

Forefront TMG



Agenda

- Forefront TMG Einfuehrung
- Forefront TMG Architektur
- Forefront TMG Installation
- Forefront TMG Webcaching
- Forefront TMG Webchaining
- Forefront TMG und Zertifikate
- Forefront TMG Webproxy ausgehend (Forward Proxy)
- Forefront TMG eingehende Verbindungen (Reverse Proxy)
- Forefront TMG Clients
- Forefront TMG Monitoring und Logging
- Forefront TMG Backup und Restore
- Forefront TMG VPN
- Forefront UAG - Ausblick

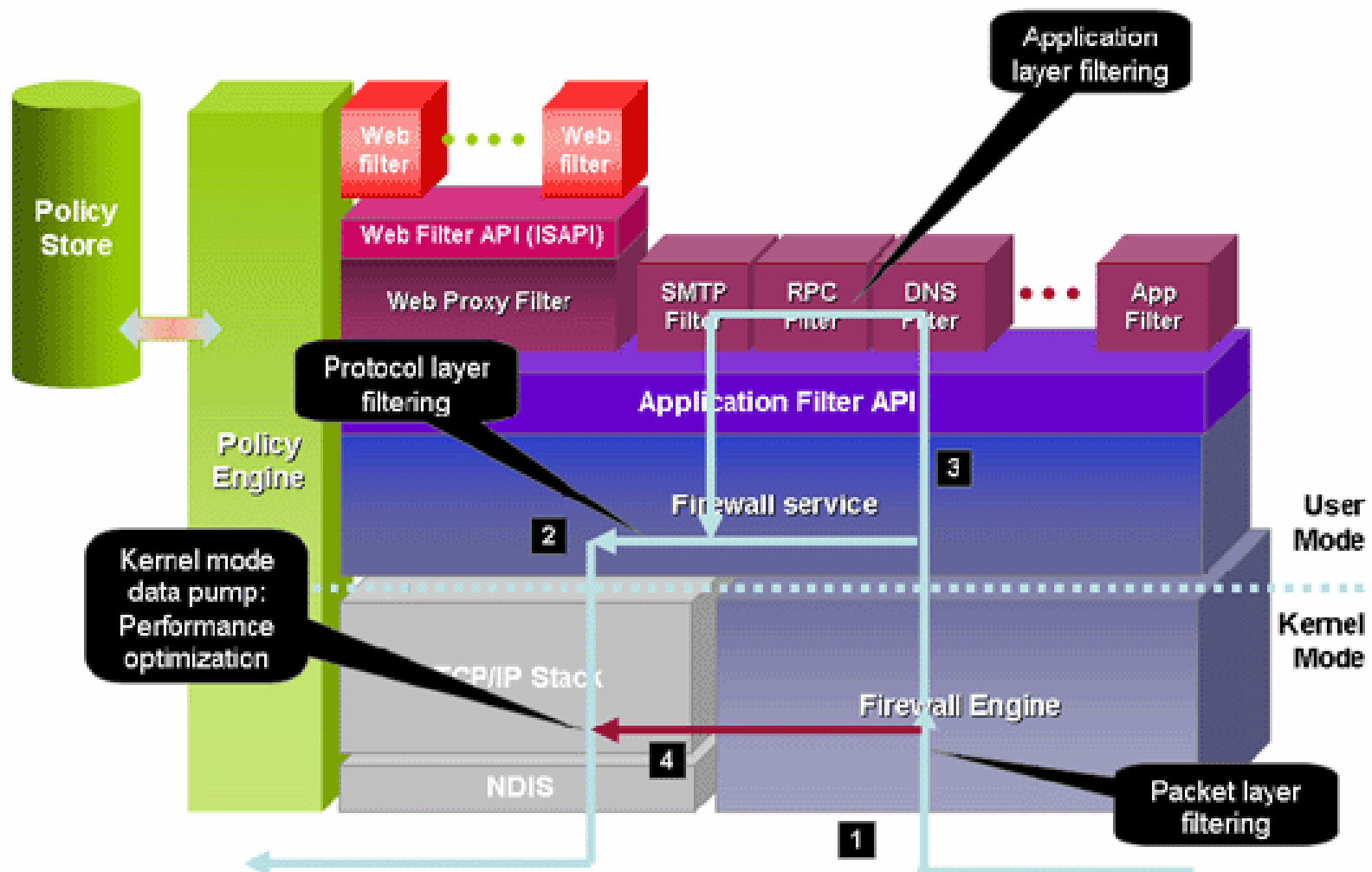
TMG Einfuehrung

- Funktionen
 - Stateful Packet Filtering Engine
 - Application Layer Firewall
 - Webproxy und Webcaching (Forward und Reverse)
 - VPN Server (Client und Site to Site)
 - SMTP Gateway mit Antispam und Antivirus
 - IDS/IPS/NIS Funktionalitaeten
- Erhaeltlich in zwei Versionen
 - Standard
 - Enterprise

