Microsoft Forefront UAG

MARC GROTE
IT TRAINING GROTE
JULI 2010

Because it's everybody's business

Microsoft Forefront

Because it's everybody's business

Agenda

Ueberblick ueber die Forefront Produktpalette
Einführung in Forefront UAG Konzepte
Einsatzgebiete
Unterschied Forefront UAG zu IAG
Systemvoraussetzungen
Einschraenkungen von UAG im Zusammenspiel mit TMG
Forefront UAG Installation
UAG Update 1 Neuerungen
UAG und TMG Best Practice Analyzer
TMG Grundlagen / Neuerungen
Zusammenspiel UAG mit TMG und Windows
UAG Grundkonfiguration
Zertifikatgrundlagen / Einsatzgebiete

Agenda

Authentifizierung und Autorisierung
Bereitstellung einer Remotezugriffsloesung fuer:
- Exchange (Outlook Web App)
- Remote Desktop Services

UAG Endpoint Security
Forefront UAG Direct Access
NAP Integration
Hochverfuegbarkeit und Skalierbarkeit
Monitoring und Troubleshooting
Backup und Recovery
Spezielle Konfigurationen
Migration von IAG zu UAG

Zunehmende Herausforderungen für die Sicherheitsumgebung

Gefährlichere Bedrohungen

- Fortgeschrittenerer
- Anwendungsorientierter
- Häufiger
- Auf Profit abzielend

Fragmentierung von Sicherheitstechnologie

- Zu viele Einzelprodukte
- Dürftige Interoperabilität
- Fehlende Integration
- Fehleranfällige Verwendung

Schwierige Verwaltung und Bereitstellung

- Mehrere Konsolen
- Ereignis-Reporting und -analyse unkoordiniert
- Hohe Kosten und Komplexität

Die Anforderungen

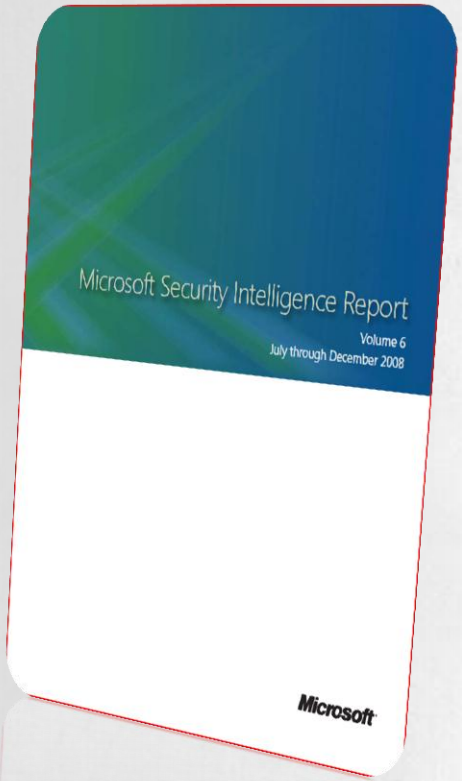
Die Microsoft-Initiativen zur IT-Sicherheit

Security Development Lifecycle

- Definiertes Vorgehen
- Sicheres Design bereitstellen und Risiken frühzeitig reduzieren

Security Intelligence Report

- Halbjährlich erscheinender Report des Microsoft Malware Protection Teams
- www.microsoft.com/sir



Engagement in Standardisierung, Strafverfolgung und Endanwender-Sensibilisierung und –Schutz

- www.microsoft.de/mse

Eingebaute Sicherheitsfunktionalitäten

- Etwa bei Windows 7, Windows Server 2008 R2, Microsoft Office, SharePoint

Was ist Microsoft Forefront?

