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

OVERVIEW

Threat Management Gateway 2010

OVERVIEW

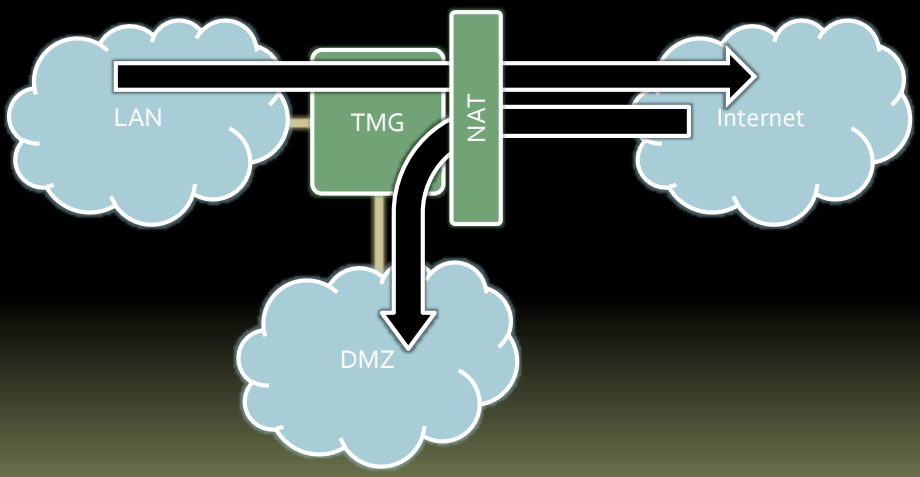
History

- Microsoft Proxy Server 1.0 (1997)
  - Windows NT 4.0, 32bit
- ISA Server 2000
  - Windows 2000, 2003, 32bit
- ISA Server 2004
  - Windows 2003, 32bit
- ISA Server 2006
  - Windows 2003, 32bit
- Forefront Threat Management Gateway 2010
  - Windows 2008/R2, 64bit

Features

- Network firewall + NAT
  - Stateful inspection
- Forward HTTP/HTTPS/FTP transparent proxy
- Reverse HTTP/HTTPS/FTP transparent proxy
- VPN server
  - PPTP, L2TP, SSTP, IPSec tunnel, DirectAccess
- Advanced features
  - Network Access Protection
  - Antimalware + Intrusion prevention

Forward vs. Reverse proxy



Features not Provided

- Bandwidth limiting
  - only IP DiffServ tagging for HTTP/S traffic
- MAC address filters/rules
  - TMG is places in TCP/IP stack
  - does not understand MAC addresses at all
- Bridge mode
  - TMG must have IP addresses and must be placed between IP networks

History

- Microsoft Proxy Server
  - forward HTTP/FTP proxy only
- ISA Server 2000
  - forward/reverse firewall + bandwidth control
  - single LAN+DMZ scenario only
- ISA Server 2004
  - rewritten, without bandwidth control
  - multi-networking
- ISA Server 2006
  - improved HTTP/S publishing, LDAP authentication
- Forefront Threat Management Gateway 2010
  - forward SSL inspection
  - antimalware + intrusion prevention

64bit version

- Can use more RAM
  - 32 GB on Windows Standard Edition
  - 2 TB on Windows Enterprise Edition
- Larger cache and better performance
  - single FWSRV process hosting the cache

Filtering

- Basic stateful protocol firewall
  - IP, TCP, UDP, ICMP, GRE, ESP, AH
- Application protocols
  - HTTP/S, DNS, FTP, SMTP, POP3, IMAP4, …
  - H.323, SIP, RSTP, …
- WebProxy application filters
  - caching, Forms/Windows/Basic/LDAP/RADIUS authentication, compression, DiffServ, load-balancing, link-translation, malware inspection

Structure

- Kernel mode driver
  - FWENG.SYS
  - net stop fweng
- User mode service
  - FWSRV – Microsoft Forefront TMG Firewall
    - previously Microsoft Firewall
  - net start fwsrv – starts both the service and driver
- Lockdown mode

