

Přístup do docházky z ostatních počítačů v síti

S docházkovým systémem je možné plnohodnotně pracovat i z dalších počítačů ve Vaší síti dle licence OS.

1. Nejprve je potřeba přímo na docházkovém serveru (PC na kterém je docházka nainstalovaná) zjistit jeho IP adresu. To provedete tak, že kliknete ve Windows vlevo dole na tlačítko *Start*, vyberete *Programy* (nebo *Všechny programy*) dále *Příslušenství* a *Příkazový řádek*. Objeví se černé okno do kterého napíšete příkaz *ipconfig* a potvrdíte klávesou *Enter*. Zobrazí se nastavení sítě a hned jeden z prvních řádků nahoře obsahuje položku *"IP adresa ...* a za ní je uvedené číselná adresa počítače docházky - docházkového serveru. Například to bude adresa *192.168.1.10*.

2. Nyní přejdete na druhý počítač, ze kterého se chcete do docházky přihlásit. Spustíte zde webový prohlížeč a do položky *Adresa* (nikoli do vyhledávání) zadáte adresu docházky, kde místo *localhost* uvedete číselnou adresu zjištěnou v předchozím bodě. Například tuto: *http://192.168.1.10/dochazka2001/*

Pokud by se docházka nezobrazila, je zřejmě na hlavním PC docházky (docházkovém serveru - viz bod 1) nainstalovaný Firewall bránící přístupu ze sítě. V něm je potřeba udělat výjimku buď pro TCP port 80, nebo pro aplikaci *c:\apache\apache\bin\httpd.exe*. Ukážeme si nastavení výjimky pro port 80 u operačního systému WinXP a Vista nebo Win7. Pro Win10 je postup níže. Akce je třeba provádět přímo na hlavním PC docházky.

Postup pro Windows XP:

Ve Windows kliknete vlevo dole na tlačítko *Start*, vyberete *Ovládací panely* a rozkliknete ikonu *Brána Firewall systému Windows*

Na kartě *Vyjímky* klepnete na *Přidat port*

Do položky *Název* zadáte *Docházka3000* a do položky *Port* napište číslo *80*.

Protokol nechte nastavený na *TCP* a klepnete na *OK*

Pak již bude možné připojit se k docházkovému systému i z jiných počítačů sítě.

Pokud máte novější operační systém Windows, záleží postup pro odblokování portu 80 ve firewallu na konkrétní konfiguraci vzhledu Vašich windows. Níže naleznete několik možných postupů, jak požadovaného cíle dosáhnout. Pokud se nepodaří první (neuvidíte uvedené položky v oknech), zkoušejte další postupy.

Postup pro Windows Vista, Win7 a novější (možnost 1):

Ve Windows kliknete vlevo dole na tlačítko *Start*, vyberete *Ovládací panely*, vlevo nahoře přepnete na *Klasické zobrazení* a rozkliknete ikonu *Brána Firewall systému Windows*

Vpravo kliknete na *Změna nastavení* a na kartě *Vyjímky* klepnete dole na *Přidat port*

Do položky *Název* zadáte *Docházka3000* a do položky *Port* napište číslo *80*

Protokol nechte nastavený na *TCP* a klepnete na *OK* a znovu *OK*

Pak již bude možné připojit se k docházkovému systému i z jiných počítačů sítě.

Postup pro Windows Win7, Win8 64bit a novější (možnost 2):

Ve Windows kliknete vlevo dole na tlačítko *Start*, vyberete *Ovládací panely*, vlevo nahoře přepnete na *Systém zabezpečení* a dále rozkliknete ikonu *Brána Firewall systému Windows*

Vlevo kliknete na *Upřesnit nastavení* a v novém okně vlevo nahoře na *Příchozí pravidla*. Poté vpravo nahoře kliknete na *Nové pravidlo* a v dalším okně kliknete na *Port* a *Další*.

Typ portu nechte zatržený *TCP* a do položky *Konkrétní místní porty* napište číslo 80. Klikněte na *Další*, nechte zatrženo *Povolit připojení* a opět klikněte na *Další*. Nechte zatržené všechny 3 body a opět klikněte na *Další*. Název zadejte *Docházka 3000* a klikněte *Dokončit*.

Postup pro Windows Win7, Win8 64bit a novější (možnost 3):

Ve Windows kliknete vlevo dole na tlačítko *Start*, vyberete *Ovládací panely*.

Vlevo nahoře přepnete na *Systém zabezpečení* a v sekci *Brána Firewall systému Windows* klikněte na odkaz *Povolit program v bráně Windows Firewall*

Klikněte na tlačítko *Povolit jiný program* a následně na tlačítko *Procházet*

Přes odkaz *Tento počítač* vyberte na disku *C:* ve složce *C:\apache\apache\bin* soubor *httpd.exe*

Poté klikněte na *Přidat*.

U nového řádku s položkou *Apache httpd server* zatrhněte obě Volby (*Domácí* i *Veřejná*) a potvrďte *OK*

Pokud se nepodaří ani podle jednoho z výše uvedených postupů akci nastavit, protože Vaše windows mají jiný vzhled a prostě uvedené volby na obrazovce nevidíte, máte zřejmě omezená práva a kontaktujte Vašeho správce sítě. Ten potřebné odblokování portu 80 zajistí přes administrátorský účet Vašeho docházkového PC.

Pokud používáte šifrovaný https protokol, je třeba ve firewallu povolit i port 443.

Síťové přístupy mohou být omezeny licencí operačního systému – viz níže část *Informace k licenci Windows*.

Podrobný postup pro Windows 10 (možnost 4):

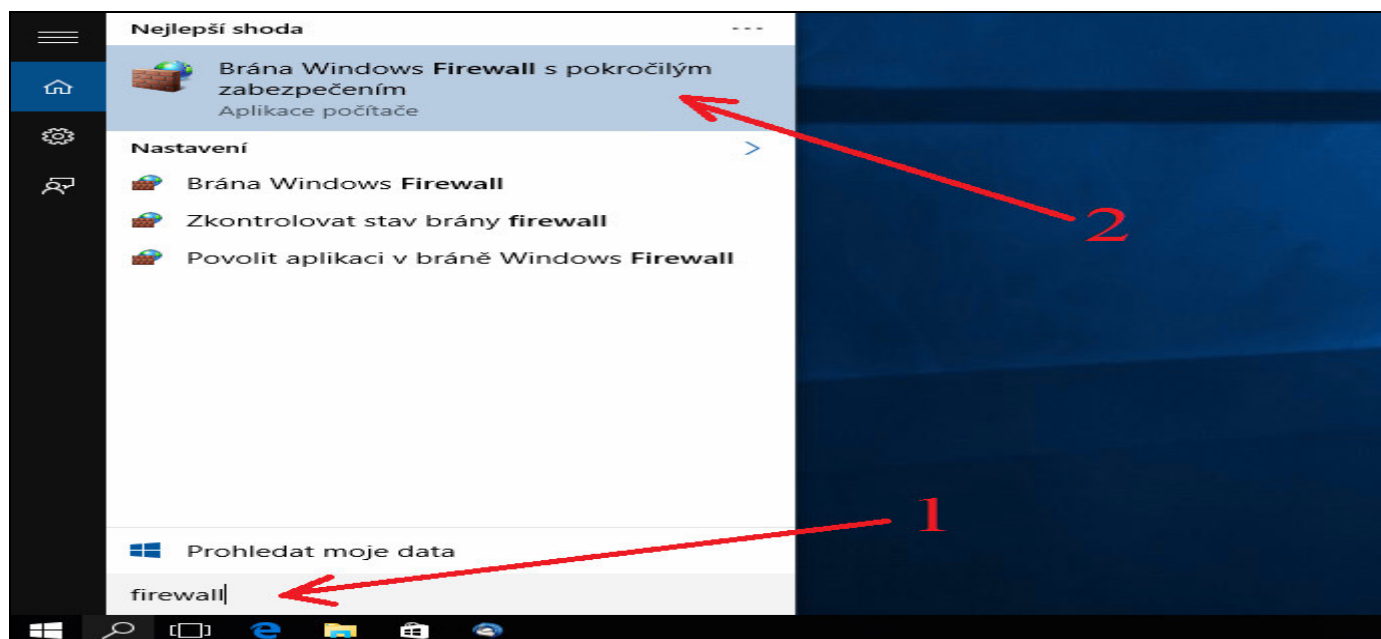
U Windows 10 si ukážeme celý postup podrobně i s obrázky. Nejprve na hlavním PC docházky odblokujeme port 80 ve firewallu a zjistíme IP adresu tohoto hlavního docházkového PC (docházkového serveru). Poté na druhém (klientském) počítači přes prohlížeč ověříme, že vše funguje a s docházkou pak lze podobně pracovat odkudkoli z místní vnitřní firemní sítě.