Because it's everybody's business

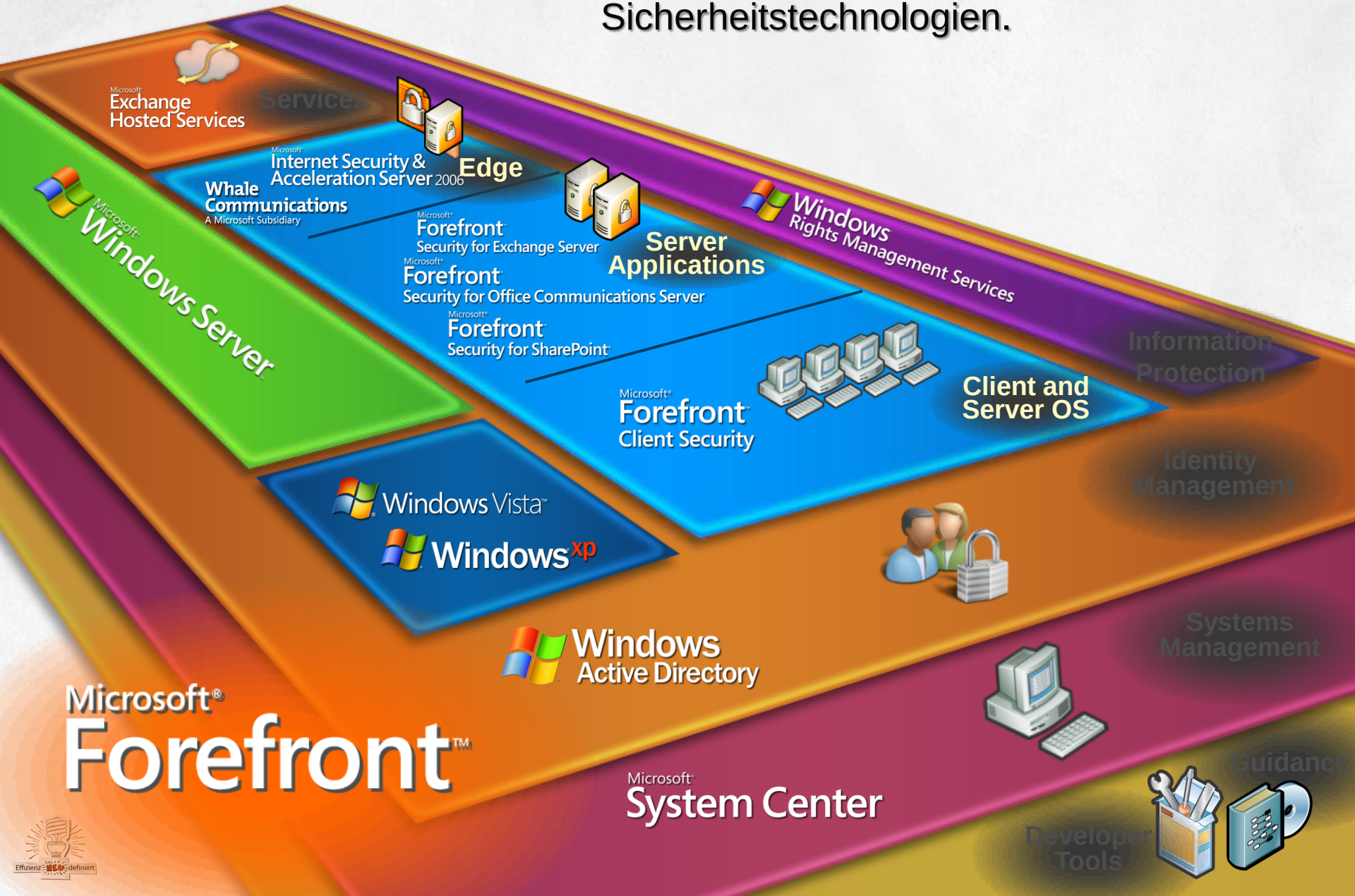
Microsoft® Forefront™

Microsoft® Forefront™

Eine umfassende Familie von Sicherheitsprodukten für die Öffentliche Verwaltung und Unternehmen, die durch enge Integration und vereinfachte Verwaltung einen größeren Schutz ermöglichen.

Because it's everybody's business

Microsoft vereint branchenführende, durchgängige und effiziente Sicherheitstechnologien.



