

Fiddler

Ing. Ondřej Ševeček | GOPAS a.s.

MCSM:Directory | MVP:Security | CISA | CISM | CEH | CHFI | CISSP

ondrej@sevecek.com | www.sevecek.com

relevantní kurzy:

GOC166 (ADFS), GOC168 (IIS), GOC169 (ISO 2700x)

14. - 17. května 2018

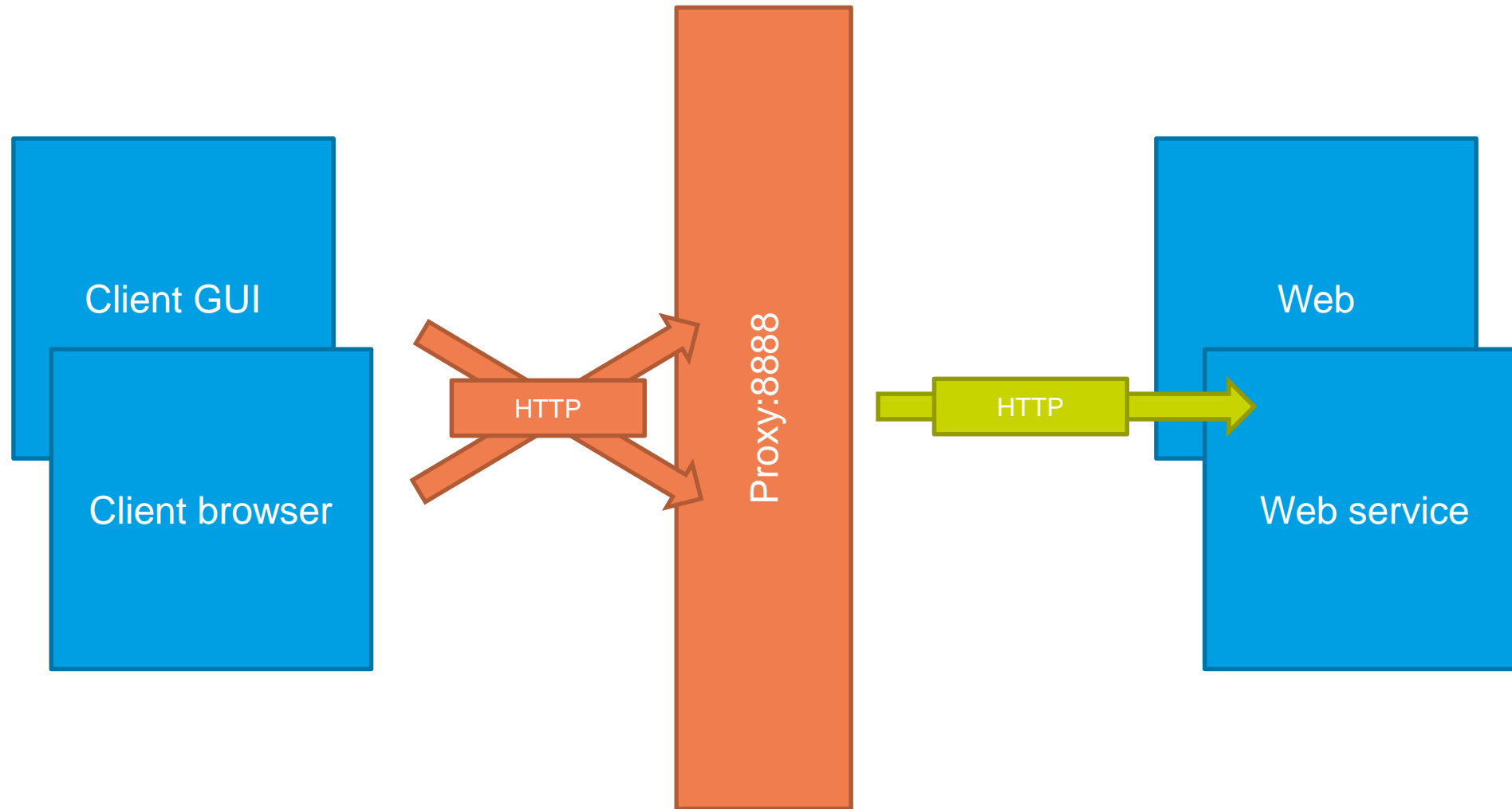
Tech·Ed
DevCon 

PRAHA 2018

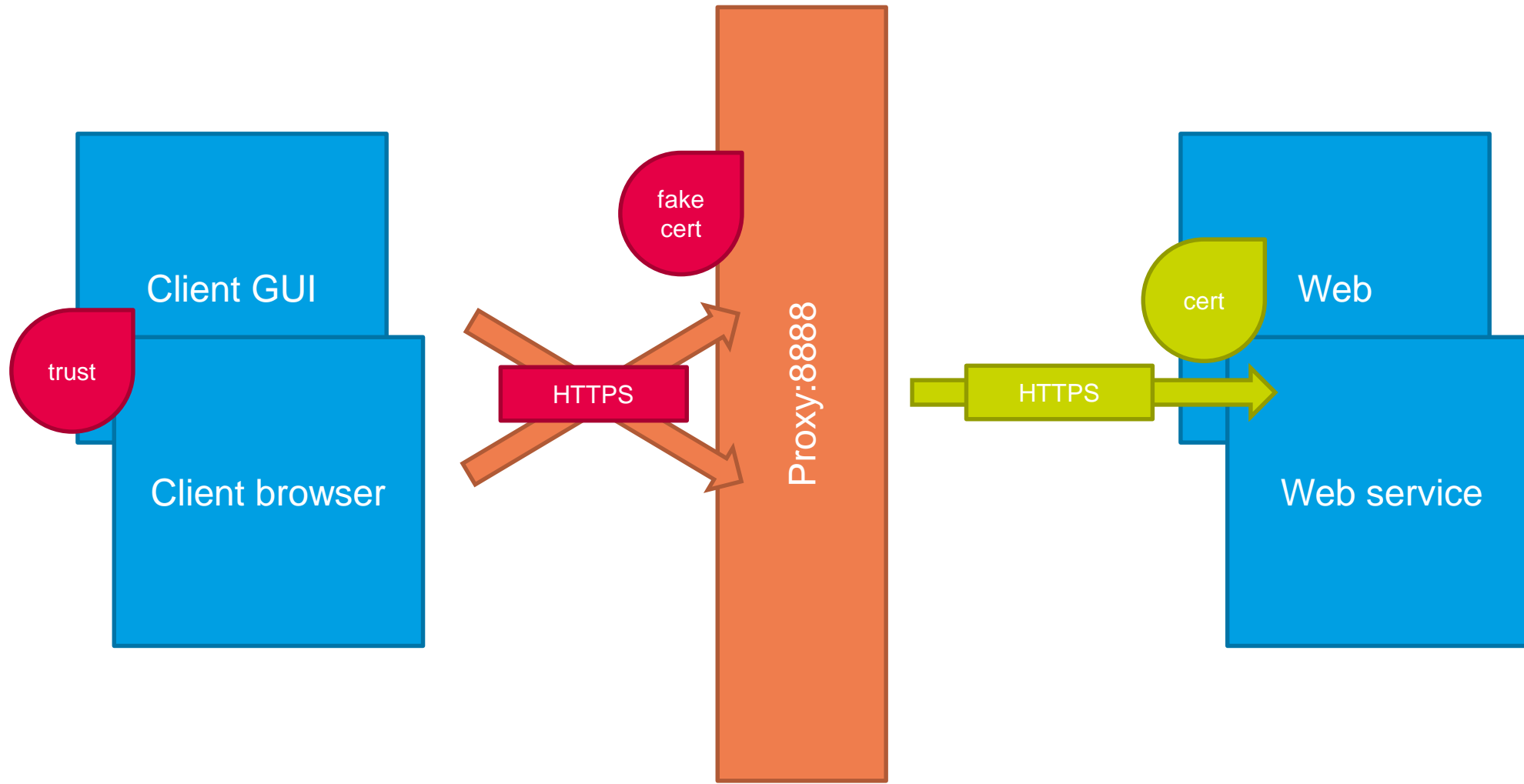
Motivation

- Browsers
 - IE, Edge, Chrome, ...
- Non-browser clients
 - winhttp, Java, ...
 - Outlook, Word, Excel, web service clients, ...
- User accounts
 - my own user, SYSTEM, Network Service, Local Service, ...

HTTP web proxy



SSL proxy



Local debugging

Fiddler

Change proxy settings to all protocols

The screenshot shows the 'Internet Properties' dialog box with the 'Connections' tab selected. The 'Local Area Network (LAN) settings' section is highlighted with a red dashed box. The 'LAN settings' button is also highlighted with a red dashed box. The 'Local Area Network (LAN) Settings' dialog box is open, showing the 'Proxy server' section. The 'Use a proxy server for your LAN' checkbox is checked, and the 'Advanced' button is highlighted with a red dashed box. The 'Advanced' dialog box is also open, showing the 'Servers' section. The 'Use the same proxy server for all protocols' checkbox is checked and highlighted with a red dashed box. The 'Servers' table is as follows:

Type	Proxy address to use	Port
HTTP:	127.0.0.1	8888
Secure:	127.0.0.1	8888
FTP:	127.0.0.1	8888
Socks:		

The 'Exceptions' section is also visible, showing a list of addresses to bypass the proxy server, currently containing '<-loopback>'. The 'OK' button is highlighted with a blue border.