1. Odblokování firewallu na hlavní PC docházky:

Dole na liště windows klikněte na ikonu lupy vedle ikony nabídky Start

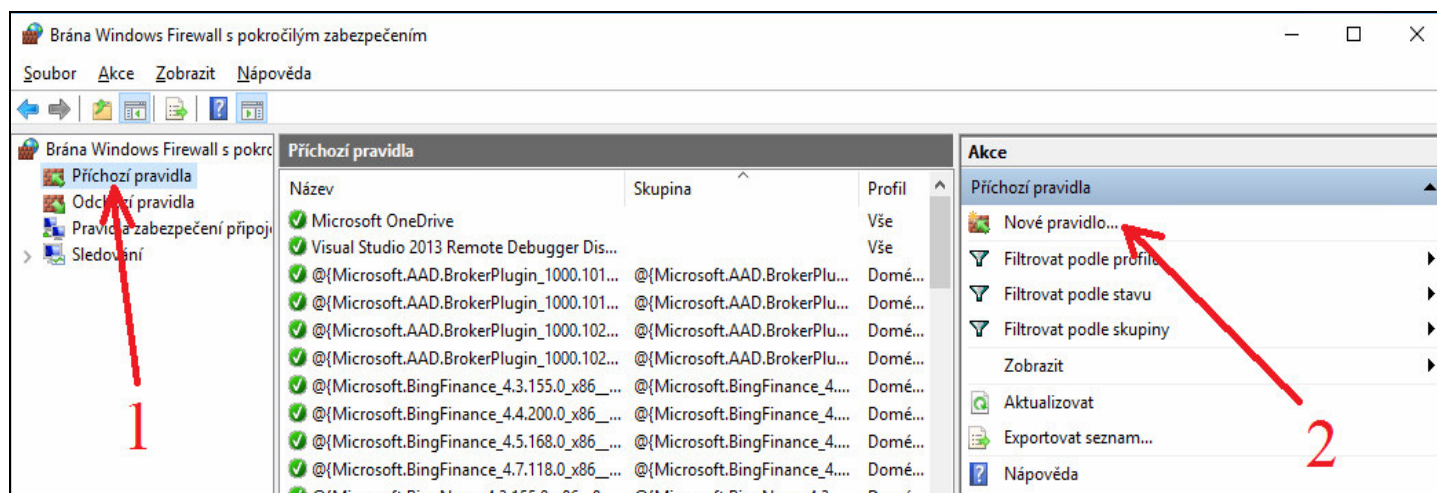


Otevře se vyhledávací dialog, do kterého dole napište slovo: firewall

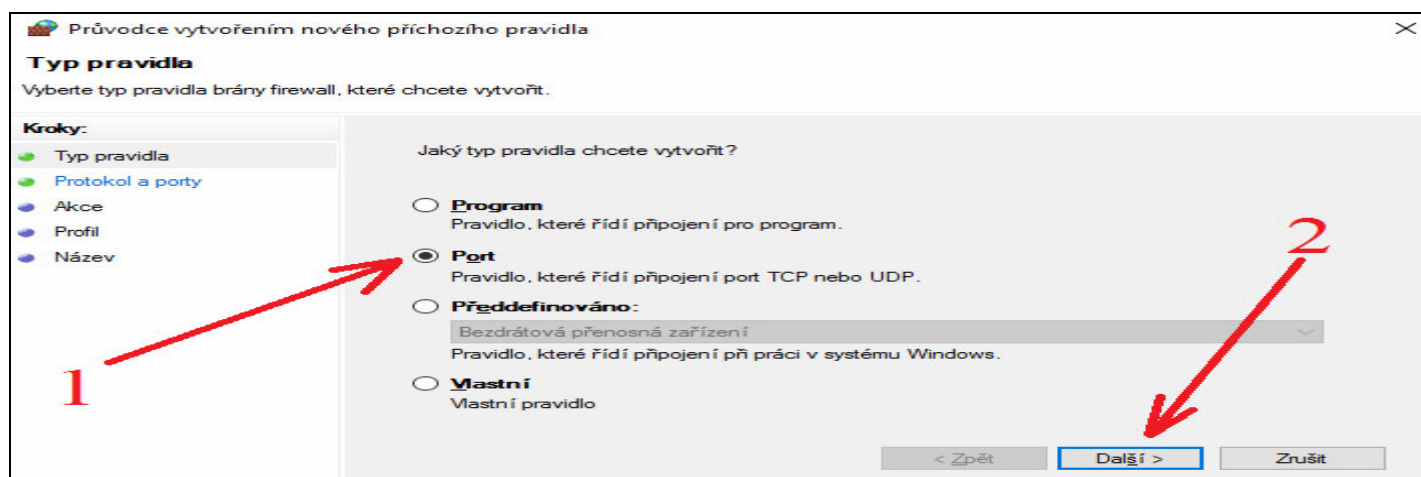


Poté z nabídky nalezených shod rozkliknete volbu „Brána Windows Firewall s pokročilým zabezpečením“.

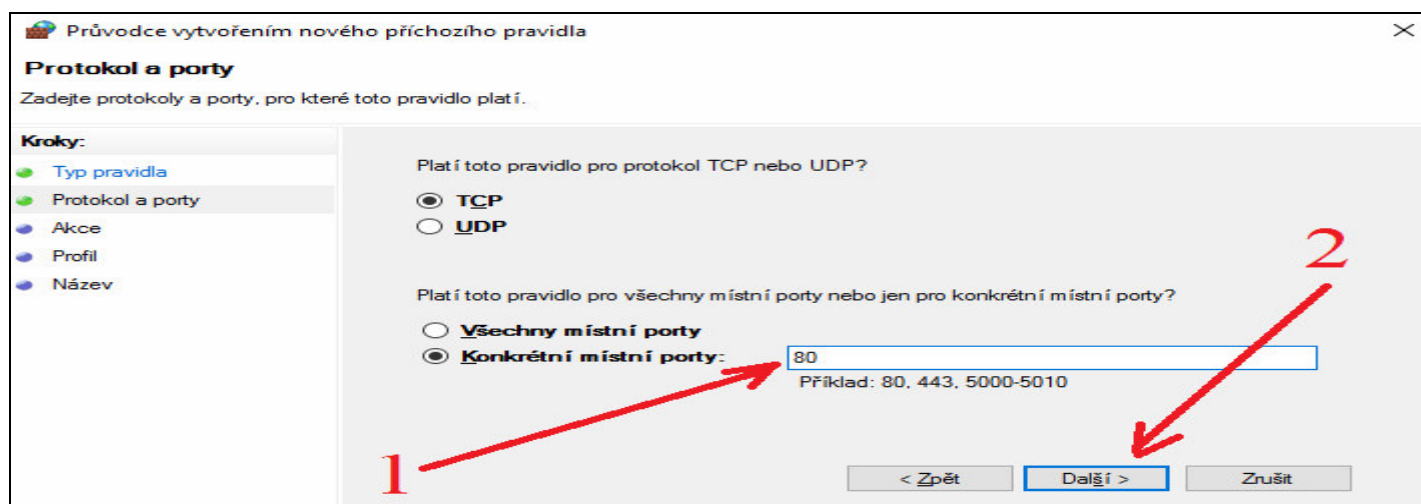
Otevře se okno nastavení firewallu, ve kterém kliknete vlevo nahoře na „Příchozí pravidla“ a poté vpravo nahoře na „Nové pravidlo“.



V průvodci vyberete typ pravidla *Port* a kliknete na *Další*



Protokol necháte vybraný *TCP* a zatrženou kolonku *Konkrétní místní porty*, do které dopíšete číslo 80. Pokud jste web server docházky Apache přeměrovaly na jiný port, dopíšete ten, který Apache používá. Ve výchozí instalaci se ale používá port 80, takže pokud jste nic neměnili, zapíšete osmdesátku. Pokud používáte i šifrovaný https protokol, je třeba ve firewallu povolit i port 443. Nakonec kliknete na *Další*.



Ve volbě *Akce* ponecháte standardní *Povolit připojení* a kliknete na *Další*.

Průvodce vytvořením nového příchozího pravidla

Akce

Určete, jaká akce má být provedena v případě, že připojení odpovídá podmínkám stanoveným pravidlem.

Kroky:

- Typ pravidla
- Protokol a porty
- Akce**
- Profil
- Název

Kterou akci lze provést, splňuje-li připojení zadané podmínky?

Povolit připojení
Budou zahmuta připojení, která jsou chráněna protokolem IPsec, i připojení, která chráněna nejsou.

Povolit připojení, je-li zabezpečené
Budou zahmuta pouze připojení, která byla ověřena pomocí protokolu IPsec. Připojení budou zabezpečena pomocí nastavení vlastností v protokolu IPsec a pravidel v uzlu pravidla zabezpečené připojení.

Blokovat připojení

< Zpět **Další >** Zrušit

V profilu ponecháte zatrženy všechny volby a opět jen potvrdíte tlačítkem *Další*.

Průvodce vytvořením nového příchozího pravidla

Profil

Zadejte profily, na které se toto pravidlo vztahuje.

Kroky:

- Typ pravidla
- Protokol a porty
- Akce
- Profil**
- Název

Kdy platí toto pravidlo?

Doména
Bude použito v případě, že je počítač připojen do své domény.

Privátní
Bude použito v případě, že je počítač připojen k privátní síti, například doma nebo na pracovišti.

Veřejný
Bude použito v případě, že je počítač připojen do veřejné skupiny v síti.

< Zpět **Další >** Zrušit

V posledním bodě průvodce zadáte pro toto nové pravidlo výstižný název, můžete uvést podrobný popis a nakonec kliknete na *Dokončit*.

Průvodce vytvořením nového příchozího pravidla

Název

Zadejte název a popis tohoto pravidla.

Kroky:

- Typ pravidla
- Protokol a porty
- Akce
- Profil
- Název**

Název:
Docházka 3000

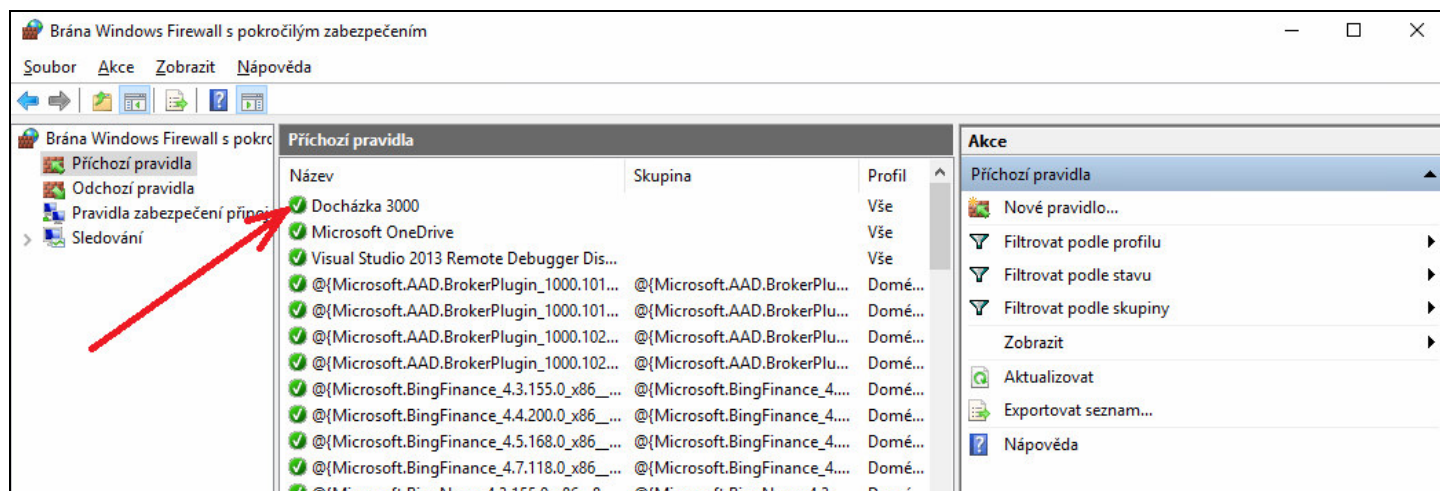
Popis (nepovinné):
Připojení do docházkového systému z ostatních počítačů v síti.

1 (red arrow pointing to 'Název' step in the sidebar)

2 (red arrow pointing to 'Dokončit' button)

< Zpět **Dokončit** Zrušit

Tímto postupem jste tedy zajistili, že bude možné pracovat s docházkou z ostatních počítačů. Firewall již nebude ve spojení po síti bránit. Nové pravidlo se přidá mezi stávající platná pravidla. To, že pravidlo funguje a není zakázáno, poznáte podle zelené „fajky“ před jeho názvem.



