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

INSTALLATION

Threat Management Gateway 2010

INSTALLATION

Installation (firewall)

- Windows Server 2008 x64 SP2
  - Standard, Enterprise, Datacenter
- Windows Server 2008 R2 x64
  - Standard, Enterprise, Datacenter
- 2 GB RAM, 2x CPU
  - recommended 4 GB, 4x CPU
- 1x NIC, 2+ NIC for full functionality
- Pre-installs
  - AD LDS, NPS, RRAS, NLB, PowerShell

Installation

- Enterprise Management Server
  - Windows Server 2008 x64 SP2
    - Standard, Enterprise, Datacenter
  - Windows Server 2008 R2 x64
    - Standard, Enterprise, Datacenter
  - 1 GB RAM
- Management Console
  - Windows Vista+
  - 1 GB RAM

Demo: Hardware Requirements

- Hardware Recommendations for TMG

Management Console

- Uses RPC connection
  - authenticated (NTLM/Kerberos), signed, sealed
  - TCP 3847
    - not dynamic, without RPC Endpoint Mapper
    - System Rule 2, protocol MS Firewall Control
- Connects directly to Standard Edition server or EMS

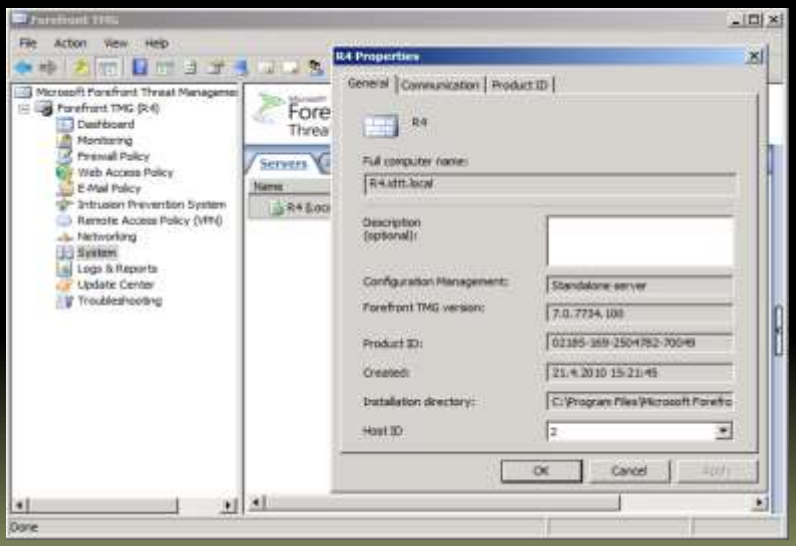
Virtual Environment

- Fully supported on SVVP Validated platforms
  - Microsoft Server Virtualization Validation Program
- Consider security

Video/Pictures

- TMG 2010 Installation

TMG version



ISA/TMG versions

Version	Release	Build number
2000	RTM SP1 FP1 SP2	3.0.1200.50 3.0.1200.166 3.0.1200.235 3.0.1200.365
2004	Beta RTM SP1 SP2 SP3	4.0.2161.153 4.0.2161.50 4.0.2163.213 4.0.2165.594 4.0.2167.887
2006	RTM SP1	5.0.5720.100 5.0.5723.493
2010	RC RTM SP1 SU1 for SP1 SU1 Rollup 1 for SP1 SU1 Rollup 2 for SP1 SU1 Rollup 3 for SP1 SP2 (requires SP1+SU1)	7.0.7733.100 7.0.7734.100 7.0.8108.200 7.0.9027.400 7.0.9027.410 7.0.9027.425 7.0.9027.441 7.0.9193.500

UAG versions

Version	Release	Build number	TMG version
2010	RTM Update 1 Update 2 SP1 SP1 Update 1	4.0.1101.0 4.0.1152.1 4.0.1269.200 4.0.1752.10000 4.0.1773.10100	RTM SU1 for SP1

Updates

- TMG RTM
- + SP1
- + Software Update1
  - + Rollup 1
  - + Rollup 2
  - + Rollup 3

Lab

- Install TMG on FW2
- Define internal IP range by selecting the London network adapter
- Close the Startup Wizard and close the TMG console