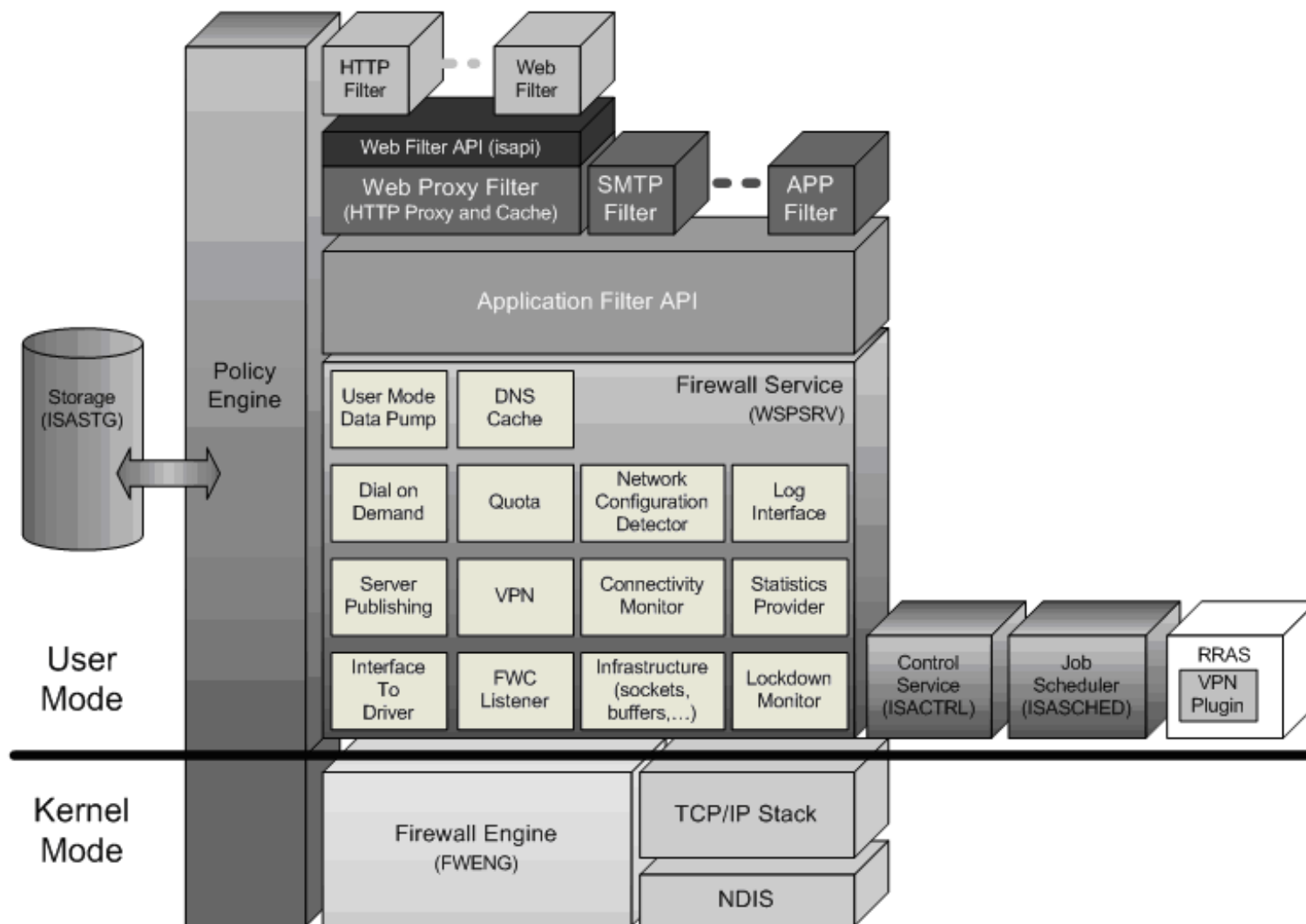
TMG Einfuehrung

- Funktionen von Forefront TMG Enterprise
 - Bis zu 32 Server in einem NLB Verbund
 - Integrated NLB mit TMG
 - Bidirektionale Affinitaet
 - NLB Health
 - CARP fuer verteiltes Caching
 - Zentrales Monitoring und Logging
 - Standalone Array (2 Server)
 - Enterprise Array mit EMS (Enterprise Management Server) moeglich

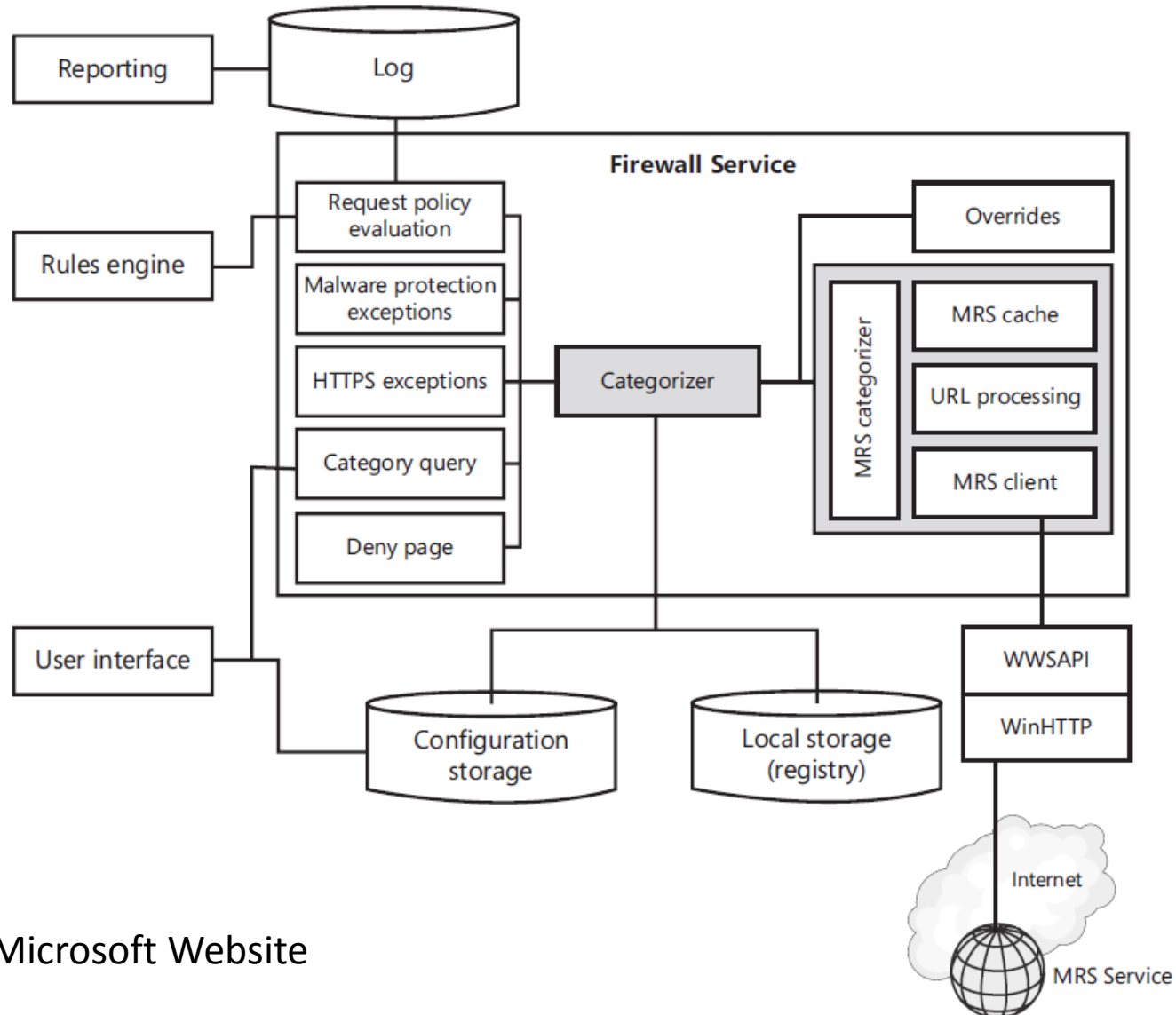
ISA/TMG Architecture



Firewall Core



TMG Komponenten



Source: Microsoft Website

Forefront TMG Installation

- Namensauflösung
- Windows Patching
- Netzwerkkarten
- Bindungsreihenfolge
- TMG Zertifikate (vorher CA installieren)
- TMG
 - 1. EMS
 - 2. TMG Array Member
- TMG SP1
- TMG Update 1
- SCW
- TMG Grundkonfiguration

TMG Storage

Connection Settings

Name:

Path:

Connection Point

☒ Select or type a Distinguished Name or Name

☐ Select a well known Naming Context:

Computer

☒ Select or type a domain or server: (Server)

☐ Default (Domain or server that you logged on to)

☐ Use SSL-based Encryption

ADSI Edit

File Action View Help

ACSI Edit

TMG-Storage (TMG-EN:2171)

