dport 4370 -j DNAT --to-destination 192.168.1.201:4370
/sbin/iptables -t nat -I PREROUTING -p tcp -i eth1 --dport 3001 -j DNAT --to-destination 192.168.1.201:3001
/sbin/iptables -t nat -I PREROUTING -p udp -i eth1 --dport 3001 -j DNAT --to-destination 192.168.1.201:3001
```

V terminálu pak bude nastavena IP adresa 192.168.1.201, maska 255.255.255.0 a brána bude nastavena na vnitřní adresu routeru, tedy na IP 192.168.1.1

Tím bude zajištěno, že pokud z internetu přijde na veřejné rozhraní routeru požadavek na porty 4370 nebo 3001 na TCP či UDP protokolech, bude tento datagram předaný do vnitřní sítě na stejný port IP adresy terminálu a ten pak bude odpověď posílat zpět přes router ven do internetu. Router pobočky při předání odpovědi terminálu zpět do internetu podle tabulek ví adresu zdroje (router centrály či poskytovatele), takže odpověď přepošle iniciátoru komunikace.

Dále je důležité, že v samotné docházce v menu „*Firma / Terminály BM-Finger*“ nebudete zadávat IP adresy terminálů, ale IP adresy routerů poboček. Takže v docházce bude pro výše uvedený příklad nastavena IP adresa terminálu na 77.78.147.145. Toto je důležité neopomenout, protože docházka nekomunikuje přímo s terminálem, ale s routerem pobočky, který se pro ní za terminál jakoby vydává (maskuje překlad portů do vnitřní sítě).



Obdobně pokud je server umístěn u nějakého poskytovatele (např. VPS provider), zadáváte do docházky jako IP adresy terminálů ve skutečnosti IP adresu routeru centrály a pro druhý terminál IP adresu routeru pobočky. Port forwarding bude nastavený jak na routeru centrály (pro vnitřní adresu terminálu na centrále), tak na routeru pobočky (pro vnitřní IP adresu terminálu na pobočce).

Na každém pracovišti může být jen jeden terminál, protože docházka komunikuje s routery, které mají zpravidla jen jedno rozhraní do internetu, takže port forwarding docházky nelze nastavit pro více než jeden vnitřní terminál. Vstupní router by musel mít přiděleno více IP adres (nebo i více internetových rozhraní s připojením), aby se například na pobočce mohlo překládat více adres pro další terminály. Máte-li tedy např. na pobočce více terminálů, použijte první řešení se zavedením VPN, které toto omezení nemá a terminálů může být libovolné množství.

Výše uvedený postup řešil přenos dat mezi programem a terminály, kdy si docházkový program na serveru sahá do terminálů pro data. Zde tedy komunikaci iniciuje server a on kontaktuje terminály. Pokud mají mít uživatelé na pobočce možnost pracovat s programem docházky nainstalovaným na serveru v centrále, je třeba proroutovat pomocí port-forwardingu i opačný směr, kdy naopak klientská PC pobočky iniciují komunikaci se serverem na centrále. Při použití port-forwardingu tedy bude na routeru centrály nastaveno routování pro TCP

port 80 tak, že data se předají na vnitřní IP adresu serveru s docházkou. Klienti na pobočkách nebudou na svých PC do prohlížečů zadávat IP adresu docházkového serveru, ale IP adresu routeru centrály. Pokud podle příručky pro nastavení https budete používat i šifrovanou variantu http protokolu, nastaví se v routování překlad portu nejen pro port 80, ale i pro 443. Není-li server docházky u vás na centrále či pobočce, ale je u providera, je většinou dostupný přes veřejnou IP serveru, kterou provider poskytuje vašemu serveru, takže pak zadávají všichni uživatelé do svého prohlížeče tuto veřejnou IP adresu (či DNS název serveru) a pak mohou s docházkou pracovat dle nastavení třeba i z domova nebo odkudkoli z internetu. Tuto službu umí poskytnout i výrobce docházky – viz níže bod 4.