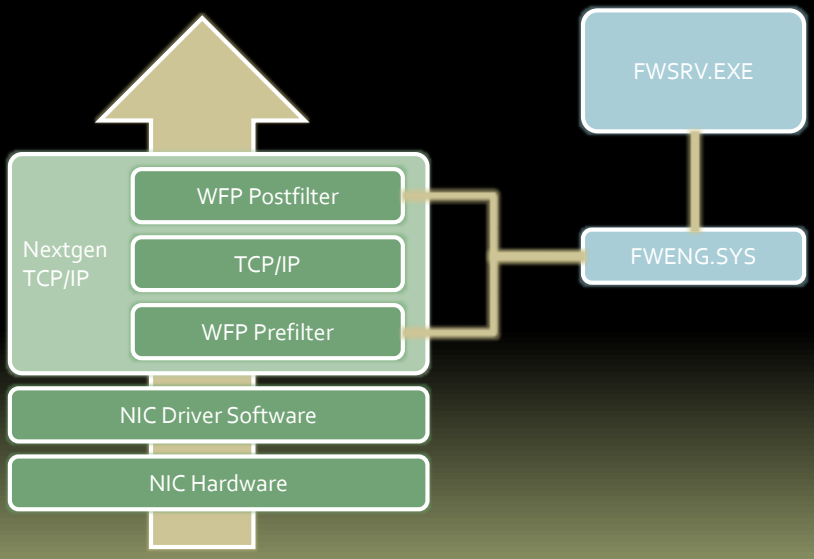
Lockdown mode

- FWENG blocks all incoming/passing traffic
  - except for some system rules (RDP, DHCP, Ping)
- TMG's own outgoing traffic is enabled

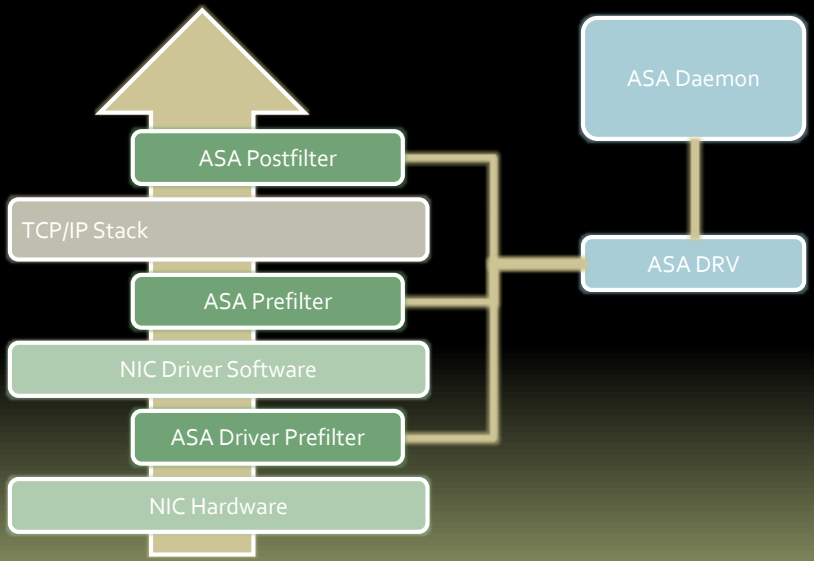
Windows Filtering Platform

- FWENG integrates with Windows Filtering Platform stack in Windows Vista+
  - cannot disable Windows Firewall service, Base Filtering Engine service and MPSDRV.SYS
  - similar lockdown mode