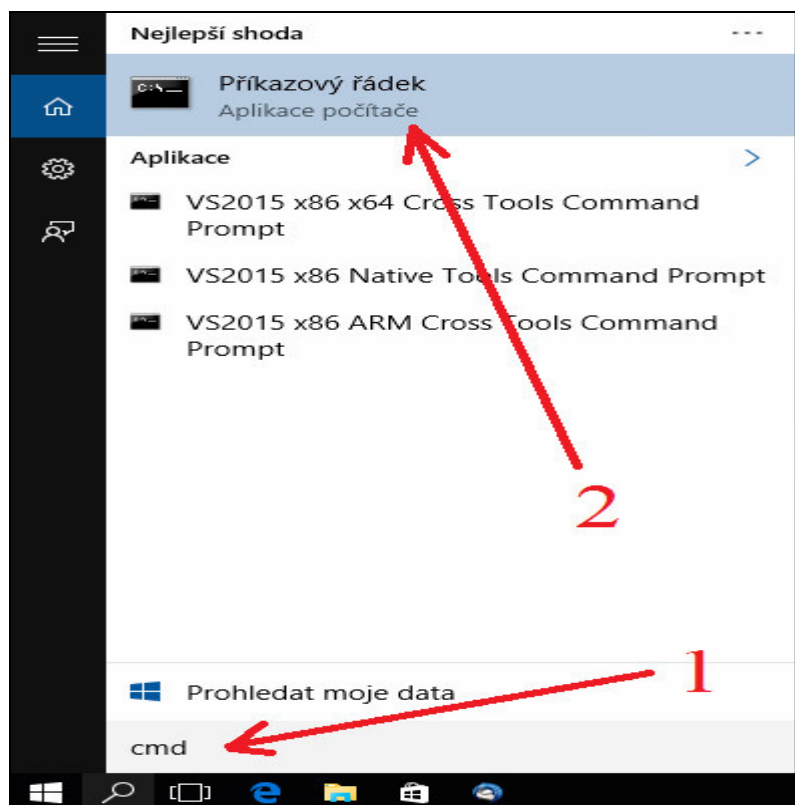
Tímto jsme nastavili firewall. Okno s nastavením firewallu již nebudeme potřebovat, takže jej můžete zavřít.

2. Zjištění IP adresy hlavního docházkového PC:

Dalším krokem je zjistit, jakou má tento hlavní počítač docházky IP adresu. Tu budeme používat pro spojení z ostatních počítačů. Opět stačí jednoduše kliknout na ikonu lupy na dolní liště windows:



A do vyhledávacího políčka zadáme příkaz `cmd`
Z nabídnutých možností vyberte *Příkazový řádek*.



Otevře se černé okno příkazového řádku, do kterého zadáte příkaz *ipconfig*

```
C:\> Příkazový řádek
Microsoft Windows [Version 10.0.10532]
(c) 2015 Microsoft Corporation. Všechna práva vyhrazena.
C:\Users\Petr>ipconfig
```

Poté dojde k vypsání parametrů nastavení počítačové sítě v tomto počítači.

```
C:\> Příkazový řádek
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f6:735c:cf5:3592%3
    IPv4 Address. . . . . : 192.168.1.25
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter 6T04 Adapter:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2002:c801:129::c801:129
    Default Gateway . . . . . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:5ef5:79fd:1025:3cb:37fe:fed6
    Link-local IPv6 Address . . . . . : fe80::1025:3cb:37fe:fed6%2
    Default Gateway . . . . . : 

Tunnel adapter isatap.{3E4E3C9B-30B5-48D3-AC20-E458EA2E0305}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
C:\Users\Petr>
```

Budete hledat řádek s položkou „IPv4 Adresa“ nebo „IPv4 Address“. Bude to hned jeden z prvních řádků. Viz zvětšený výřez na barevně invertovaném obrázku níže.

```
C:\> Příkazový řádek
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f6:735c:cf5:3592%3
    IPv4 Address. . . . . : 192.168.1.25
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter 6T04 Adapter:
```

Zde tedy vidíme, že náš hlavní počítač docházky, na kterém jsme příkaz zadali, má IP adresu 192.168.1.25
Váš počítač bude mít zřejmě IP adresu jinou, takže si jí někde poznamenejte.

Důležité je všechny výše uvedené kroky z bodů 1 i 2 spouštět opravdu přímo na hlavním PC docházky – docházkovém serveru. Tedy na tom PC, kam jste docházku instalovali z CD.

3. Ověření přístupu do docházky z ostatních PC:

Nyní tedy již máme nastaven hlavní počítač docházky tak, aby povolil síťová spojení do programu z ostatních počítačů a známe také IP adresu tohoto hlavního docházkového PC, na kterém docházka běží (web server, databáze atd.). Můžeme se tedy přesunout k jinému (klientskému) PC, které je zapojeno do stejné sítě LAN a ze kterého budeme chtít rovněž s docházkou pracovat.

Pokud v naší síti není nic dalšího, co by přenos mohlo blokovat (antivir, jiný firewall atd.), mělo by být možné na tomto klientském počítači spustit prohlížeč, zadat do něj IP adresu docházkového serveru zjištěnou výše v bodě 2 a po „odentrování“ by se měla docházka zobrazit.

Název firmy	ID firmy	Datum založení	Verze DB	Pracovníků	Přihlášení
Moje firma	1	10.03.2011	7.11	650	61997 (05.05.2016)

Adresu je třeba zadat do adresního řádku. Nikoli do řádku pro vyhledávání nebo jiného místa. Pokud vše funguje, uložte stránku do záložek, nebo jí nastavte v prohlížeči jako výchozí. Pak nebude třeba pokaždé psát adresu ručně. Lze vytvořit i zástupce na plochu tak, že do cíle zadáte např. `http://192.168.1.25/dochazka2001/` čímž se vytvoří zástupce přímo na ploše pro pohodlné spuštění docházky jedním dvojklikem myši.

Mělo by stačit zadat jen samotnou IP adresu docházkového serveru. Tedy v našem příkladě `192.168.1.25` a zmáčknout klávesu *Enter*. Pouze pokud jste náhodou webovou složku docházky přejmenovali, musíte zadat i jméno složky za adresou (např. `http://192.168.1.25/mojeslozka/`).

Pokud jste Apache web server docházky přesměroval na jiný port než 80, je třeba tento port uvést jak v kroku 1 tohoto návodu (nastavení firewallu), tak pak i zde v prohlížeči na klientském PC. například pokud jste pro apache web server docházky použili port 8080, zadáte na klientském PC adresu např. `192.168.1.25:8080`

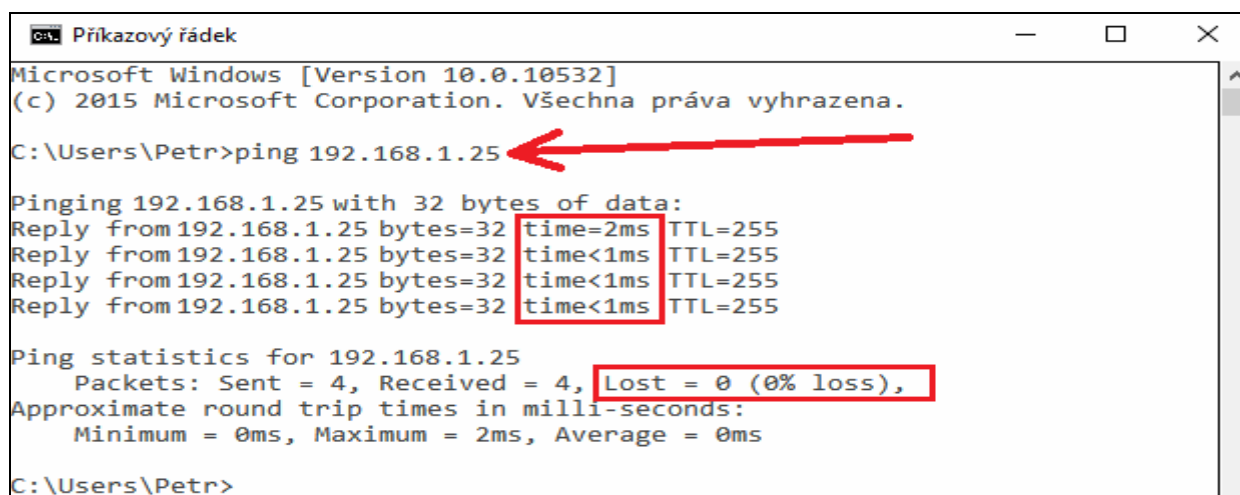
4. Řešení problémů:

Pokud časem přestane připojení do docházky z jiných PC fungovat, ale na samotném hlavním PC docházka funguje normálně, mohlo dojít k různým změnám ve vaší síti.

Například kolize IP adres, kdy nějaké jiné zařízení (počítač, tiskárna, tablet ...) dostane stejnou adresu jako hlavní docházkový server. Což se může stát při statickém přidělení IP adresy.

Závada na ethernetovém kabelu, v portu switchu, vytažený kabel v rozvaděči a podobně. Lze ověřit například příkazem *ping* spuštěným v příkazovém řádku na klientském PC.

Ověření spojení příkazem ping spuštěným na klientském PC ukazuje následující obrázek



```
cmd.exe Příkazový řádek
Microsoft Windows [Version 10.0.10532]
(c) 2015 Microsoft Corporation. Všechna práva vyhrazena.

C:\Users\Petr>ping 192.168.1.25

Pinging 192.168.1.25 with 32 bytes of data:
Reply from 192.168.1.25 bytes=32 time=2ms TTL=255
Reply from 192.168.1.25 bytes=32 time<1ms TTL=255
Reply from 192.168.1.25 bytes=32 time<1ms TTL=255
Reply from 192.168.1.25 bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.25
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Petr>
```

Docházkový server v pořádku odpovídá, časy odpovědí jsou běžné pro lokální síť a žádné pakety se po cestě neztratily. Pokud se místo časů odpovědí vypíše chybové hlášky (např. *Destination port unreachable*), je třeba hledat chybu a kontaktovat správce sítě.

Také je možné, že se změnila IP adresa hlavního PC docházky. Například pokud se IP adresy přidělují dynamicky pomocí DHCP, je třeba buď znovu projít body 2 a 3 výše uvedeného návodu, nebo IP adresu docházkovému serveru přidělit staticky (a z dhcp rozsahu jí vyjmout), nebo místo IP adresy používat doménové jméno hlavního docházkového PC.