CN=FPC2

Ch=ArrayRoot

Ch=Array

Ch=338FED3-C944-466F-68A2-44588E0C1D70

Ch=AdminSecurity

Ch=Alerts

Ch=ArrayPolicy

Ch=Attack Detection

Ch=ConnectionsAndPolicy

Ch=PrivSettings

Ch=LocalSettings

Ch=PolicyRules

Ch=RestrictedPorts

Ch=WebProxy

Ch=Cache

Ch=ChangeTracing

Ch=ClientConfigSettings

Ch=ConfigurationStorageServerConnection

Ch=ConnectivityTesters

Ch=CrossArraySettings

Ch=Extensions

Ch=Logs

Ch=MalwareInspectionSettings

Ch=NetConfig

Ch=NetworkInspectionSystem

Ch=NetworkTemplateUsed

Ch=PolicyAssignment

Ch=Reports

Ch=RuleElements

Ch=SecurityAssessmentSharing

Ch=Services

Ch=SimpleProtectionConfiguration

Ch=StatusRoutes

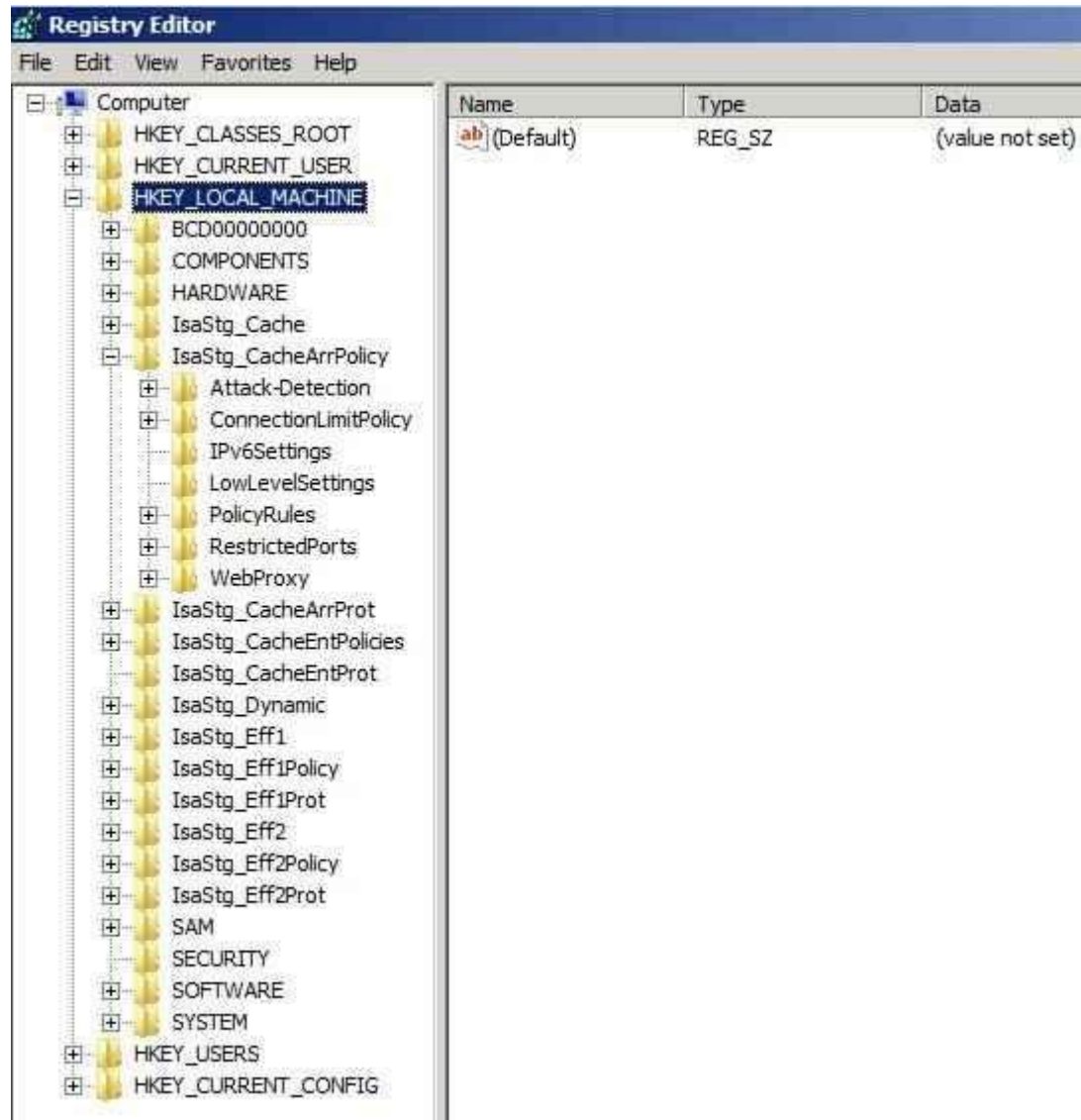
Ch=UpdateCenter

Ch=Enterprise

Ch=AdminSecurity

Name	Class	Distinguished Name	Actions
Ch=[02c367ed-b271-4062-bb7b-...	msPPolicyR...	Ch=[02c367ed-b271-4062-bb7b-...	Ch=PolicyRules
Ch=[0751ff3d-de3b-42c3-adde-...	msPPolicyR...	Ch=[0751ff3d-de3b-42c3-adde-...	More Actions
Ch=[085a640b-4b69-406a-a...	msPPolicyR...	Ch=[085a640b-4b69-406a-a...	
Ch=[111ED5D7-1ACD-4088-A5C...	msPPolicyR...	Ch=[111ED5D7-1ACD-4088-A5C...	
Ch=[17F5D563-af60-4509-a7...	msPPolicyR...	Ch=[17F5D563-af60-4509-a7...	
Ch=[1fabf11e-079f-4b75-b39f-...	msPPolicyR...	Ch=[1fabf11e-079f-4b75-b39f-...	
Ch=[202C45CC-15AC-492b-972...	msPPolicyR...	Ch=[202C45CC-15AC-492b-972...	
Ch=[24e29495-6e74-4170-b73e-...	msPPolicyR...	Ch=[24e29495-6e74-4170-b73e-...	
Ch=[27669C8A-4149-4331-A...	msPPolicyR...	Ch=[27669C8A-4149-4331-A...	
Ch=[339a72f1-05ec-4665-aabf-...	msPPolicyR...	Ch=[339a72f1-05ec-4665-aabf-...	
Ch=[36a09f20-4071-4b92-95...	msPPolicyR...	Ch=[36a09f20-4071-4b92-95...	
Ch=[382e8abe-2958-4129-8a1c-...	msPPolicyR...	Ch=[382e8abe-2958-4129-8a1c-...	
Ch=[414f2ad7-c5e9-4e57-9ff3-...	msPPolicyR...	Ch=[414f2ad7-c5e9-4e57-9ff3-...	
Ch=[43441a7c-2b0a-4ecf-96e5-...	msPPolicyR...	Ch=[43441a7c-2b0a-4ecf-96e5-...	
Ch=[4c0f1c2-b30b-11d2-9a16-...	msPPolicyR...	Ch=[4c0f1c2-b30b-11d2-9a16-...	
Ch=[4D150288-4724-4e2b-819f-...	msPPolicyR...	Ch=[4D150288-4724-4e2b-819f-...	
Ch=[4ff98cf-bd8e-4086-9a88-...	msPPolicyR...	Ch=[4ff98cf-bd8e-4086-9a88-...	
Ch=[51e9fca4-d552-41ae-e7...	msPPolicyR...	Ch=[51e9fca4-d552-41ae-e7...	
Ch=[5b4e11ae-bcf5-449e-bd8c-...	msPPolicyR...	Ch=[5b4e11ae-bcf5-449e-bd8c-...	
Ch=[5CAFEA25-698C-40b5-64b6-...	msPPolicyR...	Ch=[5CAFEA25-698C-40b5-64b6-...	
Ch=[5E3C2F88-8B3A-4682-9b44-...	msPPolicyR...	Ch=[5E3C2F88-8B3A-4682-9b44-...	
Ch=[60F76070-73b3-4b41-af...	msPPolicyR...	Ch=[60F76070-73b3-4b41-af...	
Ch=[65fcb53-981f-4638-b8...	msPPolicyR...	Ch=[65fcb53-981f-4638-b8...	
Ch=[68207300-5750-43ca-9...	msPPolicyR...	Ch=[68207300-5750-43ca-9...	
Ch=[6E8F4129-DF31-4e78-4...	msPPolicyR...	Ch=[6E8F4129-DF31-4e78-4...	
Ch=[7066f6b6-942e-40dc-bd74-...	msPPolicyR...	Ch=[7066f6b6-942e-40dc-bd74-...	
Ch=[78826D44-76E8-494D-A248-...	msPPolicyR...	Ch=[78826D44-76E8-494D-A248-...	
Ch=[7C210644-82EA-496F-A0B5-...	msPPolicyR...	Ch=[7C210644-82EA-496F-A0B5-...	
Ch=[7d315b78-aa24-4d72-8...	msPPolicyR...	Ch=[7d315b78-aa24-4d72-8...	
Ch=[79dc796b-612f-4d9d-9a...	msPPolicyR...	Ch=[79dc796b-612f-4d9d-9a...	
Ch=[83e30e3-3c2b-49a2-adbc-...	msPPolicyR...	Ch=[83e30e3-3c2b-49a2-adbc-...	
Ch=[86176638-C17E-459c-803...	msPPolicyR...	Ch=[86176638-C17E-459c-803...	
Ch=[86f6dda8-df58-4e2b-9f56-...	msPPolicyR...	Ch=[86f6dda8-df58-4e2b-9f56-...	
Ch=[8e344017-8bc5-4079-ad4c-...	msPPolicyR...	Ch=[8e344017-8bc5-4079-ad4c-...	
Ch=[96210741-c328-46c5-8b53-...	msPPolicyR...	Ch=[96210741-c328-46c5-8b53-...	