Google: Unsupported Configurations

- Installation on Windows Server Core
- Upgrade from Windows 2008 to 2008 R2 with TMG installed
- Installing TMG firewall services on Domain Controller
- Array members must be on the same OS
  - all Windows 2008 or all Windows 2008 R2
- Intradomain communications over NAT network relationship
- Unicode DNS
  - US-ASCII 7bit only
- NLB not supported with TMG Standard

Google: Unsupported Configurations

- L2TP outbound connections are not supported when TMG is configured as IPSec/L2TP endpoint
  - such as IPSec site-to-site tunnels or L2TP VPN Server
- No support for CNG certificates
- If Malware Inspection enabled on a rule, Content-Range header is stripped and not available
- FTP Upload not supported for FTP over HTTP
- Installation or use of routing protocols (OSPF, RIP etc.)
- IPv6 except for DirectAccess
- LDAP authentication supported only for Web Server Publishing rules

Threat Management Gateway 2010

UPGRADE

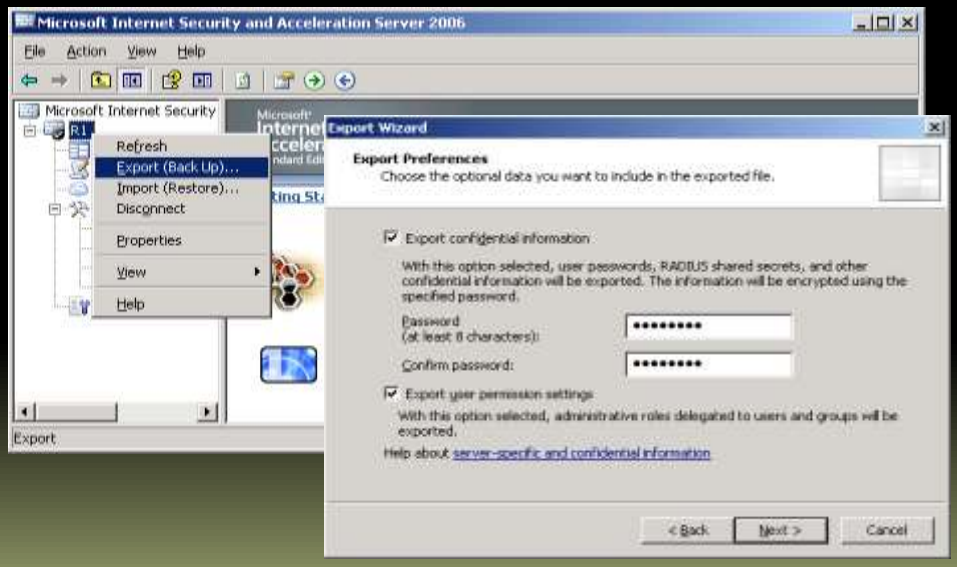
Upgrade = Migration

- ISA 2004/2006 needs Windows 2003 x32 only
  - cannot do cross-platform upgrade of OS
- Export/Import ISA 2004/2006 configuration
- Import must be done immediately after installation, yet before the Startup Wizard

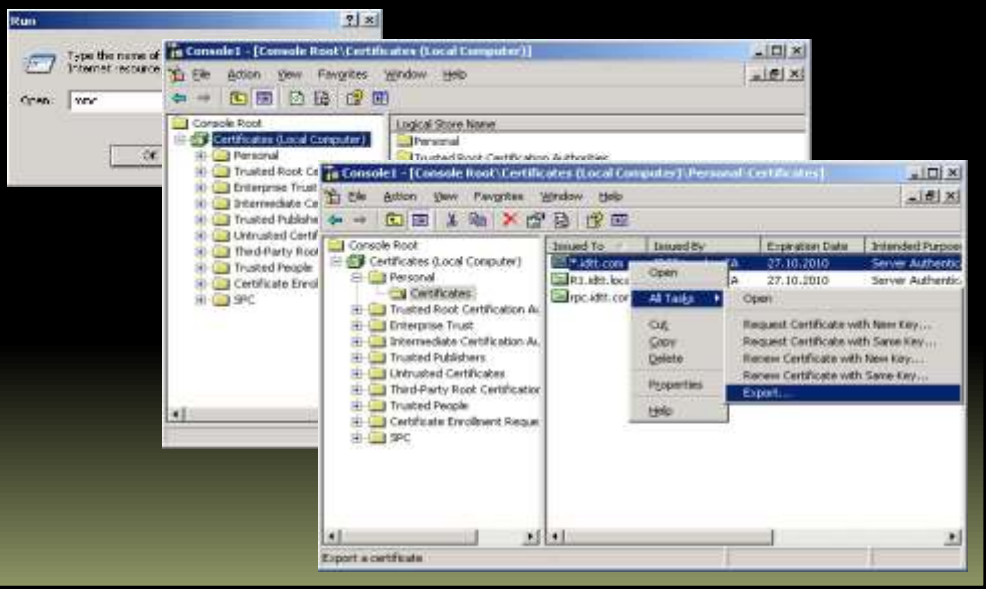
Upgrade procedure (All)