Das bisherige Forefront Identitäts- und Sicherheitsangebot

Endpunkt

Microsoft® Forefront™ Client Security

Netz-werk

Microsoft® Internet Security & Acceleration Server 2006

Intelligent Application Gateway 2007

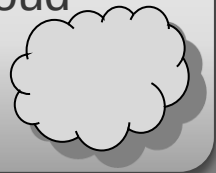
Server

Microsoft® Forefront™ Security for SharePoint®

Microsoft® Forefront™ Security for Office Communications Server

Microsoft® Forefront™ Security for Exchange Server

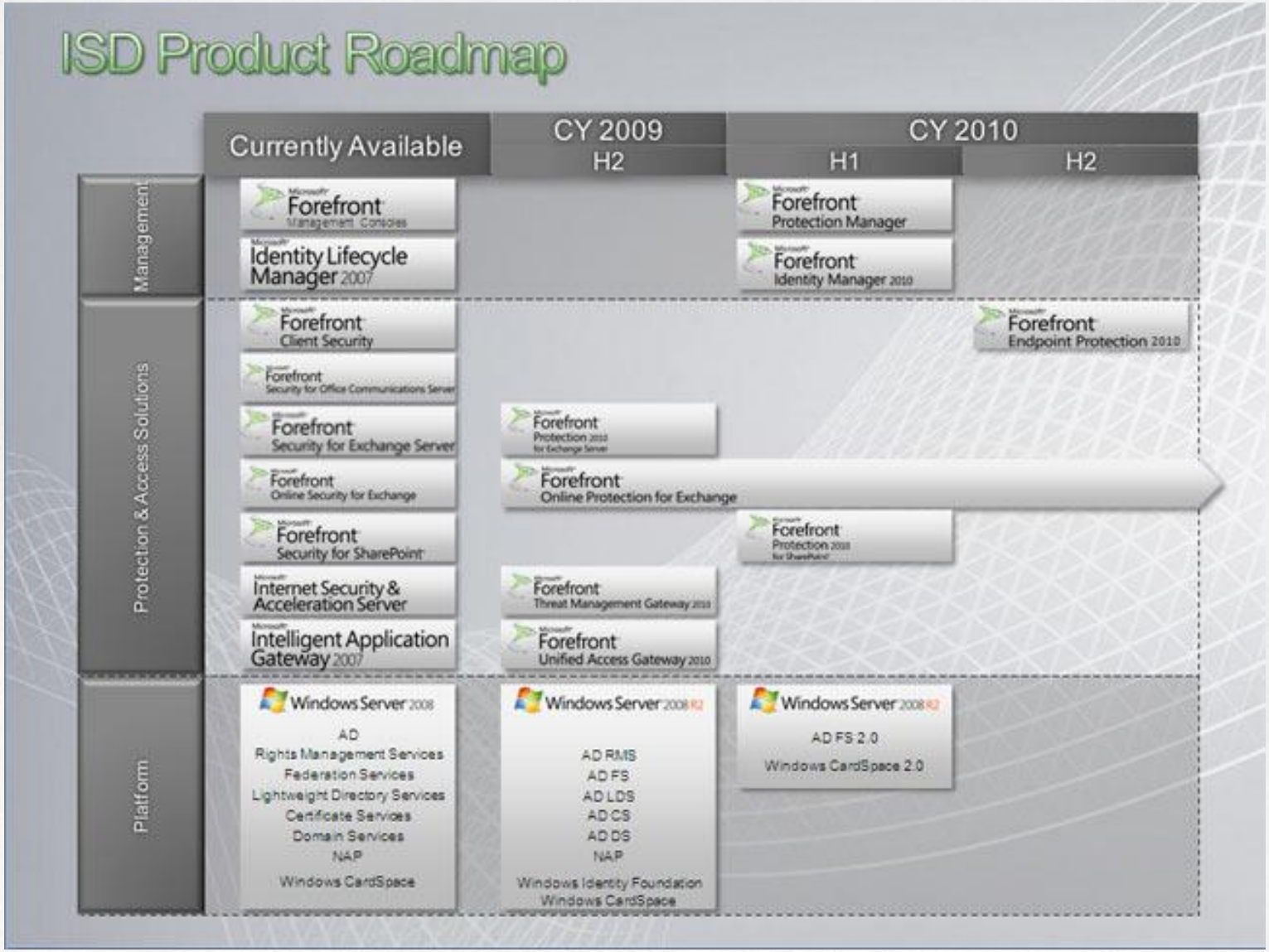
Cloud



Microsoft® Forefront™ Online Security for Exchange

Weitere Lösungen:
- Identity Management
- Rights Management
- NAP …

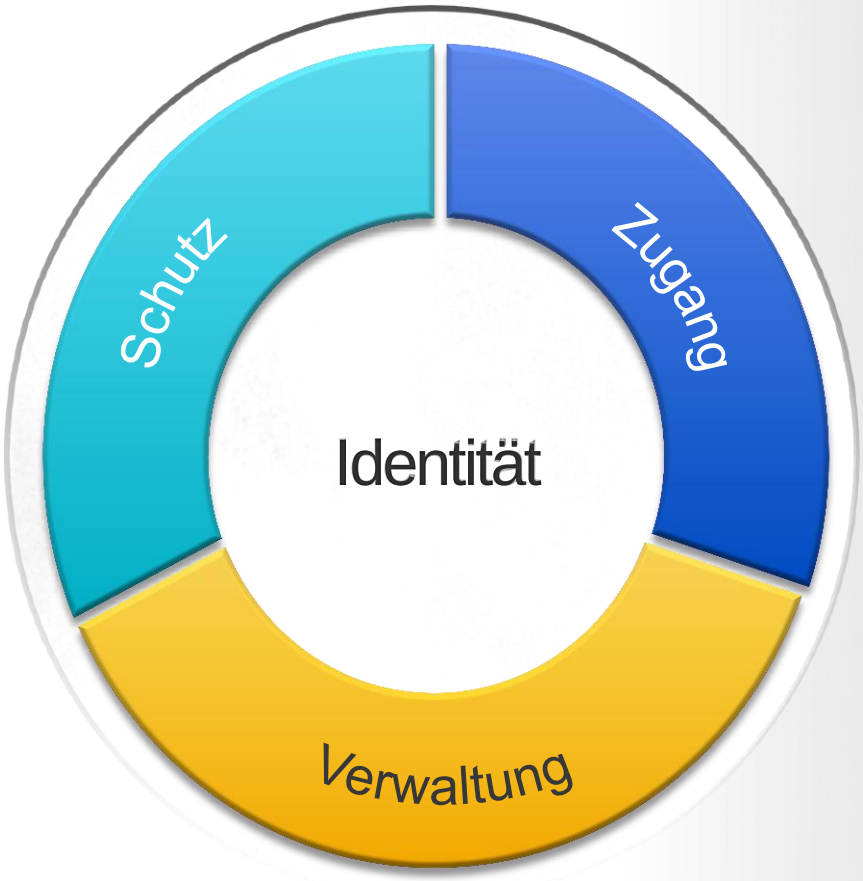
Realitaet und (nahe) Zukunft



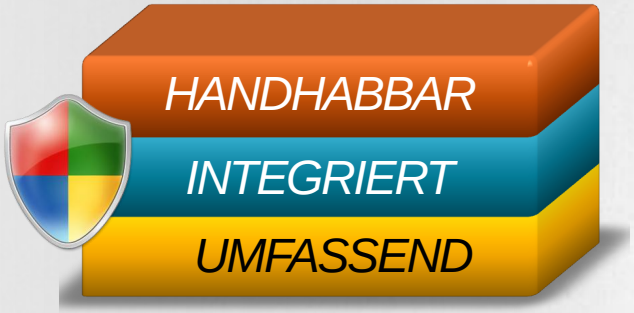
Unser Ansatz:
Business Ready Security

Because it's everybody's business

Microsoft Forefront



Sicherheits- und Identitäts-Lösungen bilden eine untrennbare Einheit.



Effizienz – IEEU – definiert

Because it's everybody's business

Forefront Protection Suite – Architektur

Because it's everybody's business

Microsoft Forefront

Vereinheitlichte Verwaltung | Ausführliches Reporting | Unternehmensweite Analyse

Forefront Protection Manager
(zentrale Verwaltungkonsole)

Security Assessment Sharing (SAS)

EINGESTELLT MAI 2010

Client- & Server-OS

Microsoft Forefront Endpoint Protection 2010

Server-anwendungen

Microsoft Forefront Protection 2010 for Exchange Server

Microsoft Forefront Protection 2010 for SharePoint

Microsoft Forefront Online Protection for Exchange

Netzwerk (Edge)