TMG Storage



Webcaching / Webchaining

- Webchaining
 - Webverkettung mit Upstream Proxy Server
 - Credentials Uebergabe moeglich
 - Malware Inspection moeglich
- Webcaching
 - Lokaler Cache fuer Webinhalte
 - Konfigurierbar
 - CARP in der Enterprise Version
 - CACHEDIR Tool zur Cache Verwaltung
 - Ueberwachung mit Perfmon

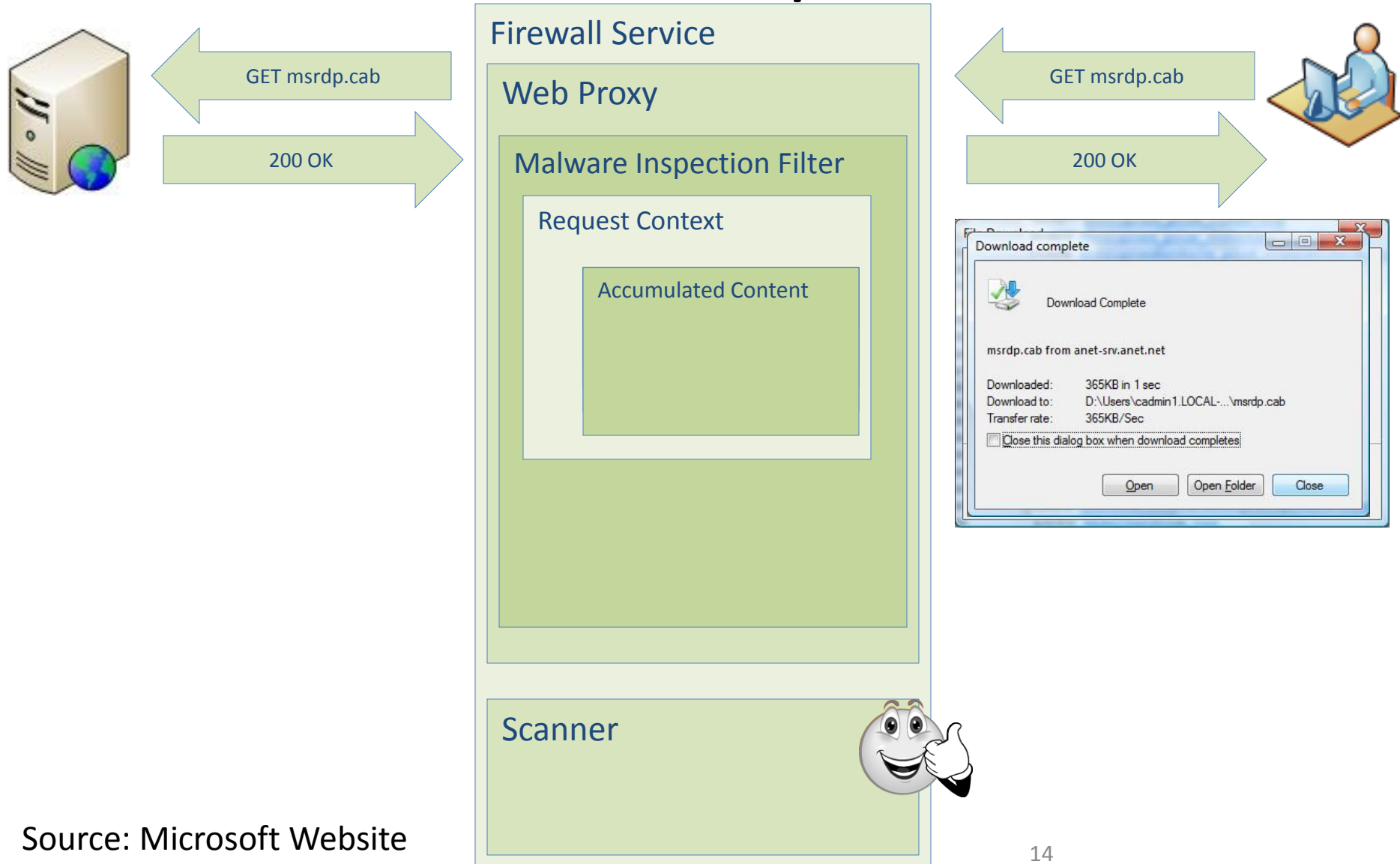
Forefront TMG und Zertifikate

- Ausgehende Verbindungen bei Verwendung der HTTPS-Inspection
- Eingehende Verbindungen bei Webserververoeffentlichungen und HTTPS Bridging
- Fallstricke bei der Veroeffentlichung
 - CN des internen Server muss mit dem Namen des Servers in der Veroeffentlichungsregel uebereinstimmen
 - Externer TMG Listener benoetigt ein Trusted Zertifikat
 - CN muss uebereinstimmen
 - Zertifikat muss trusted sein (Achtung bei Zugriffen von nicht Domaenen PC)
 - Speicherort lokaler Zertifikatspeicher des Computers
 - Private Key muss verfuegbar sein