Configure old `winhttp` SYSTEM clients

- `netsh winhttp set proxy`

```
Administrator: C:\Windows\system32\cmd.exe
```

```
C:\>  
C:\>netsh winhttp set proxy fiddler:8888
```

```
Current WinHTTP proxy settings:
```

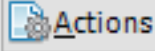
```
Proxy Server(s) : fiddler:8888  
Bypass List      : (none)
```

Enable SSL inspection


Options

General **HTTPS** Connections Gateway Appearance Scripting Extensions Performance Tools

Fiddler can decrypt HTTPS sessions by re-signing traffic using self-generated certificates.

Capture HTTPS CONNECTs 

Decrypt HTTPS traffic

... from all processes  Certificates generated by CertEnroll engine


Ignore server certificate errors (unsafe)

Check for certificate revocation


Protocols: <client>; ssl3;tls1.0

[Skip decryption](#) for the following hosts:

Help Note: Changes may not take effect until Fiddler is restarted.

Certificate 

General **Details** Certification Path

 **Certificate Information**

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- All issuance policies

Issued to: DO_NOT_TRUST_FiddlerRoot

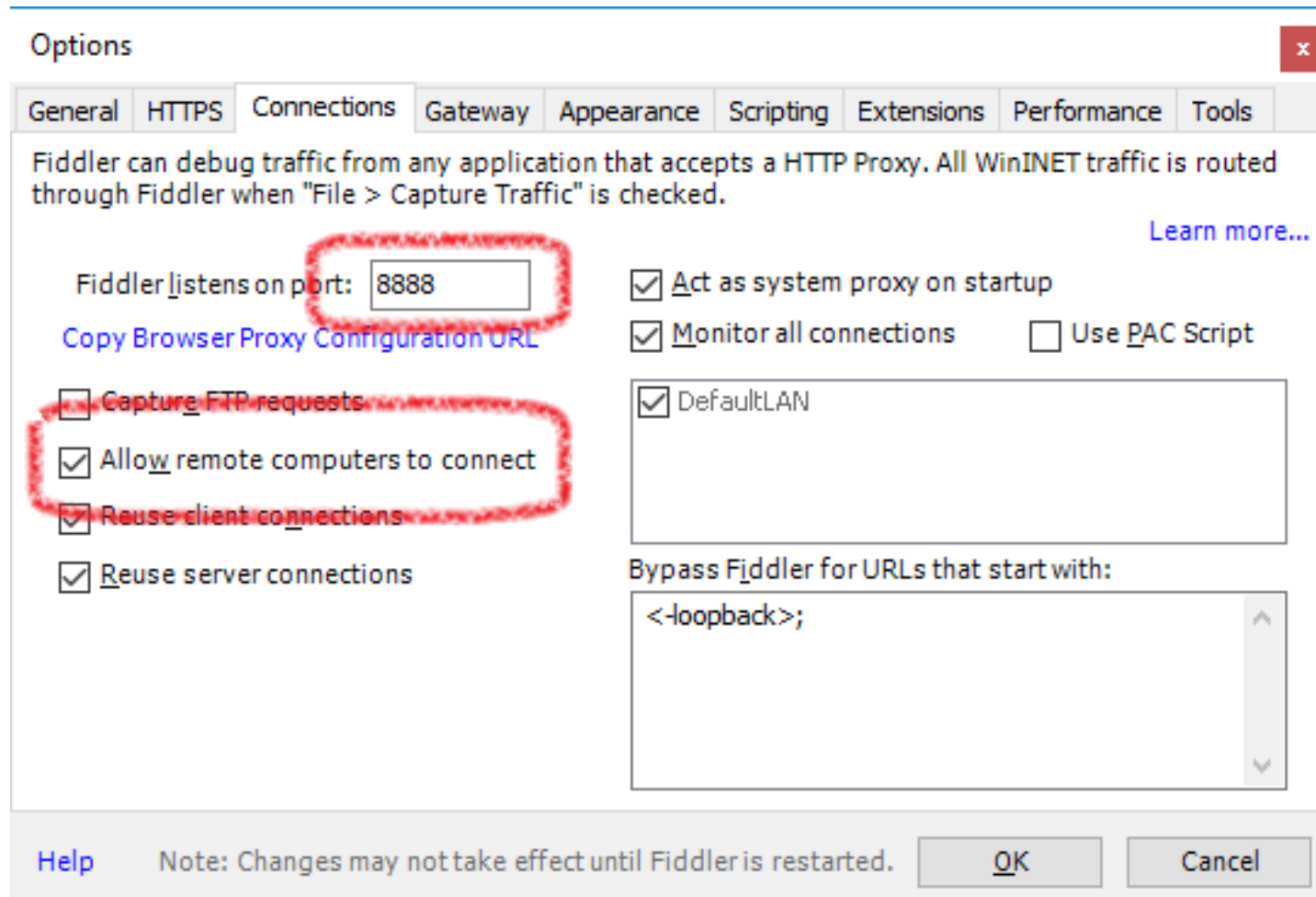
Issued by: DO_NOT_TRUST_FiddlerRoot

Valid from 13.05.2017 **to** 13.05.2023

Remote debugging is smoother

Fiddler

Enable remote proxy bindings



Verify remote proxy bindings

- must be 0.0.0.0:8888

```
Administrator: C:\Windows\system32\cmd.exe

C:\>
C:\>netstat -ano | findstr :8888
    TCP    0.0.0.0:8888      0.0.0.0:0        LISTENING       5016
    TCP    [::]:8888       [::]:0           LISTENING       5016

C:\>_
```

Windows Firewall with Advanced Security

File Action View Help

Windows Firewall with Advanced Security

Inbound Rules

Name	Program	Protocol	Local Port
FiddlerProxy	C:\Users\domain-admin\AppData\Local\Programs\Fiddler\Fiddler.exe	TCP	Any
Active Directory...	Any	ICMPv4	Any
Active Directory...	Any	ICMPv6	Any

Proxy servers for more accounts and services

```
$fdl = Read-Item 'Fiddler machine name'
```

```
Set-ItemProperty 'Microsoft.PowerShell.Core\Registry::HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings' ProxyServer "$($fdl):8888"
```

```
Set-ItemProperty ' Microsoft.PowerShell.Core\Registry:: HKEY_USERS\S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet Settings' ProxyServer "$($fdl):8888"