Microsoft Forefront Threat Management Gateway

Lösungen von Drittanbietern

RSA SECURITY

Integration Microsoft-Infrastruktur

- Active Directory
- Netzwerk-zugriffsschutz (NAP)

Effizienz – IT/O – definiert

Because it's everybody's business

Forefront Protection Suite: Sicherheitstechnologien

Because it's everybody's business

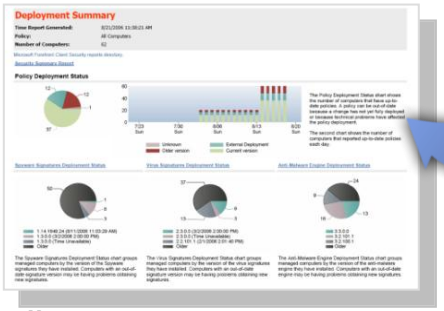
Microsoft Forefront

Effizienz – IEEU – definiert

Because it's everybody's business

Forefront Protection Manager

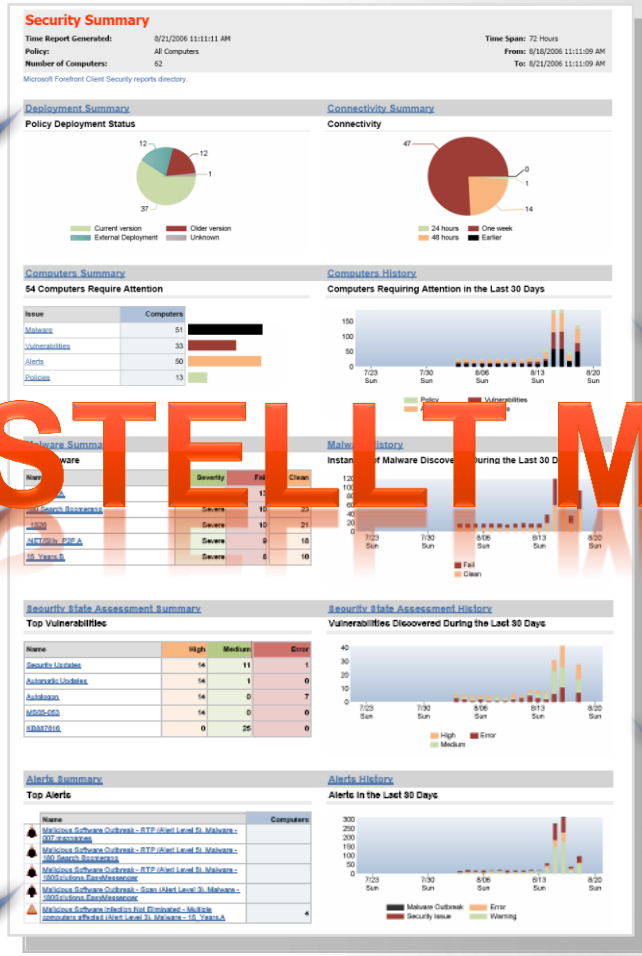
Zentrale Administration und umfangreiches Reporting