Windows Filtering Platform



Compare: Cisco ASA



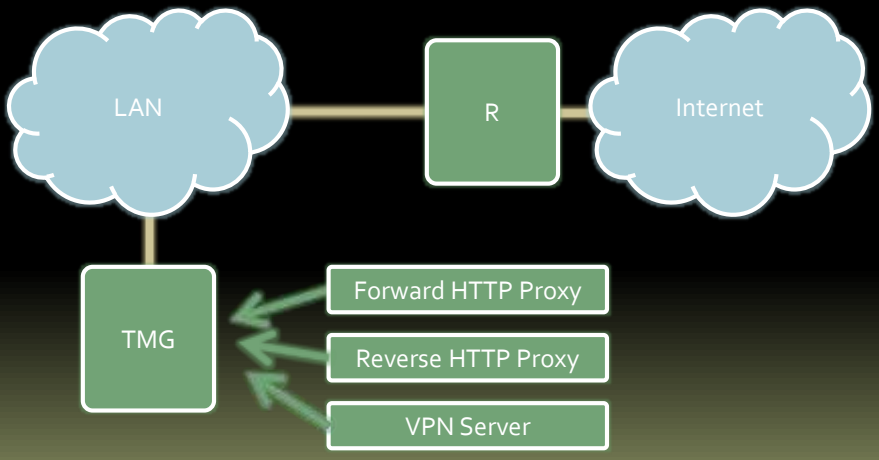
Threat Management Gateway 2010

NETWORK TOPOLOGIES

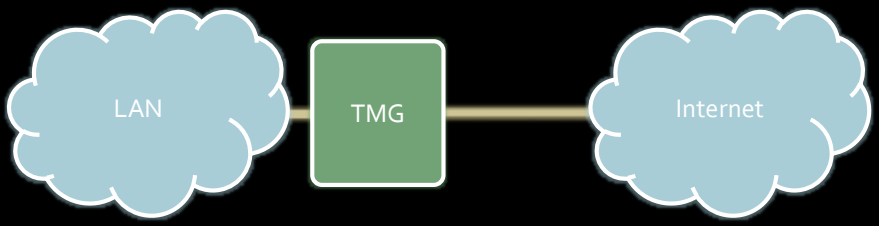
Topologies

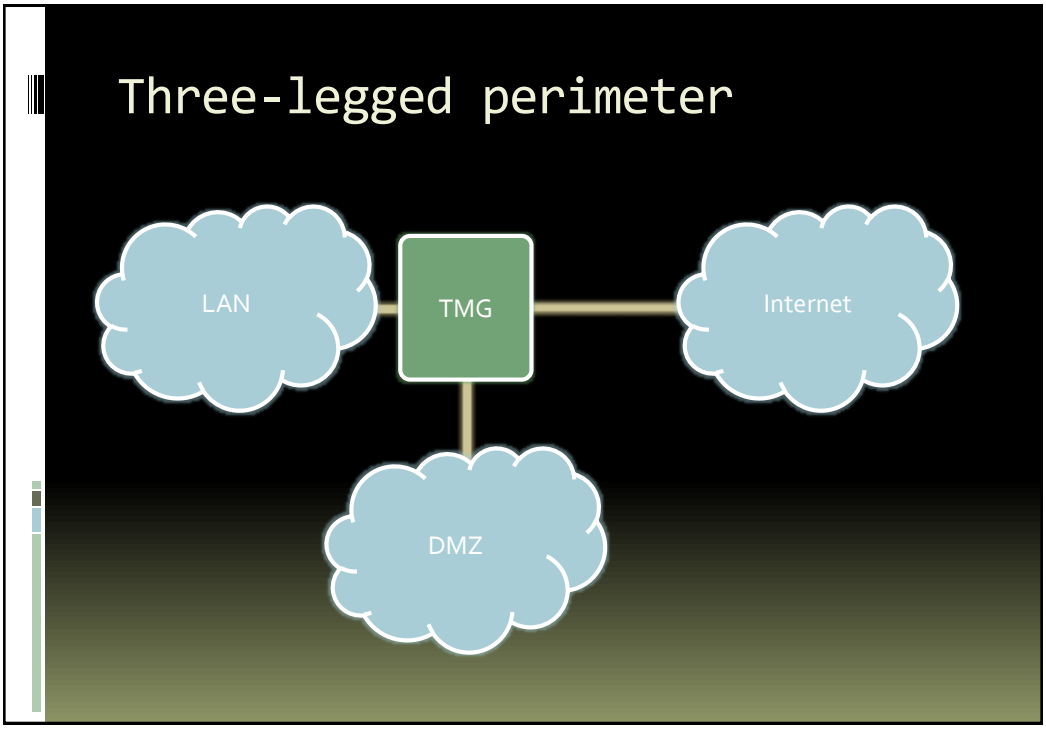
- Single NIC
  - forward HTTP/FTP proxy + VPN server only
  - no email protection
- Edge firewall
- Three-legged DMZ
- Back-end firewall