Pokud na serveru používáte další software, který je přístupný přes vzdálenou plochu (například RDP protokolem) jako třeba účetní program DUEL nebo jakýkoli jiný SW, který nemá webové rozhraní a uživatelé tedy již stejně využívají připojení na vzdálenou plochu serveru, není nezbytně nutné, aby s docházkou pracovali přes prohlížeč běžící na jejich klientské stanici, ale mohou mít ve vzdálené ploše spuštěný (vzdálený) prohlížeč, přes který budou s docházkou pracovat. Pak do adresy pro docházku nemusí zadávat internetovou IP adresu serveru, ale lze využít adresu lokální smyčky *127.0.0.1*, protože docházka i prohlížeč běží na stejném vzdáleném serveru, takže mezi nimi je spojení vlastně lokální uvnitř stejného počítače.

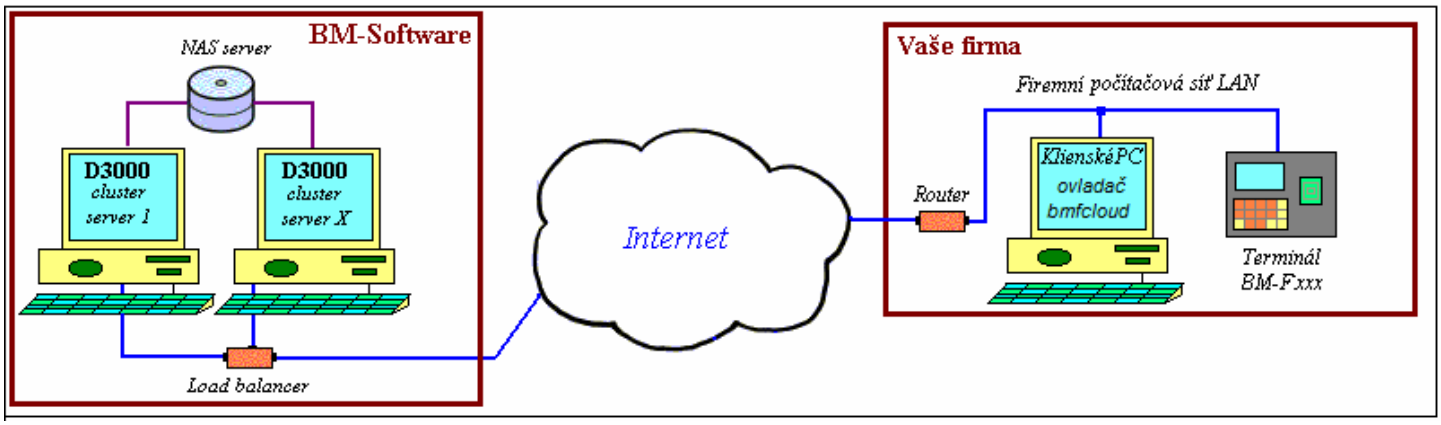
3. řešení – off-line přenos dat z terminálu

Pokud u vás nechcete používat ani jedno z výše uvedených řešení a ani níže v bodě 4 popsané řešení s cloudem u výrobce docházky, lze data z terminálu do programu dostat i pomocí souborů. Tedy ručně tak, že k terminálu přijdete, zapojíte do něj USB flash disk (flešku), dle dodaného tištěného návodu stáhnete načipované identifikace na tuto flešku do souboru a ten pak importujete do docházky opět dle dodaného tištěného návodu. Buď flešku přenesete k serveru docházky a zapojíte jí přímo do něj a provedete v docházce import, nebo jí můžete připojit i do libovolného jiného PC, které má do programu přes webový prohlížeč přístup (např. i PC na pobočce nebo jakékoli PC na centrále). Soubor lze ale odeslat i například e-mailem. Zde stačí, abyste z libovolného PC pobočky dokázali poslat e-mail někomu na centrále, což je většinou možné s úplně běžným připojením k internetu bez nutnosti použití VPN či port-forwardingu. V krajní situaci například i pomocí mobilu, který bude mít zprovozněna mobilní data (LTE, EDGE ...) a udělá třeba *wifi hot-spot* pro notebook, do kterého flešku připojíte a soubor na ní stažený z terminálu pošlete jako přílohu e-mailem někomu, kdo se dokáže přes webový prohlížeč do docházky připojit. Tento příjemce souboru jej uloží na disk (např. na plochu windows či do složky *stažené soubory* nebo kamkoli jej z e-mailu uloží), poté se přihlásí do docházky a dle tištěného návodu dodanému k systému v docházce v menu *„Zaměstnanci / Editace docházky / Import dat ostatní“* vybere uložený soubor z e-mailu, nastaví typ terminálu a spustí import dat.