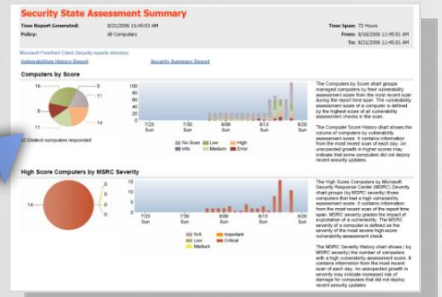
Übersicht Verteilung

Überblick Schadsoftware

Alarmierungen



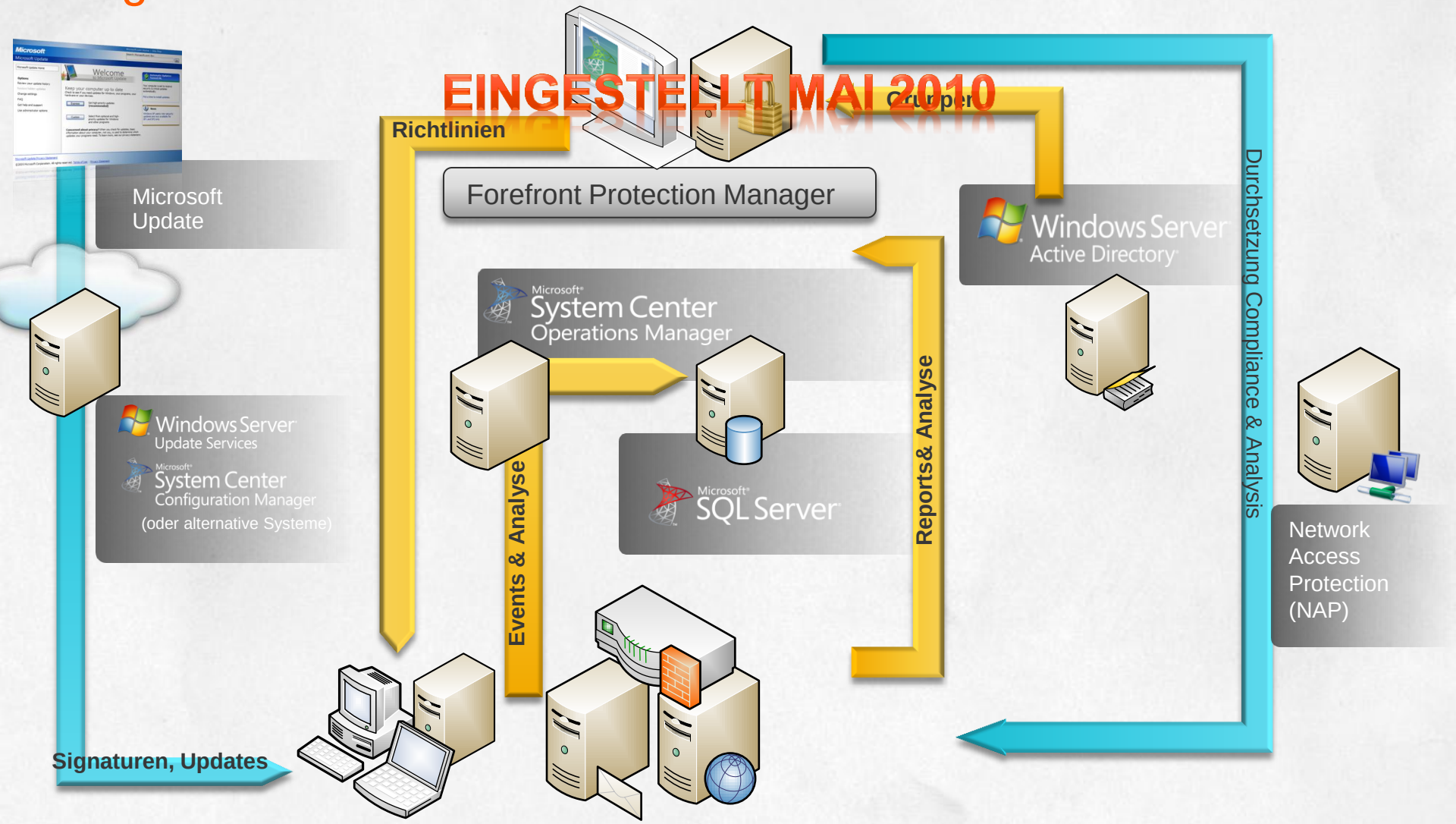
Übersicht Sicherheitsstatus Endgeräte



Gesamt-sicherheitsreport

Forefront Protection Suite

Integration in die Infrastruktur



Die Stärke mehrerer `Engines` nutzbar machen

Forefront Server Protection beinhaltet und nutzt fünf Antivirus-Engines führender Hersteller