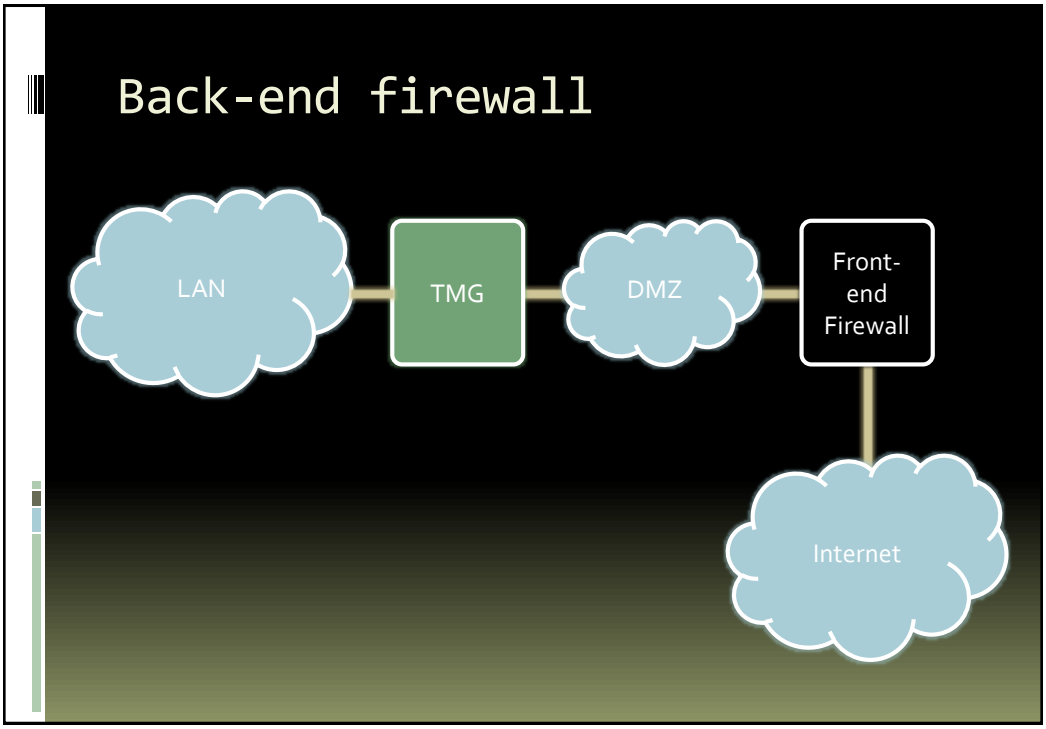
Single NIC



Edge firewall




Three-legged perimeter
LAN
TMG
Internet
DMZ


Back-end firewall
LAN
TMG
DMZ
Front-end Firewall
Internet

Hardware vs. Software?

- "Hardware firewall" is always normal computer
  - hardware firmware
  - OS + drivers + firewall software
- Windows disadvantages
  - open platform for hardware vendors
  - firmware and drivers not security certified
- ISA/TMG have had no real security vulnerability ever!

