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

ADVANCED TOPICS

Threat Management Gateway 2010

TMG CLIENTS TERMINOLOGY

Clients

- SecureNAT Client
  - no client ☺
  - just using routing (default gateway) to route packets through TMG
- Web Proxy Client
  - an application configured to use TMG as HTTP/S/FTP web proxy
- Firewall Client
  - TMG client software installed on the client computer

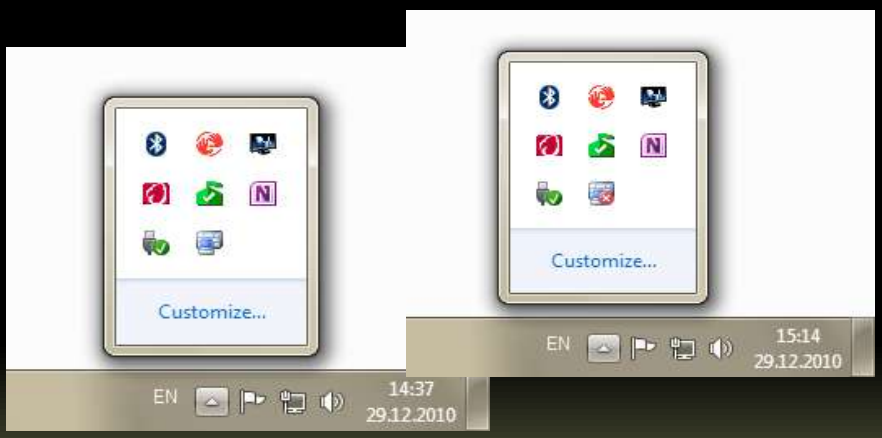
Threat Management Gateway 2010

FIREWALL CLIENTS

Firewall Client

- Seamless VPN-like connection with TMG
  - TCP/UDP only
  - "winsock proxy"
  - outbound connections only, LAN traffic directly
- Authenticated
- Encrypted
- Process name logged on TMG
- SSL Inspection notifications

Firewall Client



Support

- Supports Firewall Clients 2003+
- TMG Firewall Client runs on Windows XP+
- Firewall Client cannot be used with NLB enabled on TMG

Client Authentication

- Requires clients (users) to be authenticated
- Workgroup environment
  - credentials cannot be supplied manually
  - the local accounts must be "mirrored"

Installation

- Download manually from Microsoft
  - previous versions distributed with the client
- Install from .EXE
- Install from .MSI
  - group policy etc.

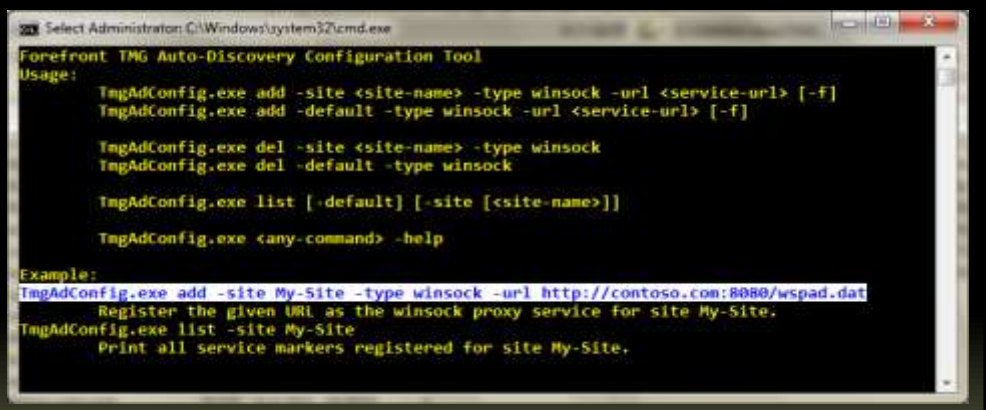
Demo: TMG Client Installation

- Show pictures

Configuration

- Proxy manually configured
- Proxy autodiscovery
  - DNS, DHCP for down-level and non-domain clients
- Active Directory discovery
  - serviceConnectionPoint installed by TMGADCONFIG utility
  - forest-wide or site-aware registration
  - requires at least TMG Firewall Client

AD Discovery



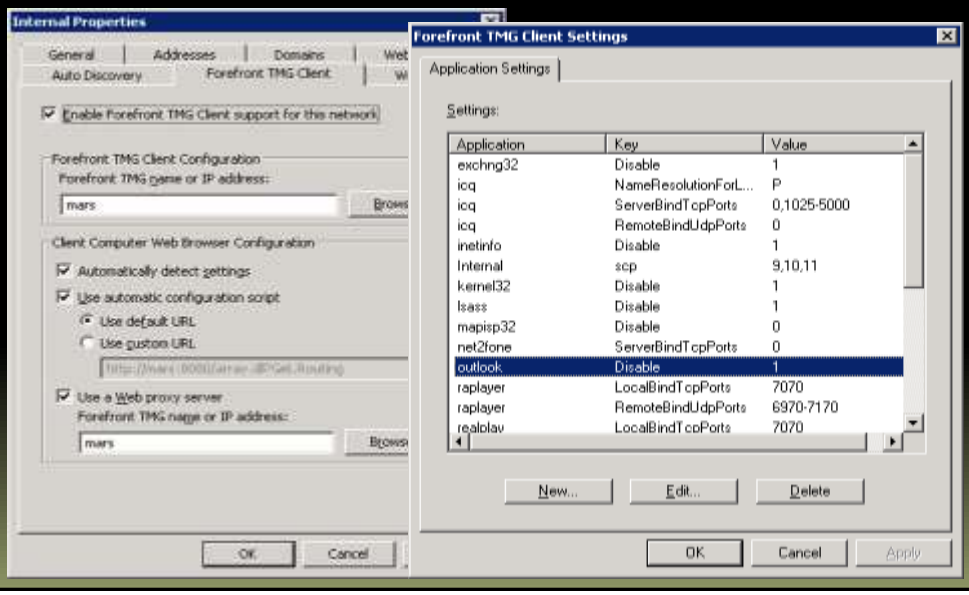
Supportability

- Problematic compatibility
  - personal firewalls
  - antivirus
- Problematic troubleshooting of client communication
  - encrypted

Lab

- Download TMGADCONFIG utility
- Configure forest-wide AD discovery
  - -default -type winsock
  - -url http://fw1.gopas.virtual/wpad.dat
- Download and install TMG Firewall Client on Seven1 computer
- Test discovery on the client computer
- Change the Telnet access rule to require All Authenticated Users
- Try TELNET from Seven1 to WEB-EXT and lookup the user name has been logged in TMG log
- Try accessing https://www.paypal.com and note the SSL Inspection Notification bubble

Advanced Settings



Threat Management Gateway 2010

SCRIPTING

Scripting

- COM interface for VBS/JS/.NET scripting
- Start with the FPC.Root object
- Documentation
  - Forefront TMG SDK (Software Development Kit)

Demo

- Investigate the sample scripts in SampleScripts folder

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

THANK YOU