Síťové spojení může také blokovat antivir nebo jiný firewall než standardní z windows (např. *Kerio* a podobné) nainstalované jak na hlavním PC docházky, tak také i na klientském PC. I pokud docházka nějakou dobu normálně funguje a poté se jakoby z ničeho nic přestane u klientů připojení dařit, může to být antivirem nebo firewallem, který se automaticky zaktualizoval a najednou začne připojení blokovat. Takové „závady“ se samozřejmě obtížně hledají a u uživatelů vyvstávají otázky typu „*Proč to nejednou nefunguje? Ještě nedávno to šlo, teď to nejde a já jsem mezi tím nic určitě neměnil.*“, V tomto případě nepomůže ani diagnostika příkazem ping, protože ten normálně funguje a tak musí nastoupit zkušený správce sítě, který umí spojení diagnostikovat.

Příkaz ping také nepomůže v případě, kdy se změní IP adresy tak, že IP adresu původního docházkového serveru dostane jiné zařízení. Ping normálně odpovídá, ale ve skutečnosti se nebaví s docházkovým serverem, což není na první pohled poznat. Může to při diagnostice vést ke špatným závěrům, čímž se nalezení závady komplikuje. Zde opět musí nastoupit správce sítě, který problém odhalí. Třeba tak, že hlavní PC docházky vypne, zkusí *ping* a už je jasné, že odpovídá něco jiného. Nebo u složitější síťové infrastruktury použije příkaz *tracert* pro sledování trasy paketů či jiné diagnostické síťové nástroje.

U složitější sítě, kde je např. více poboček spojeno přes VPN, může být problém také ve výpadku spojení mezi pobočkami (lze ověřit pingem či *tracert*). Ale místo VPN může být k propojení použito například *port-proxy*, *port-forwarding* a jiné technologie, které port 80 vstupního pobočkového routeru přesměrují na lokální docházkový server za routerem. Klienti z ostatních poboček pak do prohlížeče zadávají IP adresu routeru. Pokud se vypne hlavní PC docházky, nebo se na routeru změní pravidla, případně se změní IP adresa docházkového serveru bez zohlednění změny v pravidlech routeru, ping na router normálně funguje. Což může být opět matoucí a odhalí to až zkušený správce sítě, který její konfiguraci podrobně zná.

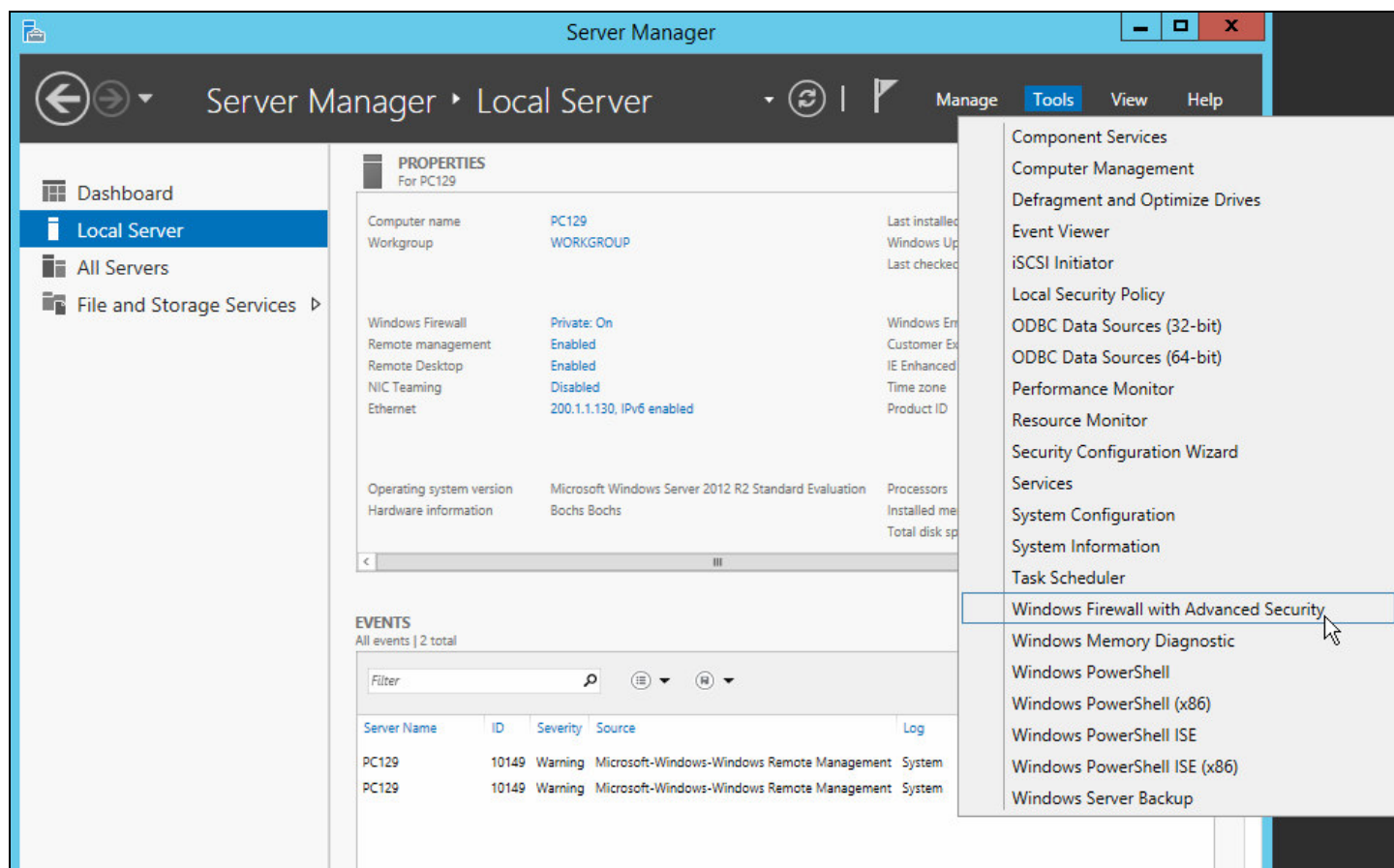
Podobných „zádrhelů“ může nastat celá řada. Proto pokud Vám na klientských PC přestane fungovat spojení do docházky, ale když si docházku pošlete přímo na jejím hlavním počítači a zde funguje, bude na čase kontaktovat správce vaší sítě, který zná podrobně její konfiguraci. Výrobce docházkového systému vám v tomto případě pomoci nedokáže, protože vaší síť a její konfiguraci prostě nemůže znát.

Podrobný postup pro Windows server 2012:

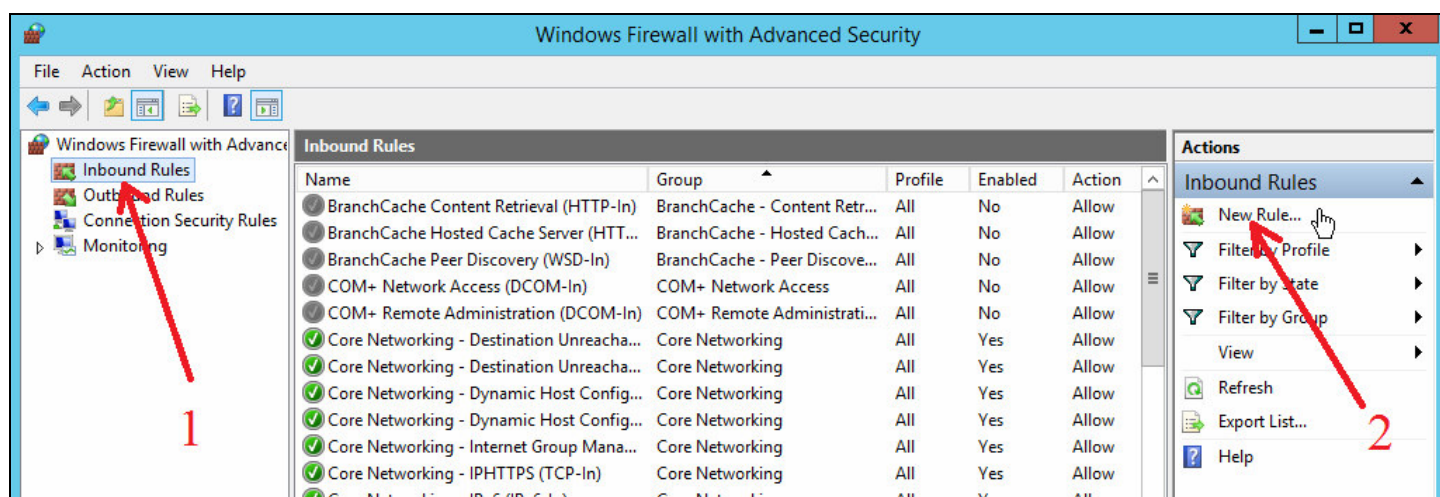
Nejprve na hlavním PC docházky odblokujeme port 80 ve firewallu a zjistíme IP adresu tohoto hlavního docházkového PC (docházkového serveru). Poté na druhém (klientském) počítači přes prohlížeč ověříme, že vše funguje a s docházkou pak lze podobně pracovat odkudkoli.

1. Odblokování firewallu na hlavní PC docházky:

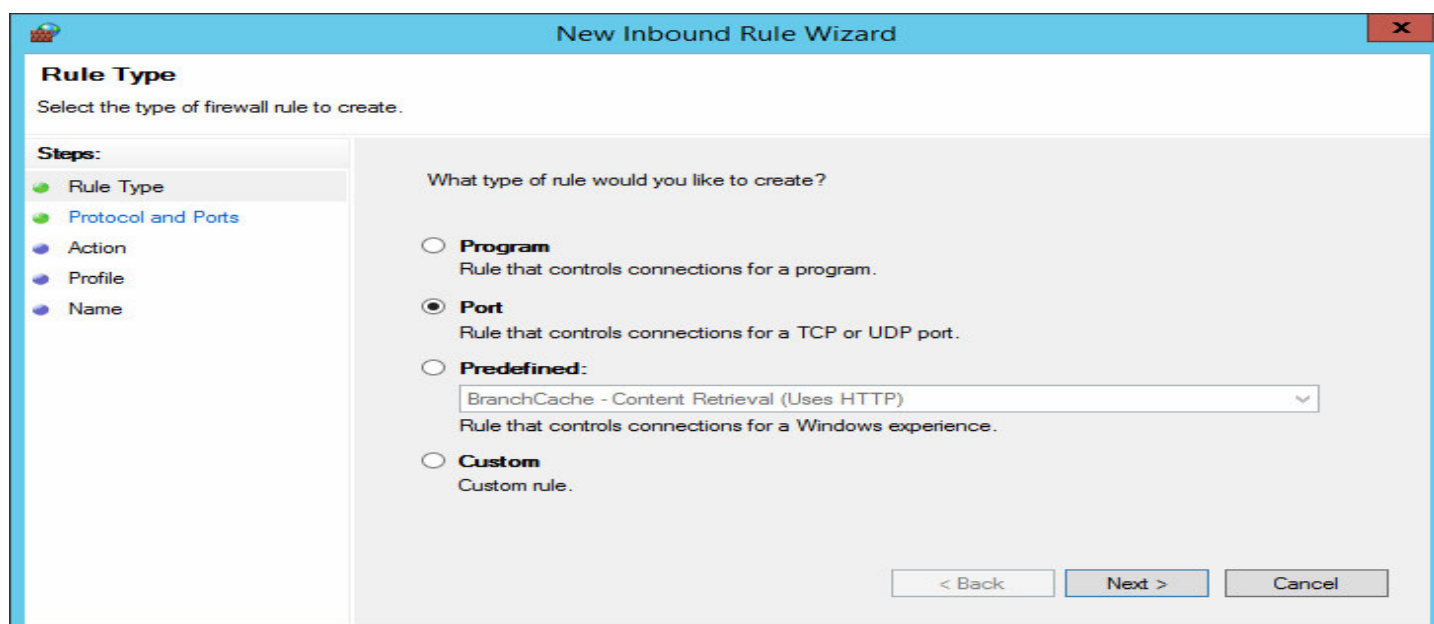
V „*server manageru*“ kliknete na nabídku nástrojů vpravo nahoře a ze seznamu vyberete položku „*Windows Firewall with Advanced Security*“