- Record old configuration
  - FQDN (name of the computer)
  - IP/DNS configuration
    - DNS Server hosted on ISA?
  - Static routes
    - route print, RRAS
- Export .XML configuration
  - plus private information
- Export server certificates
  - plus private keys

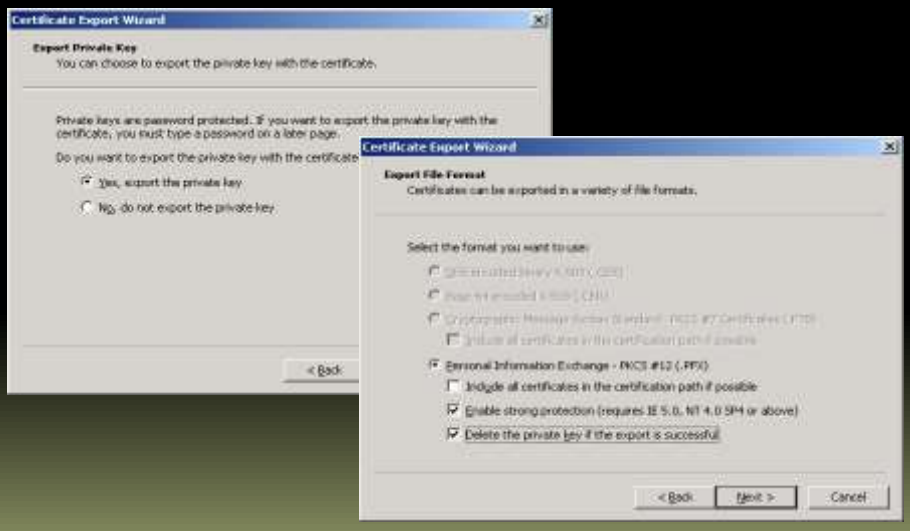
Exporting .XML configuration



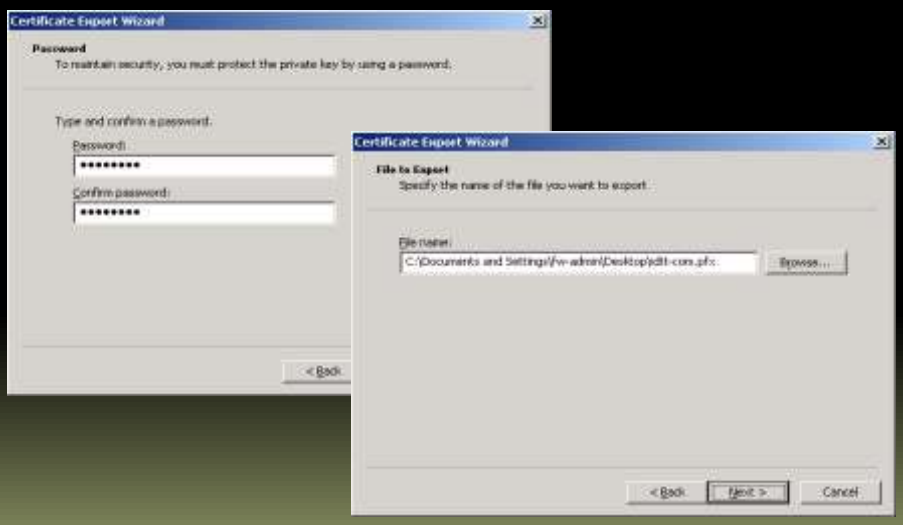
Exporting certificates



Exporting certificates



Exporting certificates



Upgrade procedure (Standard)