Microsoft

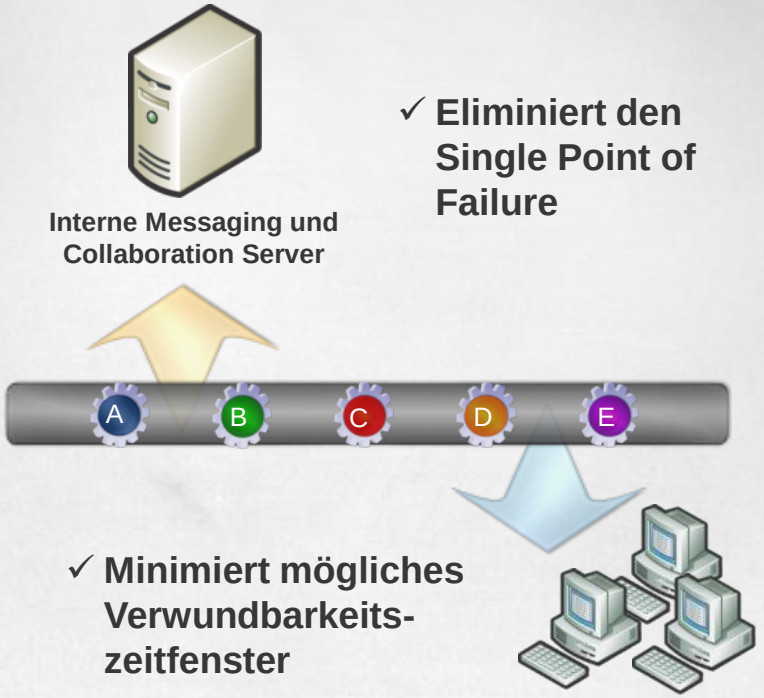
KASPERSKY lab

authentium

VirusBuster
www.virusbuster.hu

NORMAN
DATA DEFENSE SYSTEMS

Jeder Scan-Job bei Forefront Server Protection kann bis zu fünf Engines gleichzeitig verwenden



✓ **Eliminiert den Single Point of Failure**

✓ **Minimiert mögliches Verwundbarkeits-zeitfenster**

Forefront: Der Multi-Scan-Engine-Vorteil

- Schnelle Reaktion auf neue Bedrohungen
- Engines bieten gegenseites “Backup”
- Vorteil durch Unterschiedlichkeit der AV-Engines und Heuristiken

Weniger als 5 Stunden

5 bis 24 Stunden

Mehr als 24 Stunden

Reaktionszeit[1] (in Stunden)