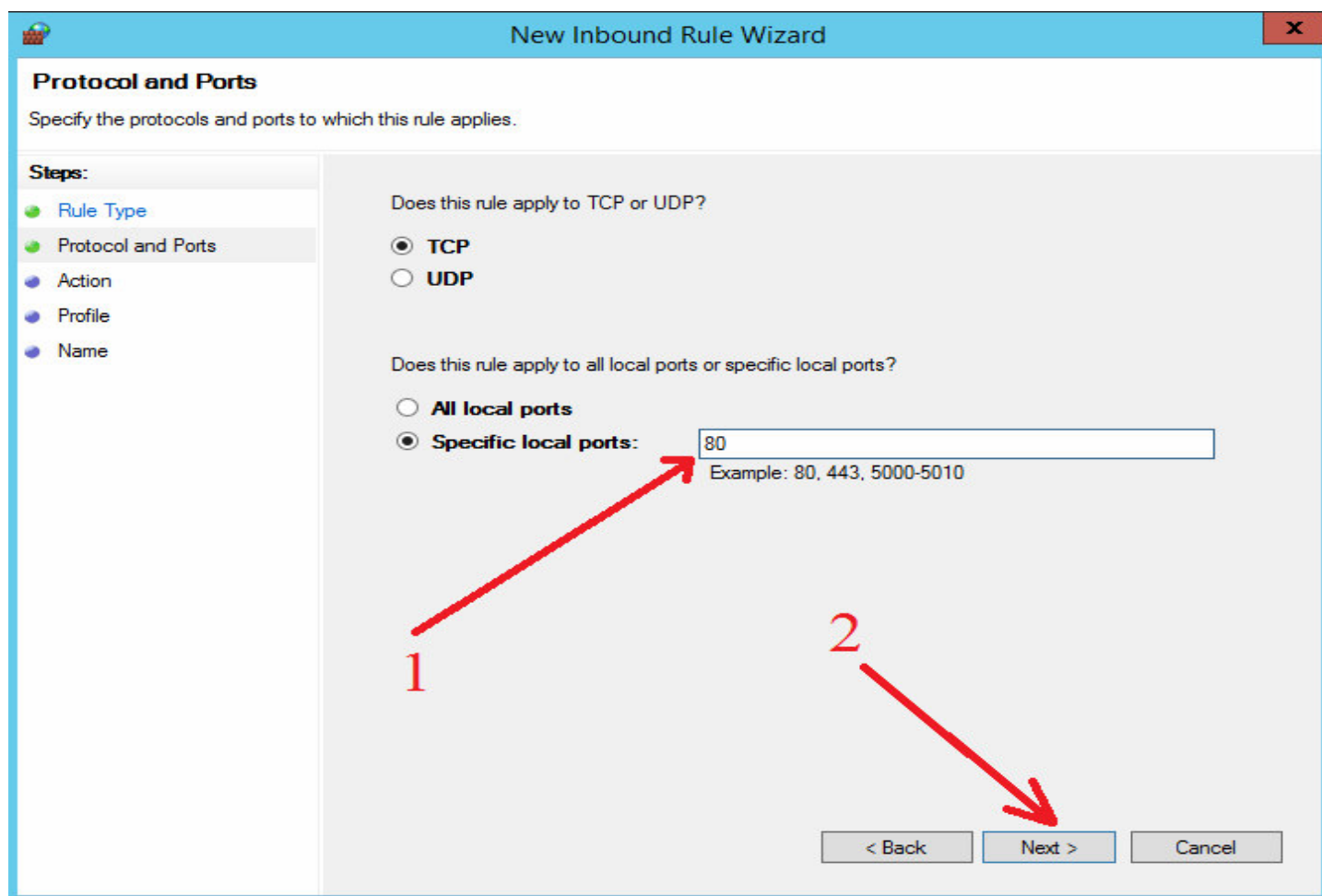
Otevře se okno nastavení firewallu, ve kterém kliknete vlevo nahoře na „*Příchozí pravidla*“ a poté vpravo nahoře na „*Nové pravidlo*“.



V průvodci vyberete typ pravidla *Port* a kliknete na *Další*



Protokol necháte vybraný *TCP* a zatrženou kolonku *Konkrétní místní porty*, do které dopíšete číslo 80. Pokud jste web server docházky Apache přeměrovaly na jiný port, dopíšete ten, který Apache používá. Ve výchozí instalaci se ale používá port 80, takže pokud jste nic neměnili, zapíšete osmdesátku. Pokud používáte šifrovaný https protokol, je třeba ve firewallu povolit i port 443. Nakonec kliknete na *Další*.



Ve volbě *Akce* ponecháte standardní *Povolit připojení* a kliknete na *Další*.

The screenshot shows the 'New Inbound Rule Wizard' dialog box at the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The main area asks 'What action should be taken when a connection matches the specified conditions?' and offers three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. A red arrow labeled '1' points to the 'Allow the connection' option. Another red arrow labeled '2' points to the 'Next >' button. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

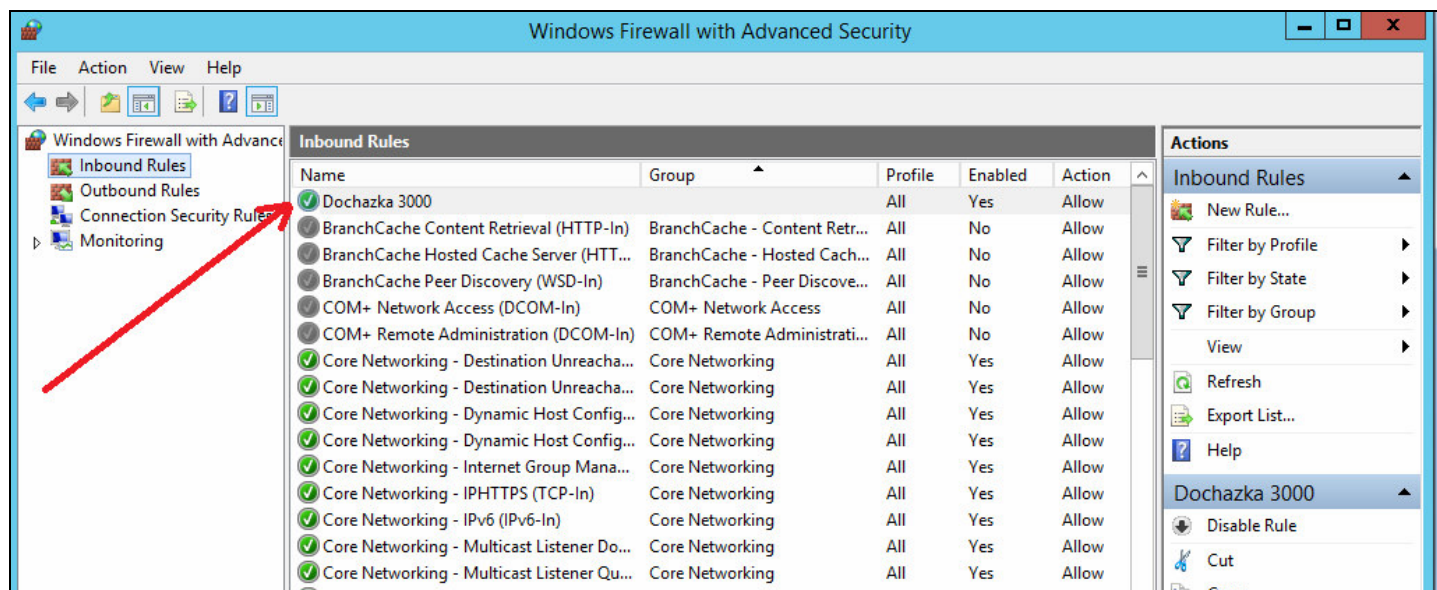
V profilu ponecháte zatrženy všechny volby a opět jen potvrdíte tlačítkem *Další*.

The screenshot shows the 'New Inbound Rule Wizard' dialog box at the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The main area asks 'When does this rule apply?' and offers three checked checkbox options: 'Domain', 'Private', and 'Public'. A red arrow points to the 'Next >' button. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

V posledním bodě průvodce zadáte pro toto nové pravidlo výstižný název, můžete uvést podrobný popis a nakonec kliknete na *Dokončit*.

The screenshot shows the 'New Inbound Rule Wizard' dialog box at the 'Name' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Name' with the instruction 'Specify the name and description of this rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The main area has two text input fields: 'Name:' with the value 'Dochazka 3000' and 'Description (optional):' with the value 'Pipojen do Dochzky 3000 z ostatnch PC'. At the bottom are buttons for '< Back', 'Finish', and 'Cancel'.

