

Ondřej Ševeček | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security |
ondrej@sevecek.com | www.sevecek.com |

THREAT MANAGEMENT GATEWAY 2010

Course

- Overview
- Planning and installation
- Networking
- Access Rules
- Publishing Rules
- Web Server Publishing Rules
- SSL and SSL Inspection
- Antimalware and intrusion prevention
- Remote Access, VPN
- Network Access Protection
- Advanced Concepts

Prerequisites

- Windows 2003/2008 server administration
- Active Directory
- TCP/IP and DNS

Administration

- Length
 - 5 days
- Lessons
 - 9:00 – 16:00
- Lunch
 - 12:00 – 13:00
- Refreshments, soft-drinks, smoking, ...

Environment

- AD domain: **gopas.virtual**
- Public DNS domain: **gopas.cz**
- Sites
 - Prague 10.10.X.X
 - Brno 10.20.X.X
 - DMZ 10.30.X.X
 - London 10.40.X.X
 - Paris 10.50.X.X
 - VPN 10.100.X.X

Lab


- On **R1** in **Routing and Remote Access** console open the **Network Address Translation** node and **remove** all **private** interfaces
 - leave there only the **public Classroom** interface
 - this operation is done to enable correct FTP operation on our virtual networks

Lab

- Start **DC1**, **FW1**, **Seven1**, **R1**, **R2**, **WEB-DMZ** and **WEB-EXT**
- On **FW1** try from command line
 - nslookup
 - server 81.0.0.177
 - www.google.com
- And **ping** its respective **IP** address

Lab

- On **DC1** open **DNS** console
- Go into DC1 DNS Server **properties**
- On the **Forwarders** tab configure
 - **81.0.0.177**
- Note: you do not have any firewall exceptions, so the setting will not work for some time until module 3



Ondřej Ševeček | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security |
ondrej@sevecek.com | www.sevecek.com |

THANK YOU