Tuto off-line metodu se stažením dat pomocí flešky a následným importem do programu přes jeho webové rozhraní používají například stavební firmy, které mají zedníky na stavbách, je tam někde umístěný terminál připojený pouze do napájení a bez jakéhokoli datového spojení na server. Pracovníci čipují docházku na terminálu a občas (třeba jednou za týden nebo za měsíc a podobně) někde vezme flešku, objede autem staveniště a z terminálů postahuje data do souborů na fleše. Poté přijede na centrálu, spustí si docházku a datové soubory naimportuje do programu.
Tuto metodu s off-line přenosem dat pomocí flešky lze použít i pokud primárně využíváte automatický přenos dat po síti některým z výše uvedených postupů, ale z nějakého důvodu přestane komunikace dočasně fungovat a potřebujete například rychle zpracovat mzdy, jenže IT specialista není momentálně k dispozici aby datové přenosy po síti hned zprovoznil. Data prostě postahujete z terminálů pomocí flešky a naimportujete do docházky a můžete udělat mzdy hned i když síť vám zprovozní třeba až za týden.

4. řešení – použití cloudu výrobce docházky na *www.dochazka.eu*

Pokud vám nevyhovuje stále ani jedno z výše uvedených řešení, můžete využit možnosti cloudu poskytovaného přímo výrobcem programu Docházka 3000, firmou BM-Software. Jako výrobci docházkového programu *Docházka 3000* poskytujeme již od roku 2003 službu, kdy server docházky běží u nás a je pro vás dostupný odkudkoli, kde máte možnost se libovolným způsobem připojit k internetu.



Není třeba zavádět ani VPN ani port-forwarding a navíc můžete mít libovolný počet poboček či pracoviště s libovolným počtem terminálů na každé z nich. Tento systém funguje tak, že celá docházka běží u nás na našem serveru, terminály jsou u vás na pracovištích a jediné co je třeba pro automatický přenos dat z terminálů do programu udělat je, že na některý váš počítač nainstalujete malý komunikační prográmek. Ten bude načítat data z vašich terminálů ve vaší síti pobočky a odesílat je http protokolem na náš cloudový server. Takže od nás se k vám do vaší sítě my nikdy nepřipojujeme a nemusíte v nastavení vaší sítě dělat žádné změny. Není třeba otevírat do internetu žádné adresy či porty navíc. Tento program běží u vás a on odesílá data k nám. My tedy žádné spojení do vaší sítě nepotřebujeme.

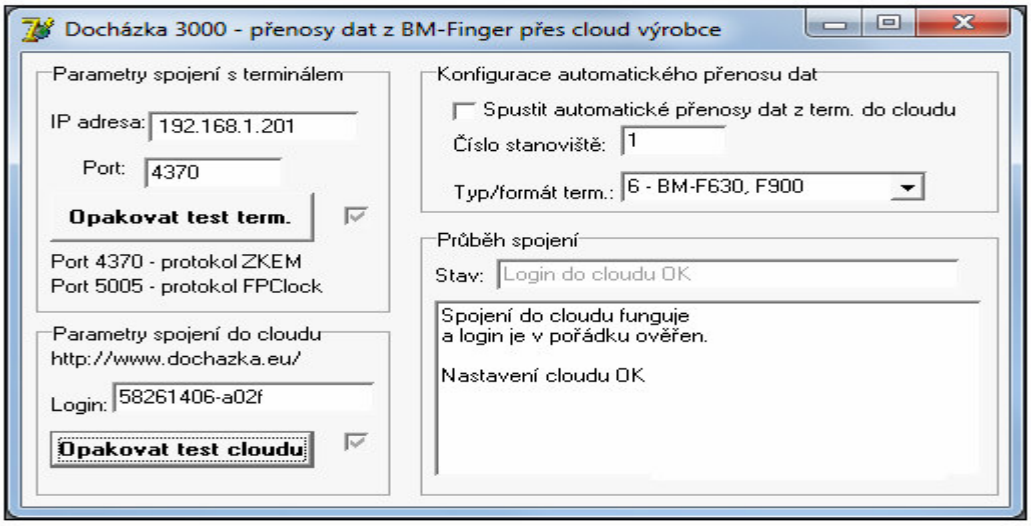
Veškeré informace o této možnosti provozu docházky naleznete na webu na adrese http://cloud.dochazka.eu/ nebo http://www.dochazka.eu/cloud/

5. řešení – použití cloudového ovladače terminálů

Tento postup využívá instalaci cloudového ovladače terminálu BM-Finger pro systém Docházka 3000 verze 8.06 a vyšší.