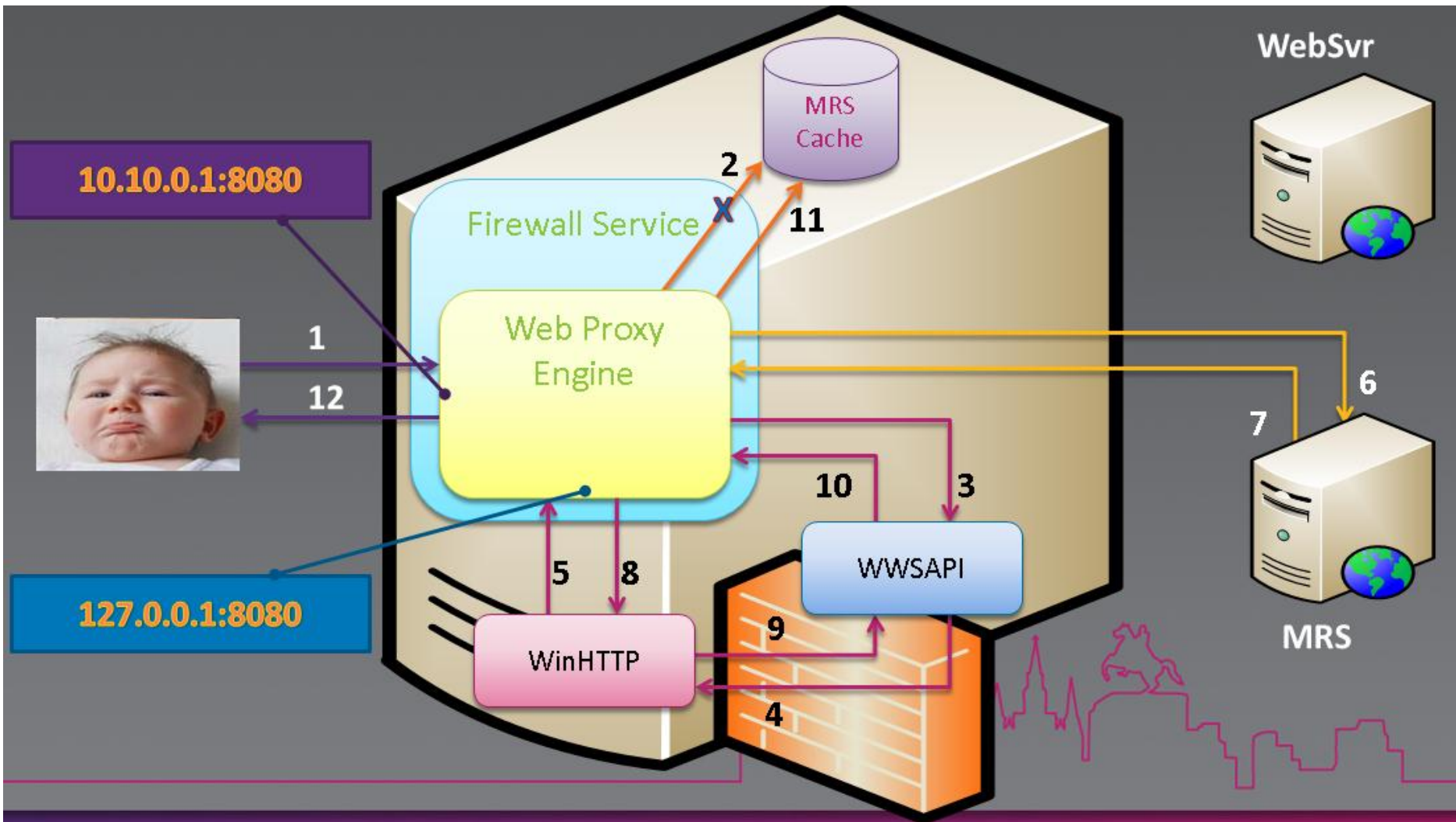
TMG Webproxy ausgehend

- Umfangreiches Regelwerk
 - IP Adressbeschränkung
 - Protokollbeschränkung
 - MIME Types
 - Zeitpläne
 - Benutzer- und Gruppenauthentifizierung
- Malware Inspection
- HTTPS Inspection
- NIS (Network Inspection System)
- HTTP Filtering