- Replace the server
  - re/install, join domain, rebuild IP/DNS config
- Import server certificates
- Install TMG
- Import .XML configuration

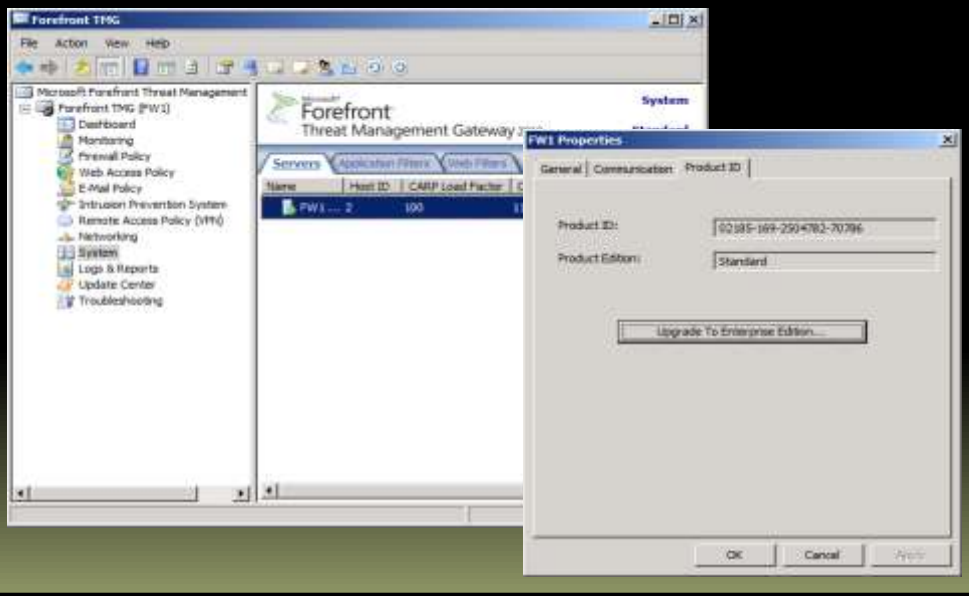
Upgrade procedure (Enterps.)

- Install new EMS server
- Import .XML configuration
- Replace the array members
  - re/install, join domain, rebuild IP/DNS config
- Import server certificates
  - into all future array members
- Install TMGs
  - specifying the EMS server

Upgrade from Std. to Ent.

- ISA 2006 must have been reinstalled
- TMG 2010 can be upgraded later
  - just buy the product code

Upgrade from Std. to Ent.