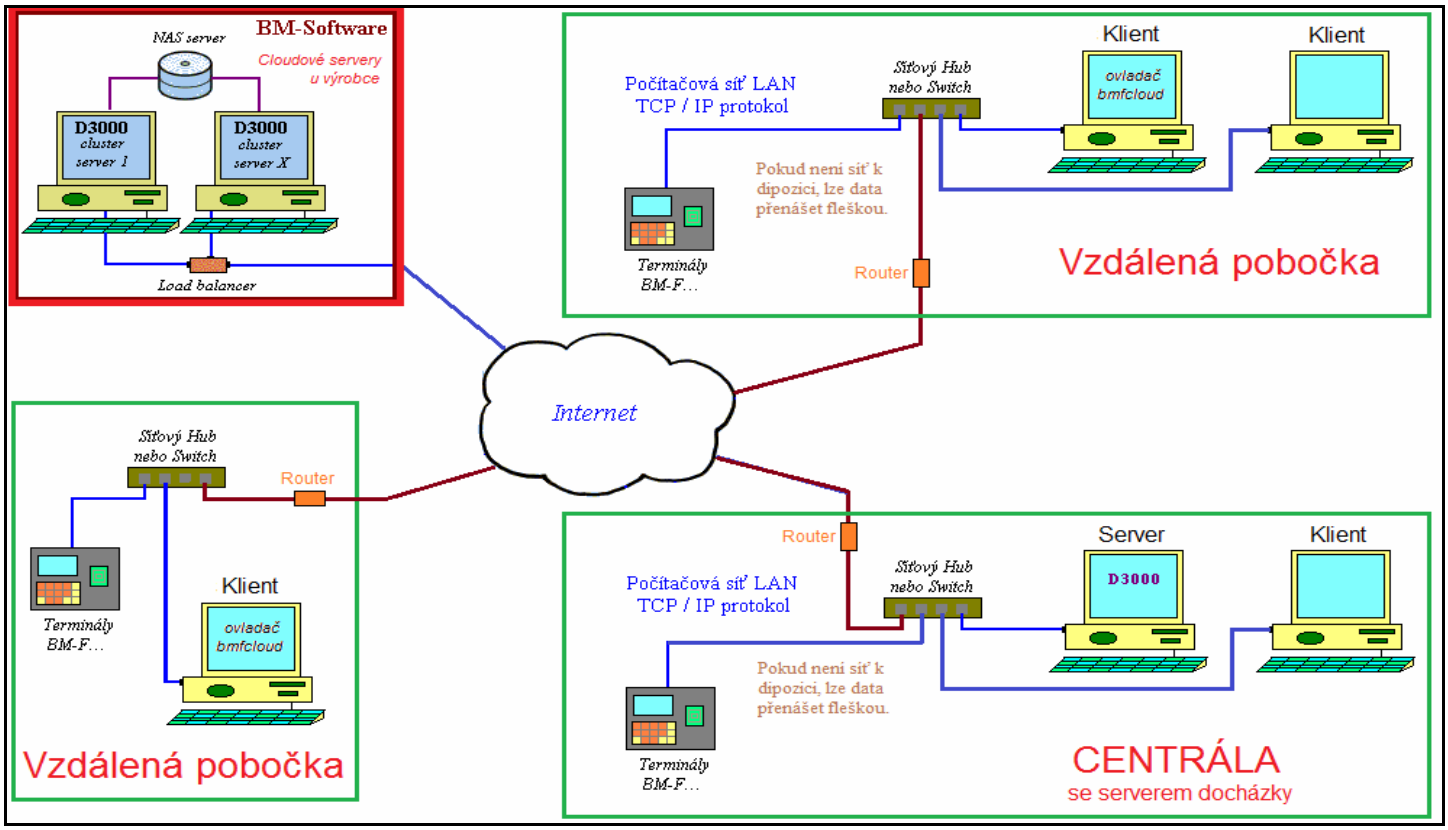
Program Docházka 3000 máte nainstalovaný na vašem lokálním PC (případně serveru) například na centrále firmy a s terminály centrály komunikuje napřímo pomoci lokální počítačové sítě LAN. Jenže dále máte jednu nebo více poboček, které nemají do sítě LAN na centrále přístup, nechcete mezi centrálou a pobočkami zařizovat VPN ani nastavovat routování portů popsané ve druhém bodě výše uvedeného návodu, ani nechcete přecházet s celou docházkou do cloudu. Data i aplikace chcete mít na svém serveru. Využijete tedy možnost toho, že pobočky budou data z terminálů posílat na cloudový server výrobce a systém Docházka 3000 nainstalovaný na počítači v centrále si je bude z cloudového serveru stahovat.