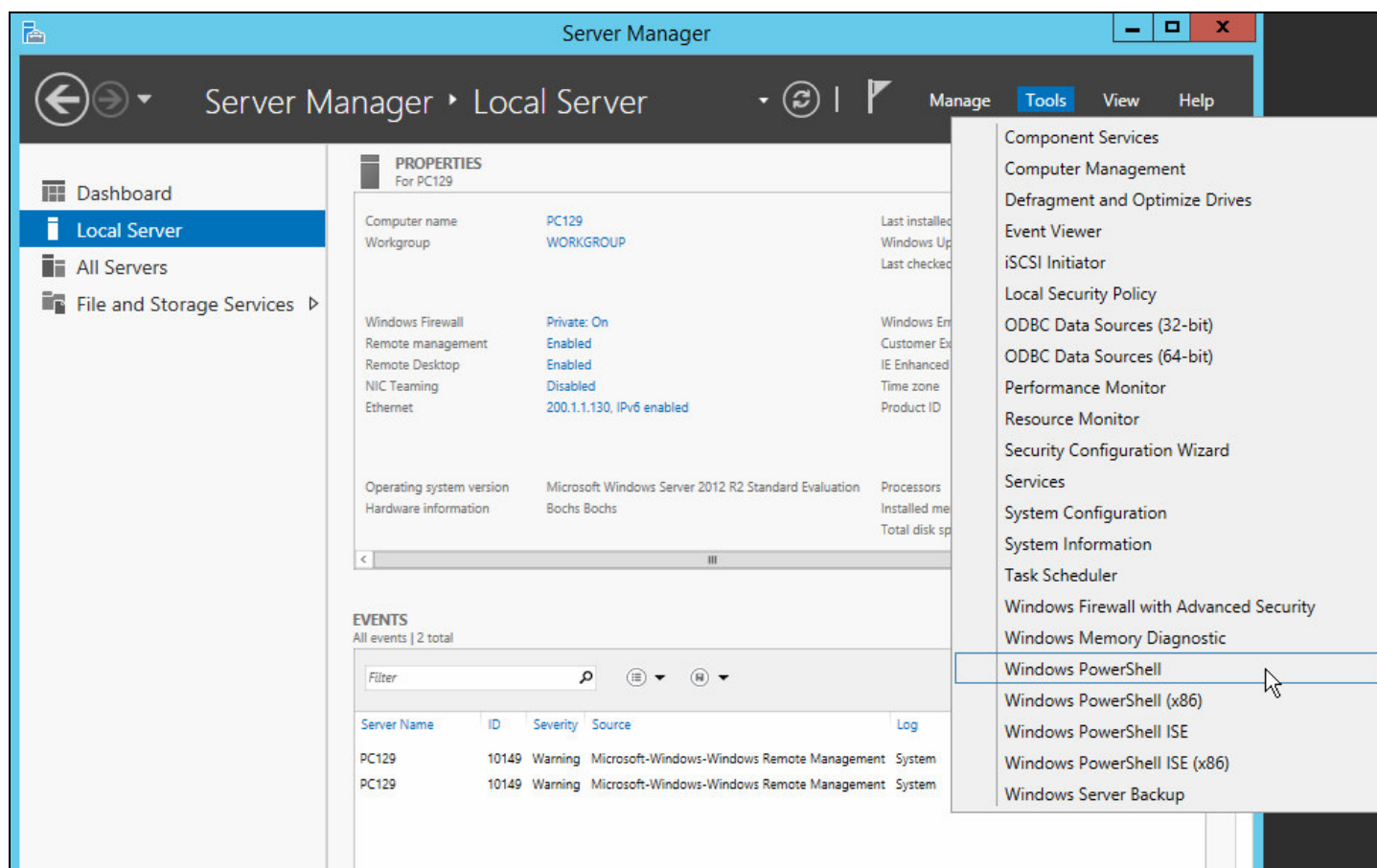
Tímto postupem jste tedy zajistili, že bude možné pracovat s docházkou z ostatních počítačů. Firewall již nebude ve spojení po síti bránit. Nové pravidlo se přidá mezi stávající platná pravidla. To, že pravidlo funguje a není zakázáno, poznáte podle zelené „fajky“ před jeho názvem.



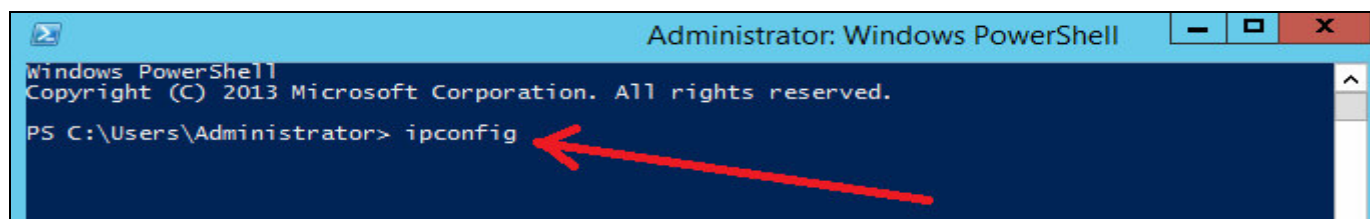
Tímto jsme nastavili firewall. Okno s nastavením firewallu již nebudeme potřebovat, takže jej můžete zavřít.

2. Zjištění IP adresy hlavního docházkového PC:

Dalším krokem je zjistit, jakou má tento hlavní počítač docházky IP adresu. Tu budeme používat pro spojení z ostatních počítačů. V *server manageru* rozkliknete nabídku nástrojů (*tools*) a vyberete položku *Windows PowerShell*



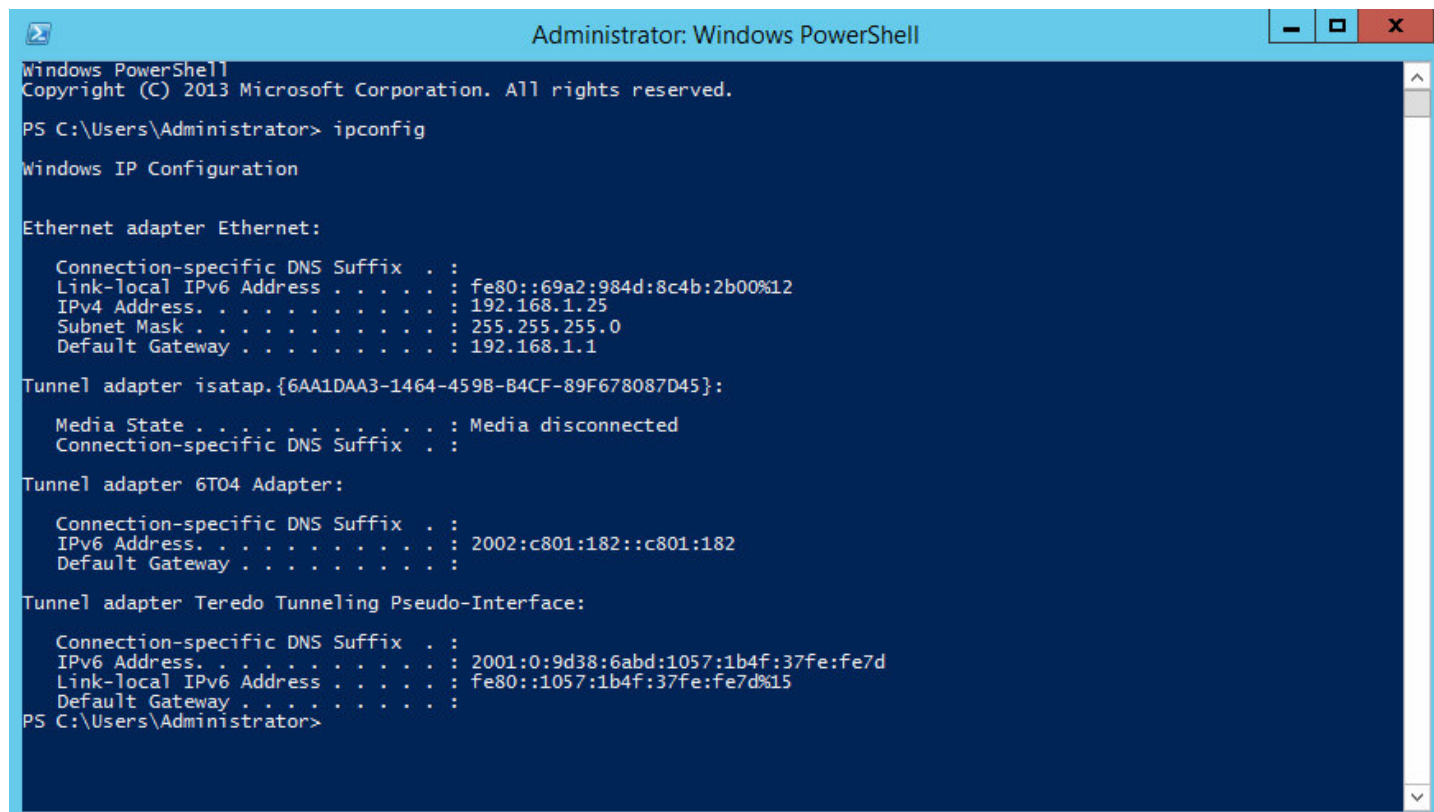
Otevře se modré okno příkazového řádku, do kterého zadáte příkaz *ipconfig*



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig
```

Poté dojde k vypísání parametrů nastavení počítačové sítě v tomto počítači.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::69a2:984d:8c4b:2b00%12
    IPv4 Address. . . . . : 192.168.1.25
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{6AA1DAA3-1464-459B-B4CF-89F678087D45}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter 6T04 Adapter:

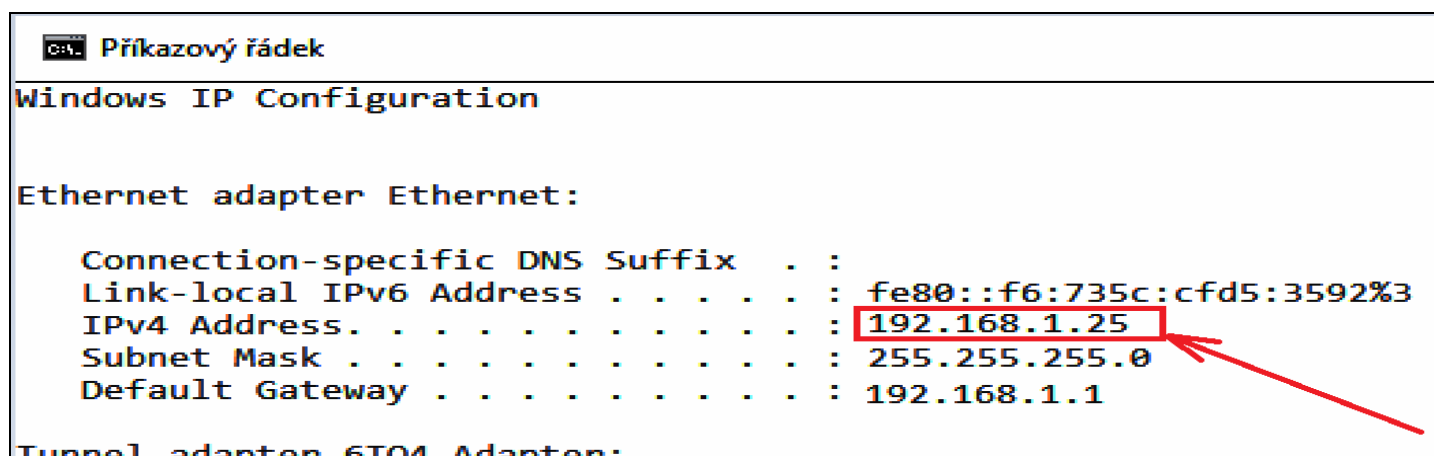
    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2002:c801:182::c801:182
    Default Gateway . . . . . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:9d38:6abd:1057:1b4f:37fe:fe7d
    Link-local IPv6 Address . . . . . : fe80::1057:1b4f:37fe:fe7d%15
    Default Gateway . . . . . : 

PS C:\Users\Administrator>
```

Budete hledat řádek s položkou „IPv4 Adresa“ nebo „IPv4 Address“. Bude to hned jeden z prvních řádků. Viz zvětšený výřez na barevně invertovaném obrázku níže.



```
Příkazový řádek
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f6:735c:cf5d:3592%3
    IPv4 Address. . . . . : 192.168.1.25
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter 6T04 Adapter:
```

Zde tedy vidíme, že náš hlavní počítač docházky, na kterém jsme příkaz zadali, má IP adresu 192.168.1.25
Váš počítač bude mít zřejmě IP adresu jinou, takže si jí někde poznamenejte.