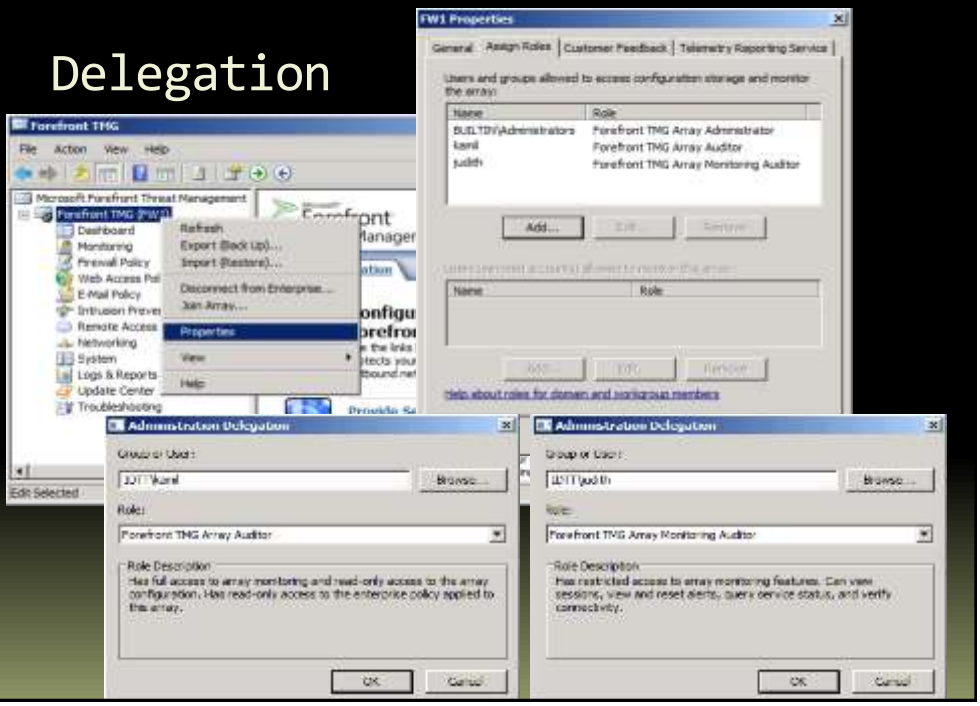
Upgrade from evaluation

- Evaluation expires in 120 days
- Run full-version installation setup
  - the setup finds the previous installation and upgrades automatically
- Settings are kept

Least privilege installation

- Local Administrators membership
- If firewall should be domain member
  - Add manually the computer account into RAS and IAS Servers group (requires Domain Admins)

Delegation



Lab

- Install Service Pack 1 on FW2
  - available at C:\Upload
- After the restart, shutdown the FW2 computer

Threat Management Gateway 2010

ENTERPRISE EDITION

Array authentication

- Either domain joined machines
  - using their own domain machine accounts
- Or workgroup (standalone) machines
  - using mirror account
  - just a local user with Administrators group membership
- Should require LDAP over SSL
  - server certificate on the Array Manager or EMS

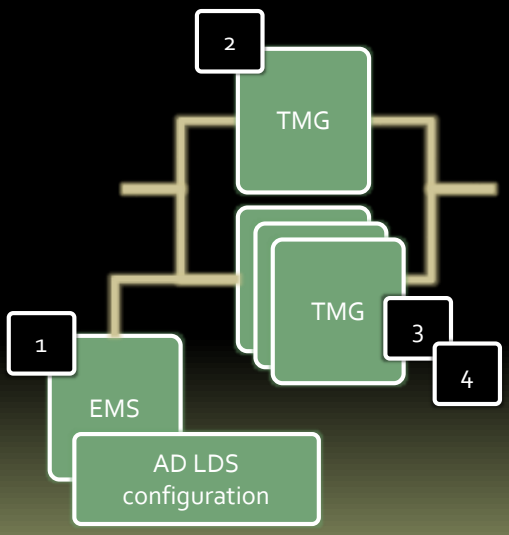
TMG Array types

- Standalone
  - one of the firewalls is Array Manager
  - stores the configuration while others replicate changes
- Enterprise
  - using designated Enterprise Management Server (EMS)

Enterprise Management Server

- Central configuration storage
  - AD LDS
  - ISASTGCTRL service (dsamain.exe)
- No firewall protection except for built/in Windows Firewall
- Cannot be installed on DC

Installing Enterprise Edition



Video/Pictures

- TMG 2010 Installing EMS

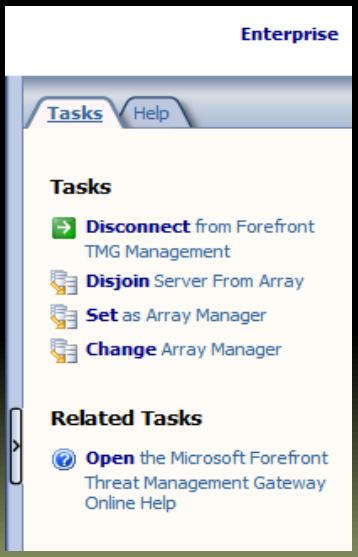
Joining/leaving arrays (Ent)