Na pobočkách poběží na nějakém PC tento komunikační program bmfingercloud.exe, který stahuje data z terminálu a odesílá je na cloudový server, odkud si je přebírá hlavní PC docházky na vaší centrále.



Tím, že uvedený princip přenosu dat využívá ke všem spojením obyčejný *http* protokol, stačí na všech pracovištích zcela běžné připojení k internetu, není potřeba dělat žádné úpravy síťové konfigurace, routování a podobně, takže nepotřebujete odborný zásah IT pracovníka z oboru počítačových sítí. Vše sami zvládnete nastavit pomocí dodávaného návodu. Navíc do cloudu se odesílá minimum anonymních dat a jsou tam uložena jen dočasně. Jedná se o záznamy obsahující číslo pracovníka a datum a čas čipnutí na jednotlivých terminálech. Žádná jména ani osobní údaje či podobně se do cloudu nepřenáší.

Příklad schémata propojení ukazuje následující obrázek:

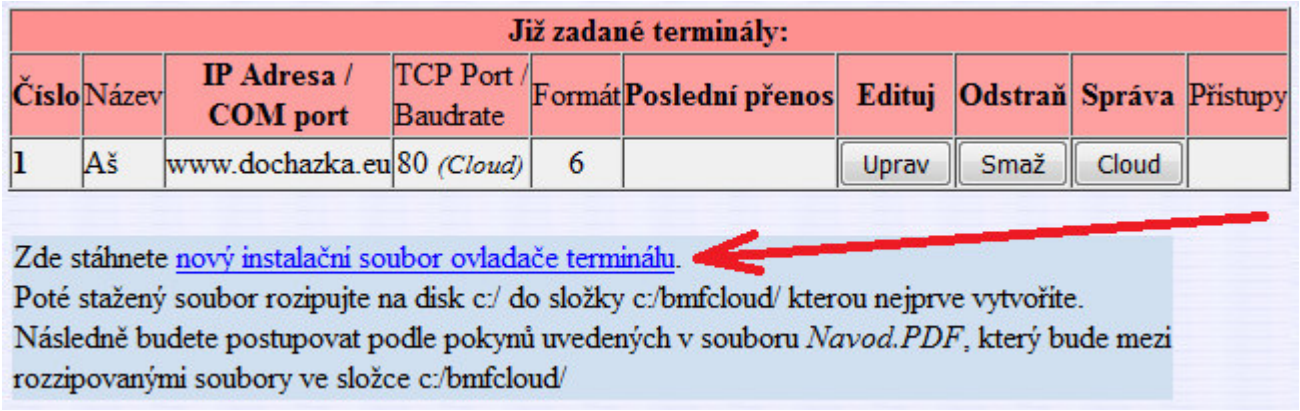


Data ze dvou vzdálených poboček odesílá ovladač nainstalovaný na PC pobočky pomocí http protokolu zcela běžným internetovým připojením do cloudového serveru výrobce BM-Software (*www.dochazka.eu)* odkud si je následně opět přes http protokol a běžné připojení k internetu přebírá docházkový server na centrále.
S terminálem na centrále komunikuje server přímo přes klasické nastavení popsané v dodané dokumentaci. Přes cloud se přenáší jen data z poboček.