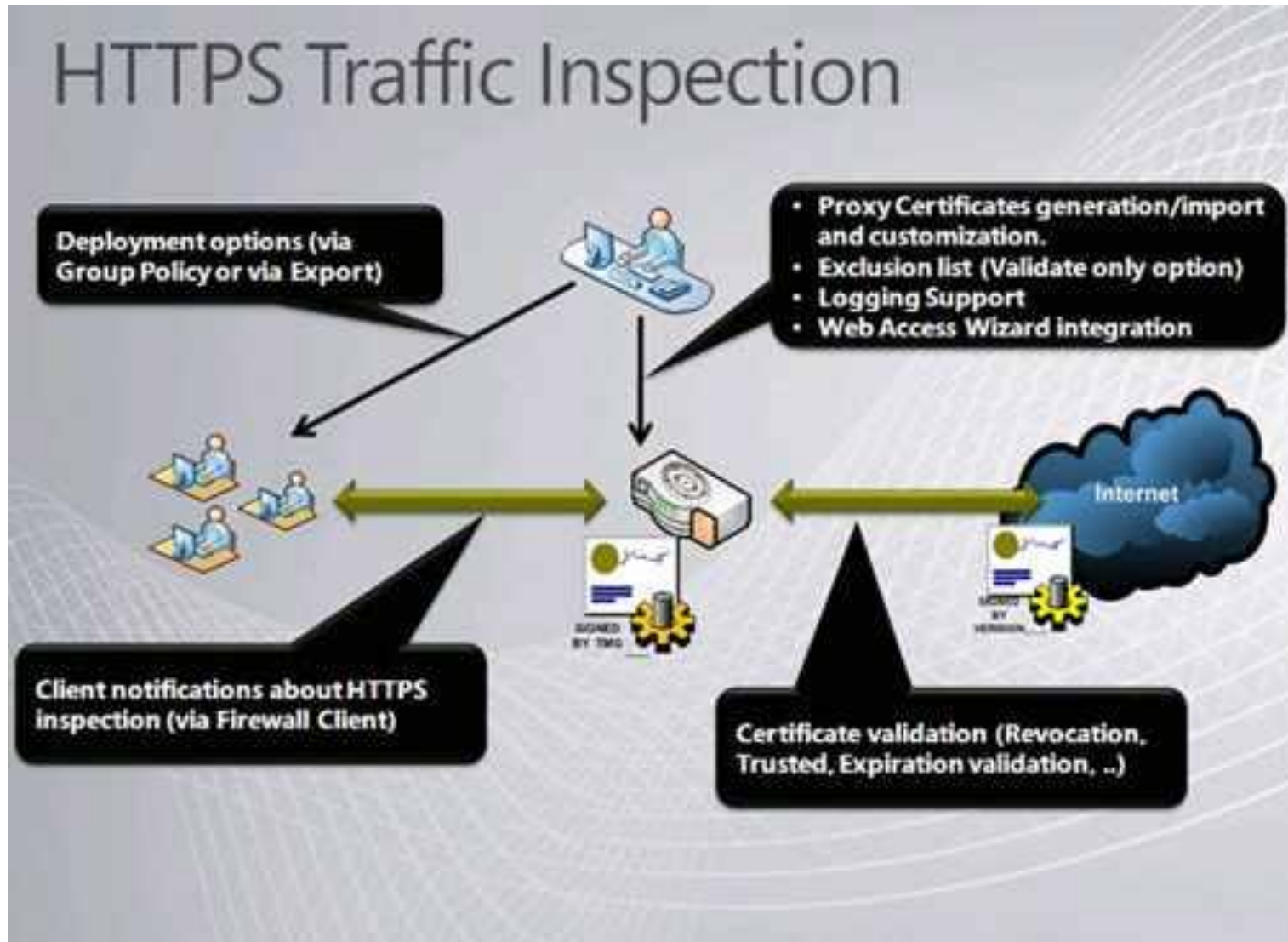
Malware Inspection



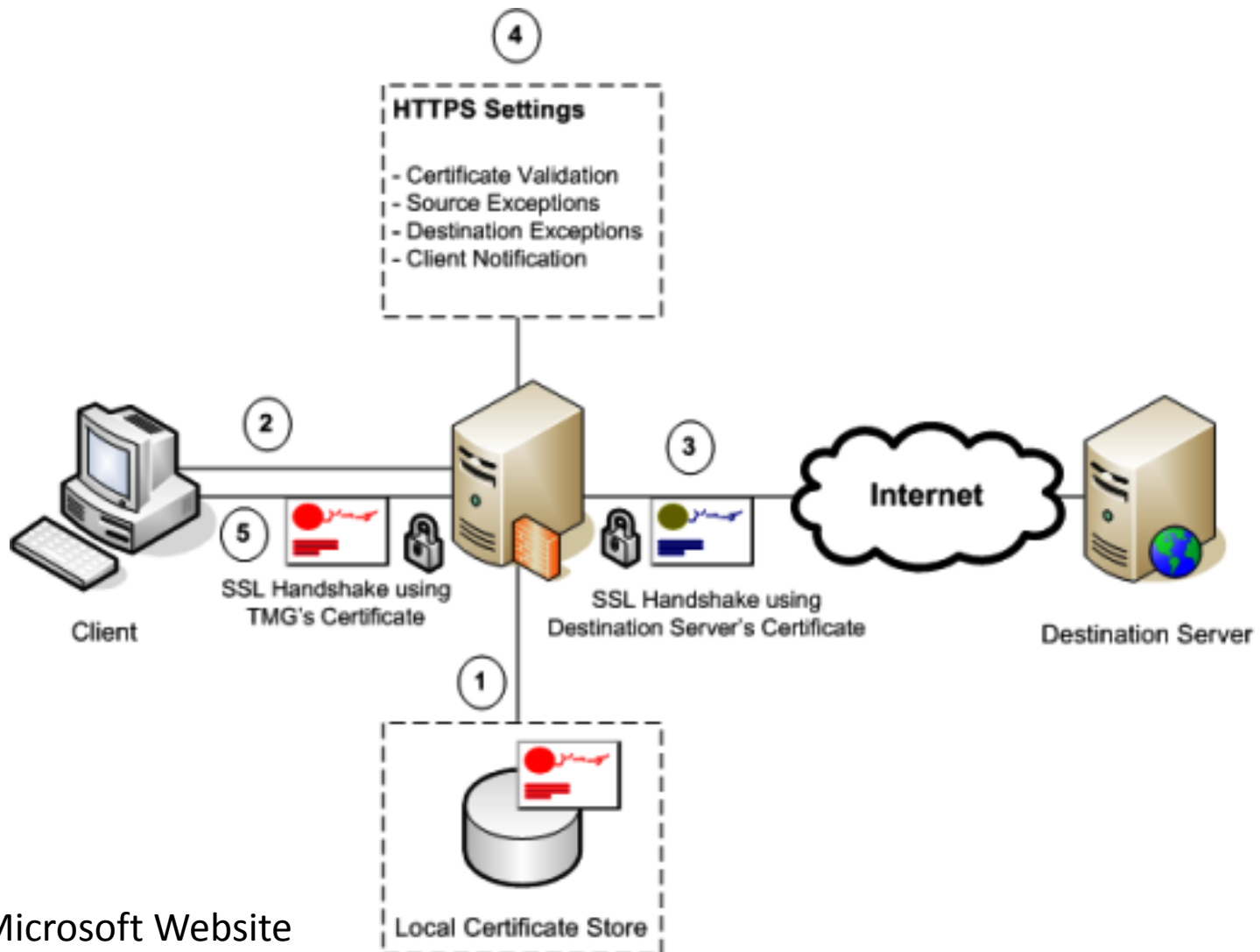
URL Filtering



HTTPS-Inspection

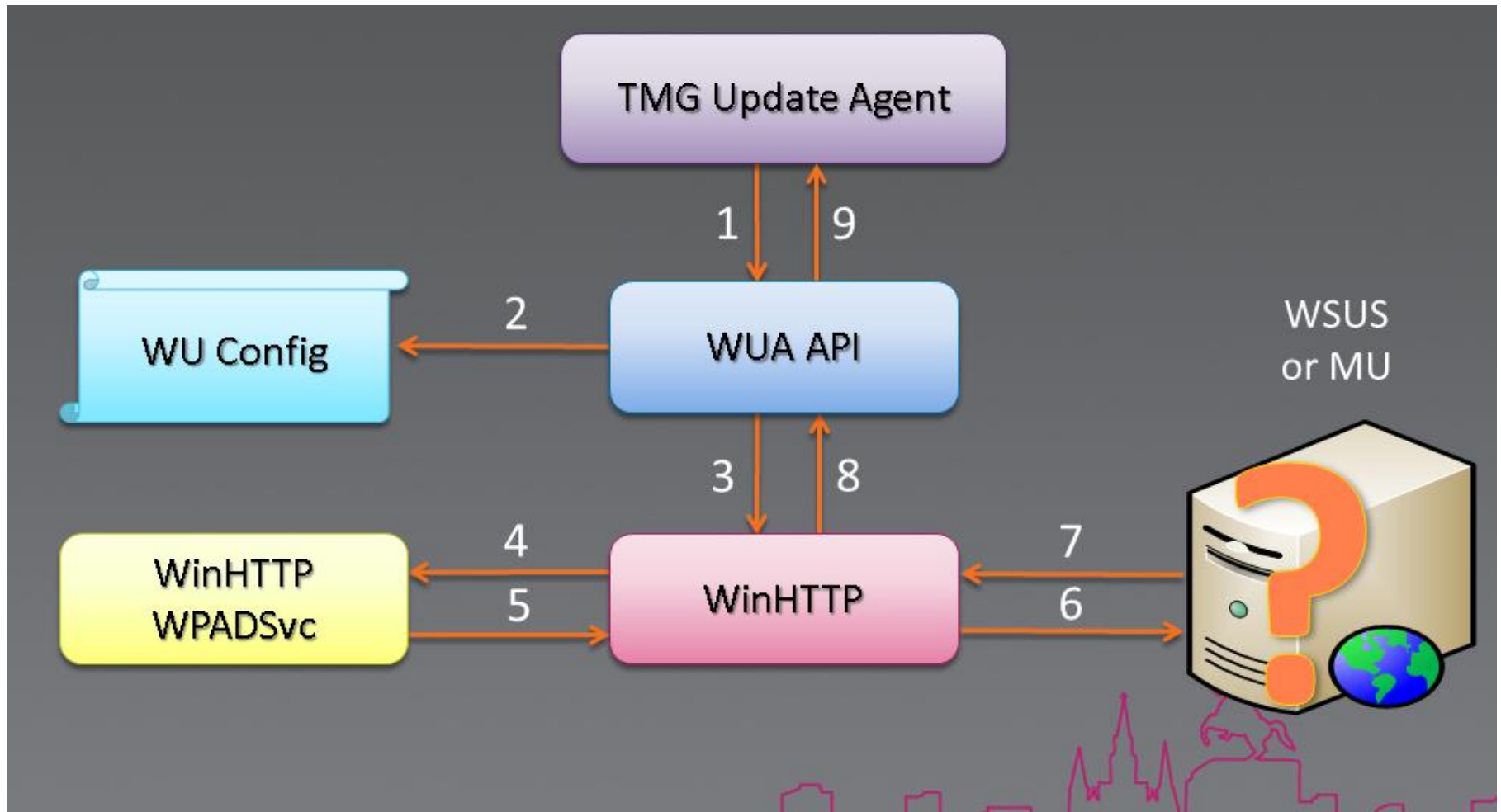


HTTPS-Inspection

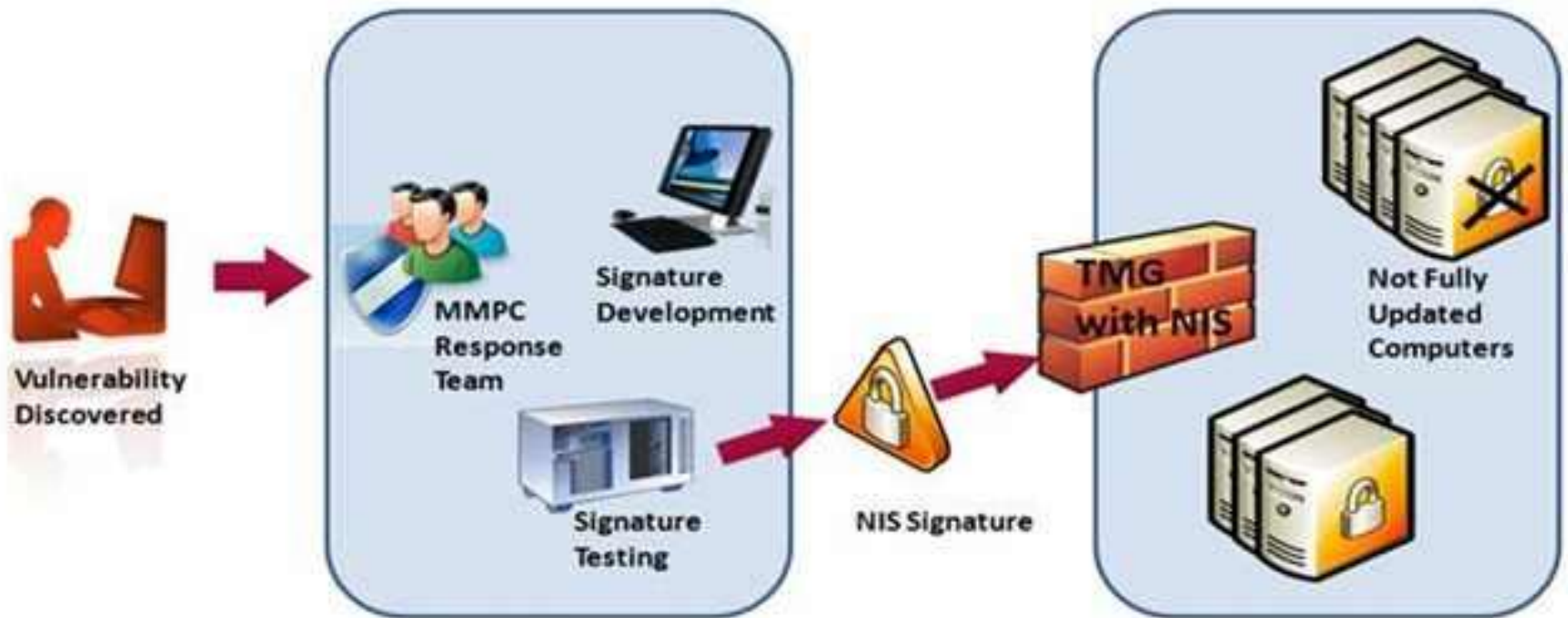


Source: Microsoft Website

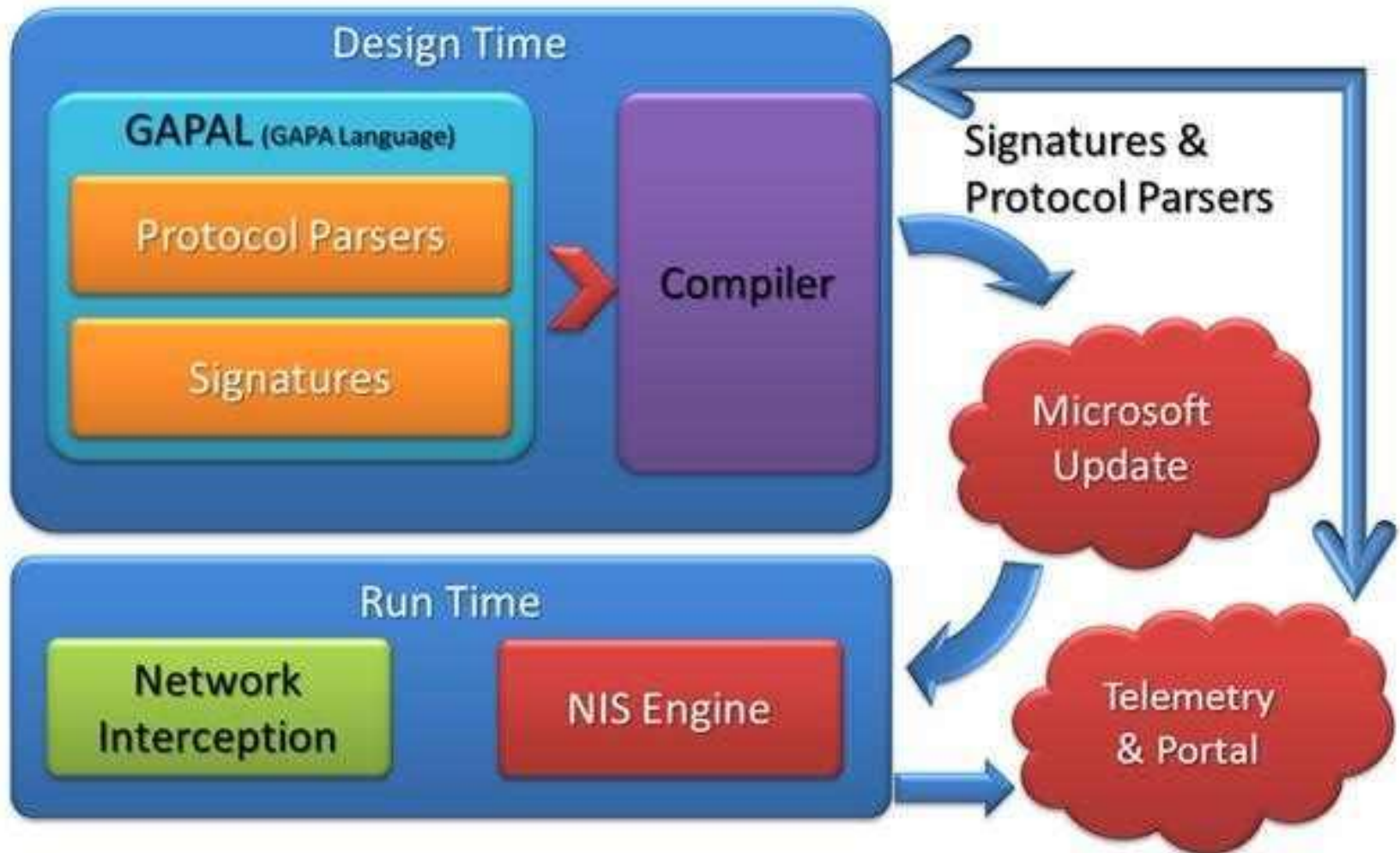
Signature Update



NIS



NIS



TMG Reverse Proxy

- Zwei grundlegende Veröffentlichungsmöglichkeiten
 - Serververöffentlichungen
 - Nicht Webserverprotokolle
 - PAT (Port Address Translation)
 - Keine erweiterten Filtermöglichkeiten
 - Webserververöffentlichungen
 - HTTP und HTTPS Serververöffentlichung
 - SSL Bridging
 - Prae Authentifizierung
 - URL Verification
 - Zertifikatprüfung
 - Regelwerk auf Benutzer- und Gruppenbasis
 - Vordefinierte Assistenten zur Exchange und Sharepoint-Veröffentlichung

Exchange Publishing

- OutlookWebApp, EAS, OA, Autodiscover
- Exchange Konfiguration
 - Zertifikate (SAN Request)
 - Internal / External Names
 - OutlookWebApp FBA deaktivieren
- TMG Konfiguration
 - Zertifikate fuer oeffentlichen Listener
 - Public Name – Internal Name
 - Usergroups
 - Authentifizierungsoptionen
 - SSL Bridging

Forefront TMG Clientarten

- Drei Clients verfuegbar
 - Webproxy Client
 - SecureNAT Client (Selten auch als SecureNET Client bezeichnet)
 - Forefront TMG Client (ehemals ISA Server Firewall Client)

Webproxy Client

- Proxy Einstellungen im Browser
- Zentrale Administration
 - WPAD (DHCP+DNS)
 - Group Policy
 - PAC File
- Verwendbar fuer HTTP/HTTPS und FTP DL only
- Verwendung von Authentifizierung in Firewallrichtlinien moeglich

SecureNAT Client

- Default Gateway oder Route zum TMG Server