Důležité je všechny výše uvedené kroky z bodů 1 i 2 spouštět opravdu přímo na hlavním PC docházky – docházkovém serveru. Tedy na tom PC, kam jste docházku instalovali z CD.

3. Ověření přístupu do docházky z ostatních PC:

Nyní tedy již máme nastaven hlavní počítač docházky tak, aby povolil síťová spojení do programu z ostatních počítačů a známe také IP adresu tohoto hlavního docházkového PC, na kterém docházka běží (web server, databáze atd.). Můžeme se tedy přesunout k jinému (klientskému) PC, které je zapojeno do stejné sítě LAN a ze kterého budeme chtít rovněž s docházkou pracovat.

Pokud v naší síti není nic dalšího, co by přenos mohlo blokovat (antivir, jiný firewall atd.), mělo by být možné na tomto klientském počítači spustit prohlížeč, zadat do něj IP adresu docházkového serveru zjištěnou výše v bodě 2 a po „odentrování“ by se měla docházka zobrazit.

Název firmy	ID firmy	Datum založení	Verze DB	Pracovníků	Přihlášení
Moje firma	1	10.03.2011	7.11	650	61997 (05.05.2016)

Adresu je třeba zadat do adresního řádku. Nikoli do řádku pro vyhledávání nebo jiného místa. Pokud vše funguje, uložte stránku do záložek, nebo jí nastavte v prohlížeči jako výchozí. Pak nebude třeba pokaždé psát adresu ručně. Lze vytvořit i zástupce na plochu tak, že do cíle zadáte např. `http://192.168.1.25/dochazka2001/` čímž se vytvoří zástupce přímo na ploše pro pohodlné spuštění docházky jedním dvojklikem myši.

Mělo by stačit zadat jen samotnou IP adresu docházkového serveru. Tedy v našem příkladě `192.168.1.25` a zmáčknout klávesu *Enter*. Pouze pokud jste náhodou webovou složku docházky přejmenovali, musíte zadat i jméno složky za adresou (např. `http://192.168.1.25/mojeslozka/`).

Pokud jste Apache web server docházky přesměroval na jiný port než 80, je třeba tento port uvést jak v kroku 1 tohoto návodu (nastavení firewallu), tak pak i zde v prohlížeči na klientském PC. například pokud jste pro apache web server docházky použili port 8080, zadáte na klientském PC adresu např. `192.168.1.25:8080`

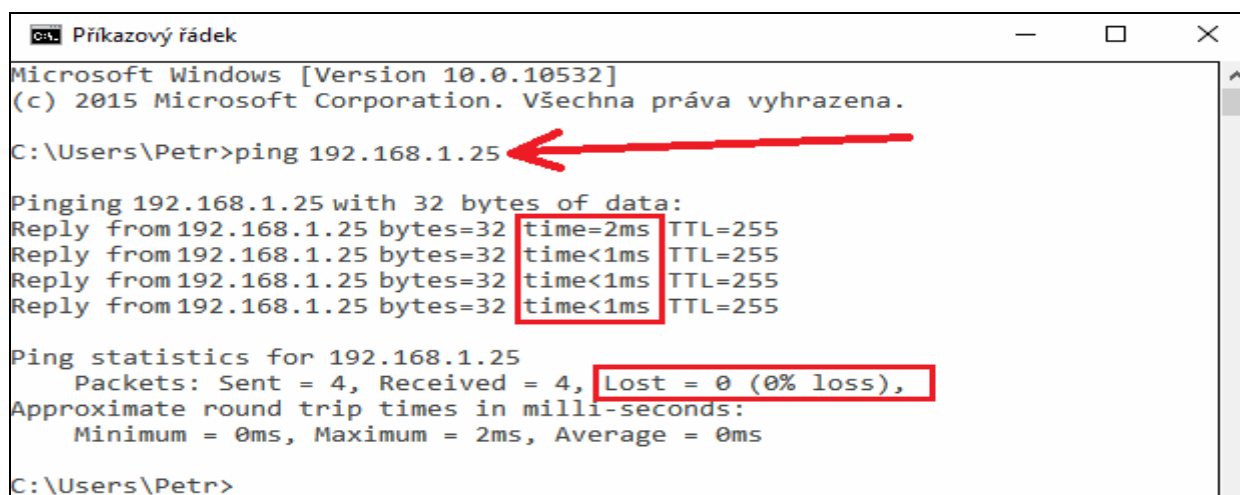
4. Řešení problémů:

Pokud časem přestane připojení do docházky z jiných PC fungovat, ale na samotném hlavním PC docházka funguje normálně, mohlo dojít k různým změnám ve vaší síti.

Například kolize IP adres, kdy nějaké jiné zařízení (počítač, tiskárna, tablet ...) dostane stejnou adresu jako hlavní docházkový server. Což se může stát při statickém přidělení IP adresy.

Závada na ethernetovém kabelu, v portu switchu, vytažený kabel v rozvaděči a podobně. Lze ověřit například příkazem *ping* spuštěným v příkazovém řádku na klientském PC.

Ověření spojení příkazem ping spuštěným na klientském PC ukazuje následující obrázek



```
cmd.exe Příkazový řádek
Microsoft Windows [Version 10.0.10532]
(c) 2015 Microsoft Corporation. Všechna práva vyhrazena.

C:\Users\Petr>ping 192.168.1.25

Pinging 192.168.1.25 with 32 bytes of data:
Reply from 192.168.1.25 bytes=32 time=2ms TTL=255
Reply from 192.168.1.25 bytes=32 time<1ms TTL=255
Reply from 192.168.1.25 bytes=32 time<1ms TTL=255
Reply from 192.168.1.25 bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.25
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Petr>
```

Docházkový server v pořádku odpovídá, časy odpovědí jsou běžné pro lokální síť a žádné pakety se po cestě neztratily. Pokud se místo časů odpovědí vypíše chybové hlášky (např. *Destination port unreachable*), je třeba hledat chybu a kontaktovat správce sítě.

Také je možné, že se změnila IP adresa hlavního PC docházky. Například pokud se IP adresy přidělují dynamicky pomocí DHCP, je třeba buď znovu projít body 2 a 3 výše uvedeného návodu, nebo IP adresu docházkovému serveru přidělit staticky (a z dhcp rozsahu jí výjmout), nebo místo IP adresy používat doménové jméno hlavního docházkového PC.

Síťové spojení může také blokovat antivir nebo jiný firewall než standardní z windows (např. *Kerio* a podobné) nainstalované jak na hlavním PC docházky, tak také i na klientském PC. I pokud docházka nějakou dobu normálně funguje a poté se jakoby z ničeho nic přestane u klientů připojení dařit, může to být antivirem nebo firewallem, který se automaticky zaktualizoval a najednou začne připojení blokovat. Takové „závady“ se samozřejmě obtížně hledají a u uživatelů vyvstávají otázky typu „*Proč to nejednou nefunguje? Ještě nedávno to šlo, teď to nejde a já jsem mezi tím nic určitě neměnil.*“, V tomto případě nepomůže ani diagnóza příkazem ping, protože ten normálně funguje a tak musí nastoupit zkušený správce sítě, který umí spojení diagnostikovat.

Příkaz ping také nepomůže v případě, kdy se změní IP adresy tak, že IP adresu původního docházkového serveru dostane jiné zařízení. Ping normálně odpovídá, ale ve skutečnosti se nebaví s docházkovým serverem, což není na první pohled poznat. Může to při diagnóze vést ke špatným závěrům, čímž se nalezení závady komplikuje. Zde opět musí nastoupit správce sítě, který problém odhalí. Třeba tak, že hlavní PC docházky vypne, zkusí *ping* a už je jasné, že odpovídá něco jiného. Nebo u složitější síťové infrastruktury použije příkaz *tracert* pro sledování trasy paketů či jiné diagnostické síťové nástroje.

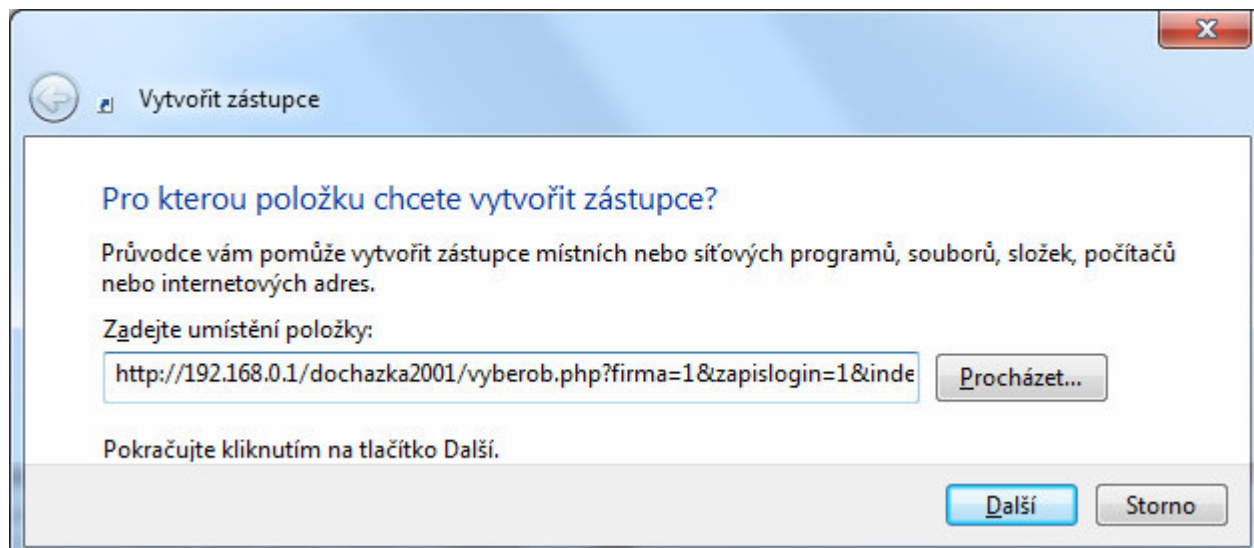
U složitější sítě, kde je např. více poboček spojeno přes VPN, může být problém také ve výpadku spojení mezi pobočkami (lze ověřit pingem či *tracert*). Ale místo VPN může být k propojení použito například *port-proxy*, *port-forwarding* a jiné technologie, které port 80 vstupního pobočkového routeru přesměrují na lokální docházkový server za routerem. Klienti z ostatních poboček pak do prohlížeče zadávají IP adresu routeru. Pokud se vypne hlavní PC docházky, nebo se na routeru změní pravidla, případně se změní IP adresa docházkového serveru bez zohlednění změny v pravidlech routeru, ping na router normálně funguje. Což může být opět matoucí a odhalí to až zkušený správce sítě, který její konfiguraci podrobně zná.