Threat Management Gateway 2010

DOMAIN MEMBERSHIP

Member of domain

- Full feature set
  - forward proxy Windows authentication (seamless)
  - firewall client (without mirrored accounts)
  - Kerberos constrained delegation
  - Protocol transition for certificate/smart card logon
- Can authenticate users simply against AD
- If compromised, the attacker is member of Users group on all internal resources

Member of domain

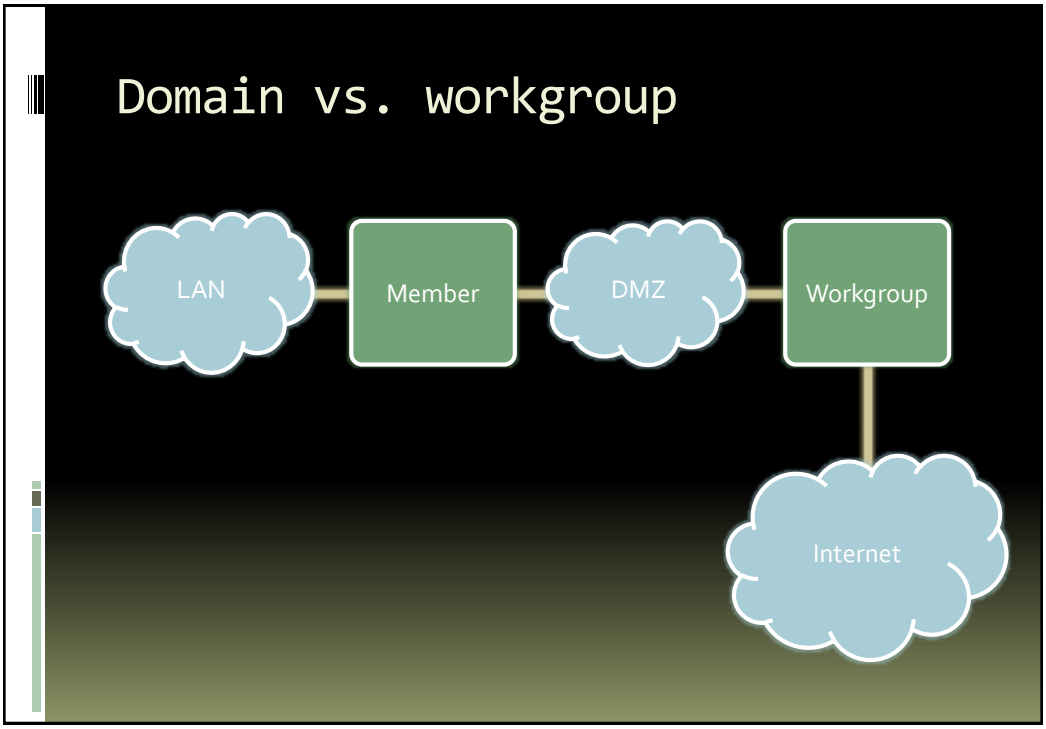
- Can create separate edge AD forest with incoming trust to the central AD
  - certificate authentication will not work for inside users