Zprovoznění tohoto způsobu dat je poměrně jednoduché. Stačí v Docházce 3000 v menu *Firma / Terminály BM-Finger“* zadat do fialového formuláře *„Vložení nového terminálu připojeného po síti LAN“* záznam s položkou *IP adresa* nastavenou na hodnotu *www.dochazka.eu*

Port nastavit na 80 a formát dle verze vašeho terminálu (viz dodaný tištěný návod k terminálu).

Když záznam uložíte (viz následující obrázek), najdete pod tabulkou zadaných terminálů stručný popis a hlavně odkaz na stažení souboru s ovladačem a návodem. Pravým tlačítkem myši kliknete na odkaz *„nový instalační soubor ovladače terminálu“* a stáhnete jej na svůj počítač, kde stažený soubor *bmfcloud.zip* rozzipujete do předpřipravené složky *c:\bmfcloud* ve které pak po rozzipování najdete v souboru *Navod.PDF* postup, podle kterého ovladač nainstalujete, nastavíte, provedete registraci vaší firmy v cloudu výrobce a celý systém přenosu dat zprovozníte.



Již zadané terminály:									
Číslo	Název	IP Adresa / COM port	TCP Port / Baudrate	Formát	Poslední přenos	Edituj	Odstraň	Správa	Přístupy
1	Aš	www.dochazka.eu	80 *(Cloud)*	6		Uprav	Smaž	Cloud	

Zde stáhnete nový instalační soubor ovladače terminálu.
Poté stažený soubor rozipujte na disk c:/ do složky c:/bmfcloud/ kterou nejprve vytvoříte.
Následně budete postupovat podle pokynů uvedených v souboru *Navod.PDF*, který bude mezi rozzipovanými soubory ve složce c:/bmfcloud/

Výhodou tohoto řešení je jeho běžná dostupnost a snadná instalace bez nutnosti změn konfigurace sítě. Ovšem omezením je to, že terminály nelze vzdáleně konfigurovat přes program Docházka 3000 v jeho admin. menu *„Firma / Terminály BM-Finger“* přes tlačítka *Správa/Info* a *Přístupy/Role* (nastavovat práva, čas atd.) ani vzdáleně nastavovat uživatele v menu *„Zaměstnanci / Editace údajů / BM-Finger“*. Tyto možnosti jsou dostupné pouze u prvního řešení s VPN a u druhého s port-forwardingem. Zároveň je třeba udržovat program Docházka 3000 aktualizovaný, tedy alespoň jednou za rok pořídit aktualizaci, aby program nebyl starší jak 12 měsíců. Jinak by díky jeho zastarání přestal přenos dat fungovat, protože cloudová infrastruktura u výrobce reaguje na nové vývojové verze programu a tak výrobce podporuje maximálně 18 měsíců staré verze SW.

Závěr:

V této příručce jste tedy nalezli pět možných řešení, jak zajistit přenos dat mezi programem docházky a čipovacími terminály umístěnými na vzdálených pobočkách. Například pokud máte centrálu v Praze, ale pobočky jsou v Brně, Ostravě, Košicích a třeba Londýně. I na pobočkách chcete mít terminály, ale docházku za všechny společně potřebujete zpracovávat centrálně v jednom programu, ve kterém uvidíte docházku všech zaměstnanců bez ohledu na to, na které pobočce právě pracují.

První dvě navržená řešení automatického přenosu dat z terminálů do programu vyžadují konfiguraci sítě ze strany správce IT nebo poskytovatele připojení k internetu, tedy odborníka na správu sítí, ale pak je zajištěn plnohodnotný přenos dat včetně možnosti vzdálené konfigurace terminálů, uživatelů přístupových práv a podobně.
Třetí řešení lze použít i když žádné připojení poboček neexistuje, ale vyžaduje ruční stažení dat z terminálu.
Čtvrté řešení je použitelné i bez zásahu odborného IT pracovníka přes počítačové sítě a nabízí automatický přenos dat z terminálu do cloudové instalace docházky na serveru výrobce. Výhodnou je i to, že nemusíte mít na starosti docházkové PC, zálohy databáze, aktualizace programu atd.
Páté řešení opět nepotřebuje konfiguraci sítě a síťových prvků, všude stačí běžné připojení k internetu a cloudový server výrobce slouží jen jako dočasné úložiště načipovaných identifikací, odkud si je stahuje hlavní PC docházky ve vaší centrále, vše jednoduše http protokolem.