- Keine Firewallregeln mit Benutzerauthentifizierung moeglich
- Alle TCP/UDP/IP Protokolle
- Ggfs. TMG Applikationsfilter notwendig fuer komplexe Protokolle
- Plattformunabhaenig (benoetigt nur TCP/IP Stack)

Forefront TMG Client

- Ehemals ISA Server Firewall Client
- Software Installation auf Endgeraet notwendig
 - Minimale Client Version ist Windows XP
- Administration mit Hilfe von INI Dateien oder zentralen TMG Einstellungen
- Firewallregeln mit Benutzerauthentifizierung fuer TCP/UDP Protokolle moeglich
 - Minimale Client Version ist Windows XP

TMG Monitoring und Logging

- Logging in
 - SQL Express lokal (Default)
 - Zentraler MS SQL Server
 - Textfiles
- Realtime Logging
- One Time Reports
- Recurring Reports
- User Activity Reports (SP1)
- Reports anpassbar mit SQL Reporting Services
- Large Logging Queue (LLQ) gegen TMG Server Lockdown Modus

TMG Backup und Restore

- Sicherung der Konfiguration oder einzelner Elemente in XML-Dateien
- Bare Metal Recovery von TMG möglich
- Scheduled Backups mit Script und Task Scheduler möglich
- Was ist noch zu sichern
 - TMG Zertifikate
 - Logdateien
 - Customized HTML Forms und custom error messages

TMG und VPN

- Client VPN
 - PPTP
 - L2TPC/IPSEC
 - SSTP
- Site to Site VPN
 - PPTP
 - IPSEC PSK und Zertifikate
 - L2TP/IPSEC
- VPN Quarantaene
 - NAP Integration
 - Keine RQS Komponenten mehr

Ausblick Forefront UAG

- Forefront TMG ist die Firewall des Unternehmens
- Forefront UAG ist die Application Layer Firewall fuer EINGEHENDEN Zugriff
- Forefront TMG ist Basis fuer Forefront UAG
- Zahlreiche Einschränkungen im Zusammenspiel UAG/TMG, bzw. des Einsatzzweckes von UAG

Ausblick Forefront UAG