Video/Pictures

- TMG 2010 Joining Array

Array management

- New in TMG 2010
- Can be disjoint later
- Array Manager can be changed later



Threat Management Gateway 2010

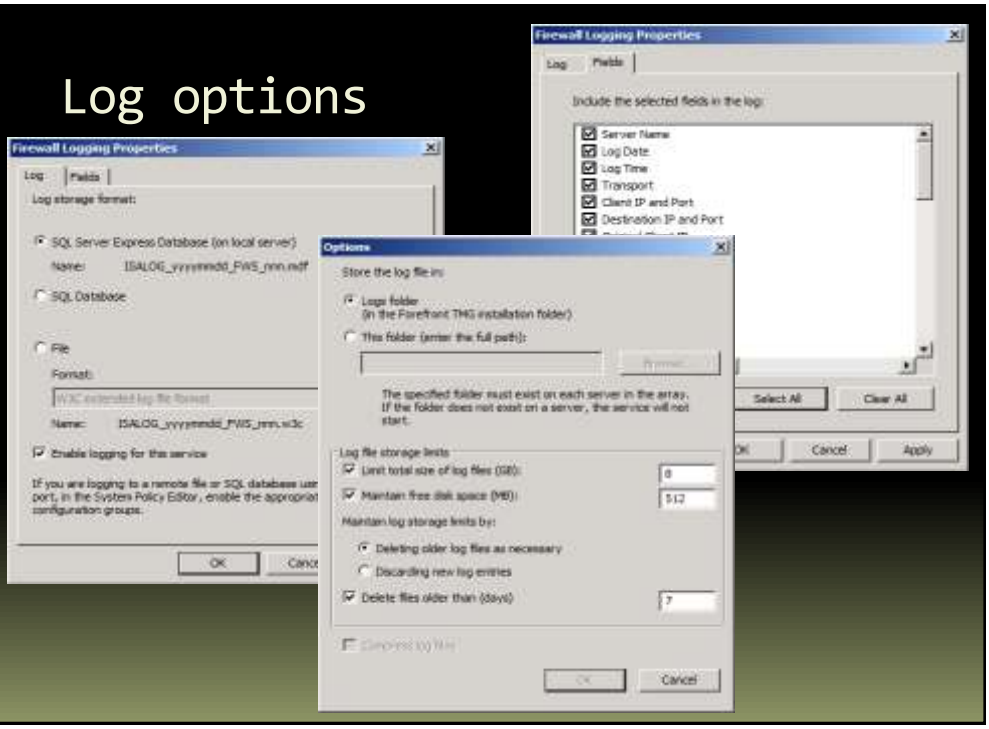
LOGS AND REPORTING

Logs and queries

- Local .TXT files
- Local SQL Server 2005 Express
  - limited to 4 GB per database
- Remote SQL Server
  - does not support built/in reporting

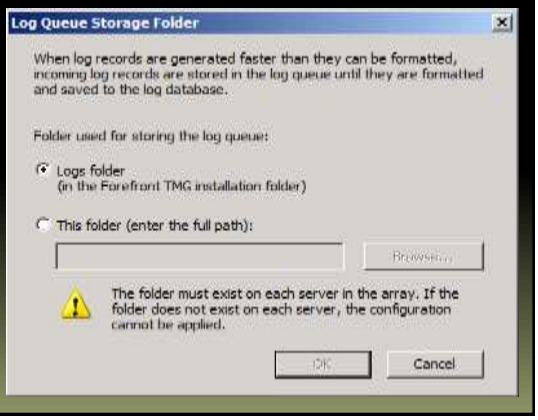
- Queries from the console (array)
  - queries all the array servers simultaneously if local logging enabled

Log options



Log Queuing

- In case the log storage is not available or is not responding promptly, TMG can cache them temporarily
- Older versions just killed FWSRV service



Example failed service 2006

Compression Failure (Decompression Failed)	9.9.2010 10:43:12	New	Other
Log failure	11.9.2010 0:02:17	New	Firewall Service
Log failure	11.9.2010 0:02:17	New	Firewall Service
Service shutdown	11.9.2010 0:02:28	New	Firewall Service
Configuration error	11.9.2010 14:54:45	New	Firewall Service
Service started	11.9.2010 14:54:58	New	Firewall Service
No connectivity	11.9.2010 14:55:12	New	Firewall Service

Alert Information

Description: The ISA Server Web filter was unable to connect to MSDE database. The MSDE Error description is: Could not obtain exclusive lock on database 'MODEL'. Retry the operation later., CREATE DATABASE failed. Some file names listed could not be created. Check previous errors.. The failure is due to error: 0x80040e14

Threat Management Gateway 2010

CONNECTIVITY VERIFIERS

Connectivity verifiers

- Every 30 sec. check connectivity
  - Ping, TCP, HTTP
- If the response is not in the timeout constraint, alert is raised
- To change the default 30 sec.
  - google: Setting Refresh Rate for Connectivity Verifiers

What to monitor

- Root DNS servers over TCP 53
- Google over HTTP GET
- Provider's SMTP smart host over TCP 25
- …

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

THANK YOU