Podobných „zádrhelů“ může nastat celá řada. Proto pokud Vám na klientských PC přestane fungovat spojení do docházky, ale když si docházku pošlete přímo na jejím hlavním počítači a zde funguje, bude na čase kontaktovat správce vaší sítě, který zná podrobně její konfiguraci. Výrobce docházkového systému vám v tomto případě pomoci nedokáže, protože vaší síť a její konfiguraci prostě nemůže znát.

Pokud chcete zajistit zaměstnancům co nejrychlejší a nejpohodlnější přístup do SW docházky do uživatelského menu, je zde možnost vytvořit na ploše ikonu odkazující na docházku obsahující v parametrech údaje pro přihlášení. Takže pak pracovník na ikonu jen klikne a naskočí mu již přihlášená docházka.

Při vytváření odkazu na ploše Windows přes pravé tlačítko myši a volby "Nový / Zástupce" se do pole "Zadejte umístění položky" vloží webový http odkaz na docházku. Například takto:

http://192.168.0.1/dochazka2001/vyberob.php?firma=1&zapislogin=1&indexza=6&heslo=mojeheslo



Místo IP adresy *192.168.0.1* zadejte IP adresu či DNS název vašeho PC s docházkou.

Položku *indexza* nastavíte na osobní číslo (index) tohoto pracovníka pod kterým je zadáný v docházce.

A položku *heslo* nastavíte na heslo které zaměstnanec při přihlášení do docházky používá.

Následně kliknete na *Další* a název zadáte například *Docházka* a nakonec kliknete na *Dokončit*.

Poslední parametr odkazu (heslo) je ale zároveň velice slabým místem tohoto postupu, protože heslo do docházky se zde uvádí v čitelné textové podobě a může je tak snadno zjistit kdokoli, kdo se dostane k PC tohoto zaměstnance. Což je hlavní důvod, proč se tento postup nedoporučuje a není ani v souladu s ochranou dat a GDPR i když je s ním pro zaměstnance přihlášení do programu pohodlné.

Pokud tedy chcete tuto metodu použít, doporučuje se aby uživatelé používali do docházky jiná hesla než mají do jiných systémů, aby případné zjištění hesla do docházky neoprávněnou osobou neohrozilo přístup jinam, například do windows, e-mailu atd.

Navíc lze v docházce nastavit povolenou IP adresu ze které se může zaměstnanec přihlašovat, takže pokud používáte statické přidělování IP adres počítačům nebo v DHCP serveru vázané na MAC adresu, nelze se přihlásit z jiného PC než z toho, které zaměstnanci patří, takže samotné zjištění hesla neoprávněnou osobou jí ještě nestačí k tomu, aby se do docházky na někoho cizího přihlásila, musela by mít přístup ještě i k jeho PC a znát tedy přihlášení do windows, kde se ale pro zvýšení zabezpečení doporučuje mít jiná hesla než do docházky, takže zjištění hesla do docházky pak pro přihlášení nestačí. A v docházce lze v menu *Historie logování* dohledat případné neplatné pokusy o přihlášení, takže lze pokus o přihlášení neoprávněnou osobou snadno odhalit. Přehled logování vidí i samotný pracovník ve svém uživatelském menu, takže i on sám může snadno zjistit že se pod jeho účtem snažil přihlásit někdo jiný, kdy se tak dělo a z jakého PC (podle IP adresy uvedené v historii logování).

Postup zároveň funguje jen tehdy, když je v administraci v nastavení firmy prázdná položka pro *Standardní heslo*.

Další možnosti například pro integraci do intranetu nebo pro ikonu s přihlášením bez hesla najdete v příručce *integrace_dochazky.pdf*

Ochrana osobních údajů – soulad s GDPR

Program od verze 7.60 poskytuje moduly a funkce pro zajištění souladu s obecným nařízením o ochraně osobních údajů (dále GDPR). To se týká i vhodnosti šifrování datových přenosů mezi klientským počítačem a docházkovým serverem. Všechny potřebné informace k souladu s GDPR naleznete v docházce v menu *Zaměstnanci / Nařízení GDPR / Dokumentace*.

Pro zajištění šifrovaného datového přenosu mezi hlavním PC docházky a klientským počítačem využijete zejména návod na CD ve složce *\Prirucky* v souboru *Sifrovane_spojeni_https.pdf*. V nastavení firewallu dle postupu na předchozích stranách je pak potřeba povolit port 443, přes který se přenáší šifrované spojení mezi klientskými počítači a hlavní PC docházky (serverem docházky). Pokud s hlavním PC docházky nekomunikují ovladače (d2001.exe) starších identifikačních systémů BM-Term, BM-Scan, BM-RJ02 a stravovacího systému, které běží na jiných PC než samotném serveru a neumí komunikovat šifrovaně, a zároveň nepoužíváte aplikační rozhraní WebAPI docházky pro externí aplikace běžící na jiných počítačích, je možné povolit ve firewallu jen port 443 a port 80 zakázat, čímž nešifrovaný přenos úplně znemožníte a uživatele tím donutíte používat šifrované spojení vždy.

A screenshot of the Windows Firewall rule configuration window titled "Průvodce vytvořením nového příchozího pravidla". The window is on the "Protokol a porty" step. The "Typ pravidla" is set to "Příchozí". The "Protokol" is set to "TCP". The "Porty" are set to "Konkrétní místní porty" with the value "443" entered in the text box. A red arrow points to the "443" text box. The "Příklad" below shows "80, 443, 5000-5010". The "Zpět" and "Další" buttons are visible at the bottom.

Uživatelé pak budou na docházkový server přistupovat šifrovaným protokolem *HTTPS*. Je tedy třeba upravit odkazy v ikonách či oblíbených položkách tak, aby byl šifrovaný protokol skutečně použit, což je popsáno ve výše uvedené příručce *Sifrovane_spojeni_https.pdf*. Na přihlašovací obrazovce docházky se pak bude vedle hesla zobrazovat ikona zeleného zámečku, stejně jako v adresním řádku prohlížeče:

A screenshot of the web application "Dochazka 3000" in a browser. The address bar shows "https://192.168.1.100/dochazka2001/" with a green lock icon. The page header includes "Dochazka 3000 verze 7.60 MySQL Autor: BM Software" and buttons for "Tablet", "Mobil", and "Watch". The main content area displays "Výrobce: BM-Software, 69107 Němčičky 84, Česká republika" and a table with columns: "Název firmy", "ID firmy", "Datum založení", "Verze DB", "Pracovníků", and "Přihlášení". The right sidebar contains a login form titled "Přihlášení do systému." with fields for "Firma" (Agrostar), "Heslo", and a "Přihlásit" button. A red arrow points to the green lock icon in the address bar, and another red arrow points to the green lock icon next to the password field in the login form.

Informace k licenci Windows:

informace k výběru verze operačního systému pro hlavní PC docházky

Síťový přístup více uživatelů není z pohledu programu Docházka 3000 nijak omezen a programu je jedno, jestli s ním pracuje jediný uživatel přímo z hlavního PC docházky nebo jestli do něj přistupují současně desítky či stovky pracovníků přes webové rozhraní. Licence docházky počty síťových přístupů nijak neomezuje.

Ovšem zásadní rozdíl je to z pohledu licence operačního systému Windows. Pokud máte docházku nainstalovanou na hlavním PC (docházkovém serveru) s desktopovou edicí operačního systému (např. Windows XP, Vista, 7, 8 či Windows 10) ať již ve verzi Home nebo Profesional, není tento operační systém z licenčních podmínek firmy Microsoft určen k použití jako server. Používat desktopové verze Windows k serverovým účelům je Microsoftem obecně zakázáno. Licence určují několik výjimek – lze využívat například sdílení souborů a tiskáren nebo IIS, a to do určeného počtu připojených zařízení (počítačů, telefonů...).

Jak je uvedeno výše, není problém nainstalovat Docházku 3000 na hlavní PC s desktopovou verzí operačního systému Windows, pokud bude s programem pracovat jediný uživatel přímo z tohoto PC nebo po síti. Pro více uživatelů pracujících s docházkou současně je třeba nainstalovat program na serverovou verzí operačního systému Windows Server (2003, 2008, 2012, 2016 nebo 2019), kdy alespoň dle informací od Microsoftu není nutné pro webové přístupy pořizovat klientské licence (CAL). Nebo místo webového serveru Apache použít desktopovou licenci povolený webový server IIS (viz návod *Zmena_web_serveru_na_IIS* na instalačním CD docházky ve složce *Prirucky* a v něm část pro Windows 7 a 10), pokud vám stačí omezený počet síťových připojení daný konkrétní verzí desktopového operačního systému (5, 10 nebo 20 dle verze OS).

Protože je problematika licencování OS Windows pro síťové přístupy někdy složitější, je vhodné konzultovat výběr verze a licence operačního systému Windows přímo s výrobcem, pokud má s programem zároveň po síti pracovat větší počet uživatelů. Vyhněte se tak buď porušení licence operačního systému, nebo naopak zbytečně drahého nákupu nepotřebných klientských licencí pro serverové verze Windows.

~~Další možností je instalace docházkového systému na operační systém Linux, kde není licenční omezení na síťové přístupy a to, jestli bude s programem pracovat jen jeden uživatel nebo současně stovky uživatelů, nestojí z pohledu licence operačního systému žádné finanční prostředky. Postup instalace programu na Linux je popsán na instalačním CD docházky ve složce *Linux*.~~

Pokud potřebujete docházku provozovat síťově s přístupem mnoha uživatelů ze svých PC a nemáte ve firmě Windows Server ani jej nechcete pořizovat a nejste si jisti možností použití desktopové verze operačního systému Windows pro toto defakto serverové použití, lze docházku provozovat na cloudovém serveru výrobce. Viz informace na webu <https://www.dochazka.eu/cloud/>