- SSL VPN
- Direct Access
- Remote App Publishing
- Portalloesungen
- Hochverfuegbarkeit
 - NLB und Arrays
- Endpoint Access Policies
 - Forefront UAG, NPS, NAP
- Application Optimizer fuer ...
 - Sharepoint
 - Exchange
 - CRM uvm.

Ausblick Forefront UAG

	TMG	UAG
Application Intelligence and Publishing	✓	✓
End Point Security		✓
SSL Tunneling		✓
Information Leakage Prevention		✓
Robust Authentication Support (KCD, ADFS, OTP)	✓	✓
Product Certification (Common Criteria)	✓	✓ New
NAP Integration	✓	✓ New
Terminal Services Integration		✓ New
Array Management	✓	✓ New
Enhanced Management and Monitoring (MOM Pack)	✓	✓ New
Enhanced Mobile Solutions		✓ New
New and Customizable User Portal		✓ New
Wizard Driven Configuration	✓	✓ New
Globalization (RTL Languages)	✓	

Buch

Ca. 907 Seiten Umfang
Von drei Forefront MVP
Dieter Rauscher
Christian Gröbner
Marc Grote

seit 15.09.2010 verfügbar

Veröffentlichung September 2010

Basiert auf Microsoft Forefront TMG

Standard und Enterprise

Das Buch beschreibt die Implementierung
von Forefront TMG anhand
einer fiktiven Firma



Lust auf Links?

- Forefront TMG Blog + Infos
<http://www.forefront-tmg.de>
- ISA / TMG Informationen (EN)
<http://www.isaserver.org>
- ISA / TMG Informationen (DE)
<http://www.msisafaq.de>
- Technet TMG Dokumentation
<http://technet.microsoft.com/en-us/library/cc441438.aspx>
- Forefront UAG Blog
<http://blogs.technet.com/b/edgeaccessblog/>
- Forefront TMG Blog
<http://blogs.technet.com/b/isablog/>
- ISA/TMG Skripte
<http://www.isascripts.org>
- ISA/TMG Tools
<http://www.isatools.org>
- And many many more

Das Ende

- Vielen Dank fuer Ihre Aufmerksamkeit

Fragen?