```

```
Set-ItemProperty ' Microsoft.PowerShell.Core\Registry:: HKEY_USERS\S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Internet Settings' ProxyServer "$($fdl):8888"
```

```
Set-ItemProperty ' Microsoft.PowerShell.Core\Registry::  
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings' ProxyServer  
"$($fdl):8888"
```

```
netsh winhttp set proxy "$($fdl):8888"
```

Testing non-browser clients

```
(New-Object Net.WebClient).DownloadString("https://www.google.com")
```

```
# Note: more examples at
```

```
# https://www.sevecek.com/Lists/Posts/Post.aspx?ID=289
```

Extended Protection for Authentication

Internet Information Services (IIS) Manager

WFE > Sites > portal

File View Help

Connections

- Start Page
- WFE (SVCK\sp-admin)
 - Application Pools
 - Sites
 - bi
 - eshop
 - finance
 - intranet
 - intranet.sevecek.eu
 - loans
 - orders
 - portal
 - SharePoint Central Ad
 - SharePoint Web Servic
 - transport
 - warehouse

Authentication

Group by: No Grouping

Name	Status	
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	
Digest Authentication	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

Advanced Settings

Extended Protection:
Required

[Click here for more information online](#)

Administrator: Windows PowerShell

```
PS C:\>  
PS C:\> Get-AdfsProperties | select Extended*  
  
ExtendedProtectionTokenCheck  
-----  
Require  
  
PS C:\>
```

Extended Protection on RD Gateway

- HKLM\System\CurrentControlSet\Control\LSA
 - SuppressExtendedProtection = DWORD = 3 (1 -bxor 2)

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\TerminalServerGateway\Config\Core
 - EnforceChannelBinding = DWORD = 0

Client certificate authentication

- Export .PFX with private key
- Export .CER without private key

- Import .PFX into current user profile
- Save .CER as Documents\Fiddler2\ClientCertificate.cer

Děkuji!

Ing. Ondřej Ševeček | GOPAS a.s.
ondrej@sevecek.com | www.sevecek.com

relevantní kurzy:

GOC166 (ADFS), GOC168 (IIS), GOC169 (ISO 2700x)

Aktuální a navazující kurzy sledujte na www.gopas.cz

DÁREK PRO VÁS!

Vyplňte dotazníkové hodnocení
a získejte tričko **TechEd-DevCon 2018!**



SOUTĚŽ! SOUTĚŽ! SOUTĚŽ!

Soutěžte o titul **TechEd Best Developer**
a **TechEd Best IT PRO!**