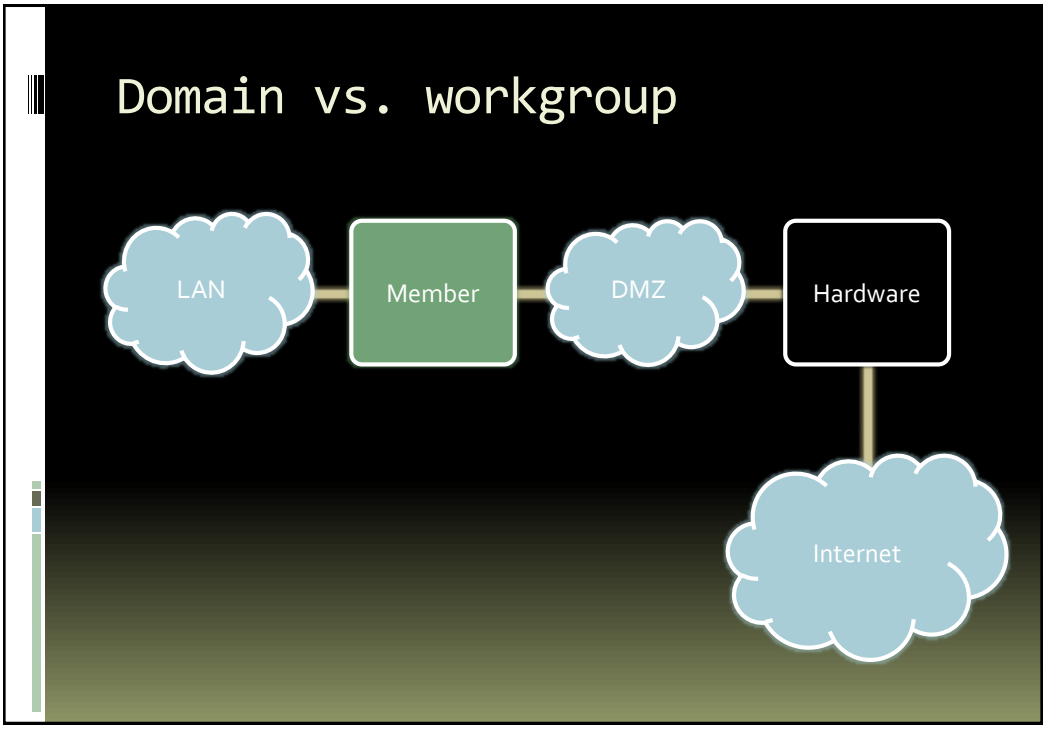
Video

- Computer group membership

Workgroup member

- RADIUS authentication
  - only user authentication
  - cannot use user groups
- LDAP authentication
  - Active Directory LDAP only
  - can use groups
  - cannot be used for forward proxy and access rules


Domain vs. workgroup
LAN
Member
DMZ
Workgroup
Internet


Domain vs. workgroup
LAN
Member
DMZ
Hardware
Internet

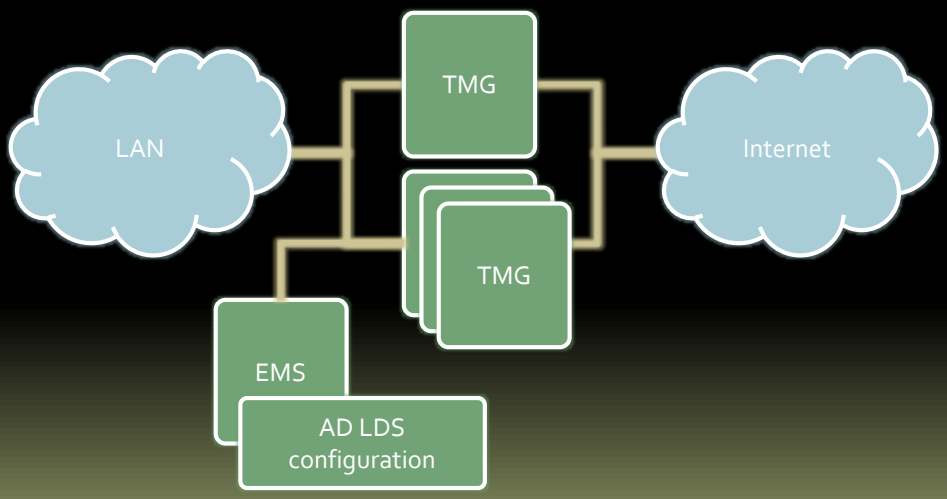
Threat Management Gateway 2010

ENTERPRISE EDITION

Standard vs. Enterprise

- Standard Edition
  - Standalone firewall with individual configuration
  - Can use NLB, but…
  - cca 1500$ per CPU socket
- Enterprise Edition
  - Separate configuration storage in AD LDS for more than one machine
  - All firewall hosts download configuration in regular 15 sec. intervals
  - cca 6000$ per CPU socket

Enterprise Edition



Can I Use Standard Edition as a Cheap Array?

- Not easily
  - may be for cold standalone replace
- NLB not supported
- If one firewall services fails, the NLB node would still remain active
  - custom script monitoring would be required
- HTTP Web Proxy does not use NLB
  - uses CARP with autodiscovery
  - would require custom .PAC/WPAD file editing

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

THANK YOU