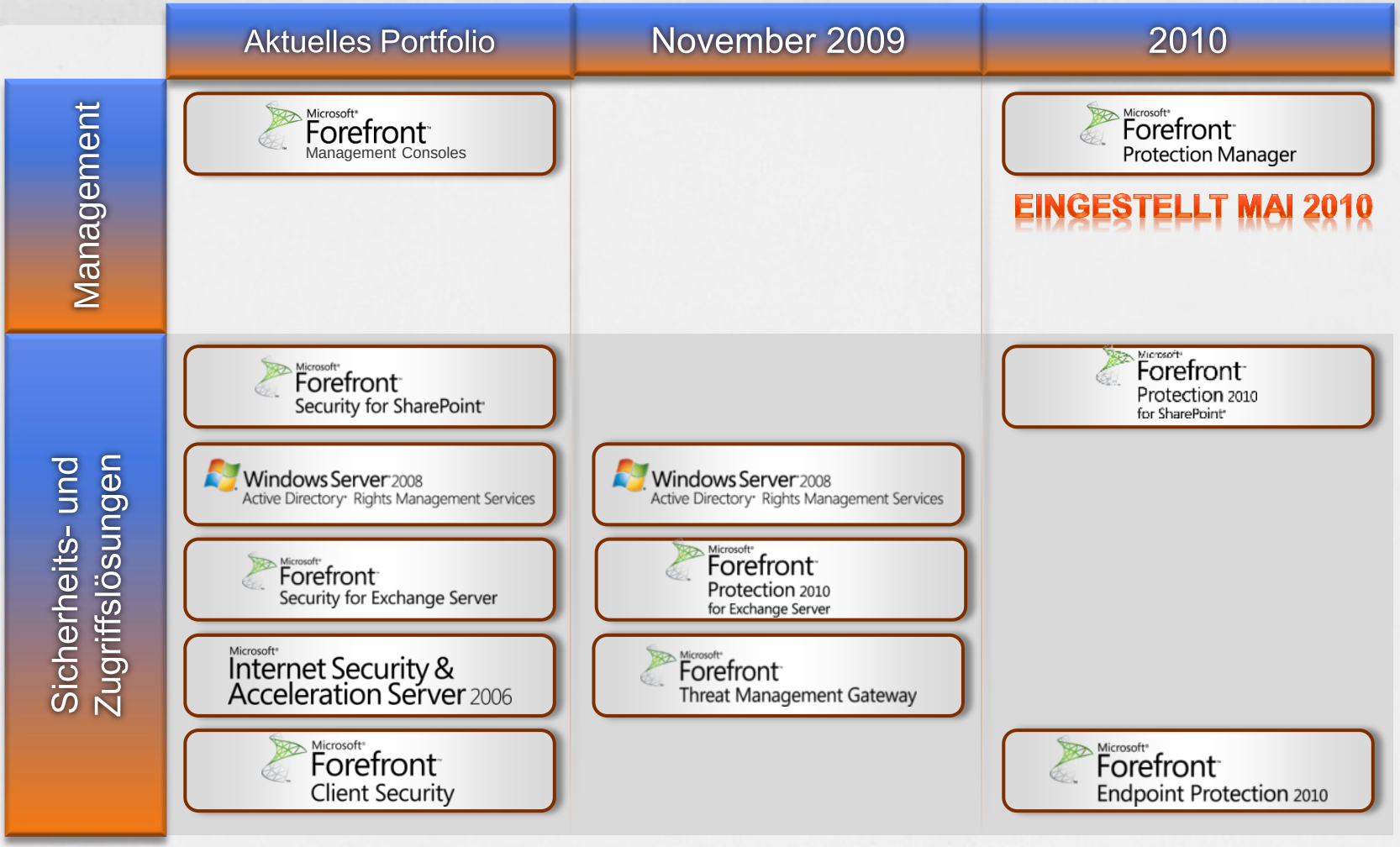
`Single-Engine` Lösung

WildList Number	Malware Name	Forefront Engines	Vendor A	Vendor B	Vendor C
01/09	autorun_itw542.ex_	0.00	1185.47	89.83	1161.83
01/09	buzus_itw3.ex_	0.00	2.92	10.87	53.98
01/09	conficker_itw5.dl_	0.00	0.00	113.55	0.00
01/09	koobface_itw18.ex_	0.00	360.65	0.00	1050.18
01/09	momibot_itw2.ex_	0.00	0.00	0.00	982.05
01/09	pinit_itw2.ex_	42.85	205.03	0.00	873.23
01/09	zbot_itw30.ex_	0.00	0.00	0.00	0.00
01/09	zbot_itw31.ex_	0.67	990.50	1.17	53.75
01/09	zbot_itw39.ex_	0.00	946.40	0.00	0.00
02/09	agent_itw94.ex_	0.00	0.00	204.17	723.10
02/09	autorun_itw580.ex_	0.00	341.37	917.60	336.67
02/09	autorun_itw585.ex_	0.00	602.93	0.00	0.00
02/09	autorun_itw594.ex_	0.00	704.05	0.00	42.40
02/09	magania_itw21.ex_	0.00	0.00	0.00	522.60
02/09	onlinegames_itw624.ex_	0.00	386.88	22.12	0.00
02/09	onlinegames_itw627.ex_	0.00	207.33	60.88	7.42
02/09	onlinegames_itw643.ex_	0.00	22.13	6.22	32.18
02/09	zbot_itw42.ex_	0.00	1120.87	0.00	0.00
03/09	autoit_itw90.ex_	0.00	0.00	0.00	1101.62
03/09	autorun_itw597.ex_	0.00	555.12	0.00	16.88
03/09	autorun_itw598.ex_	0.00	2.88	187.27	667.85
03/09	autorun_itw601.ex_	0.00	510.32	0.00	0.00
03/09	autorun_itw616.ex_	0.00	555.12	0.00	16.88
03/09	ircbot_itw485.ex_	0.00	3.37	0.37	79.05
03/09	mariof_itw2.ex_	0.00	309.40	945.95	653.03
03/09	onlinegames_itw651.ex_	0.00	0.00	145.48	55.47
03/09	zbot_itw43.ex_	0.00	757.28	0.00	0.00

** 0.00 denotes proactive detection

[1] Source: AV-Test.org 2009 (www.av-test.org)

Die Forefront Roadmap – Business Ready Security



bitte beachten: Änderungen vorbehalten

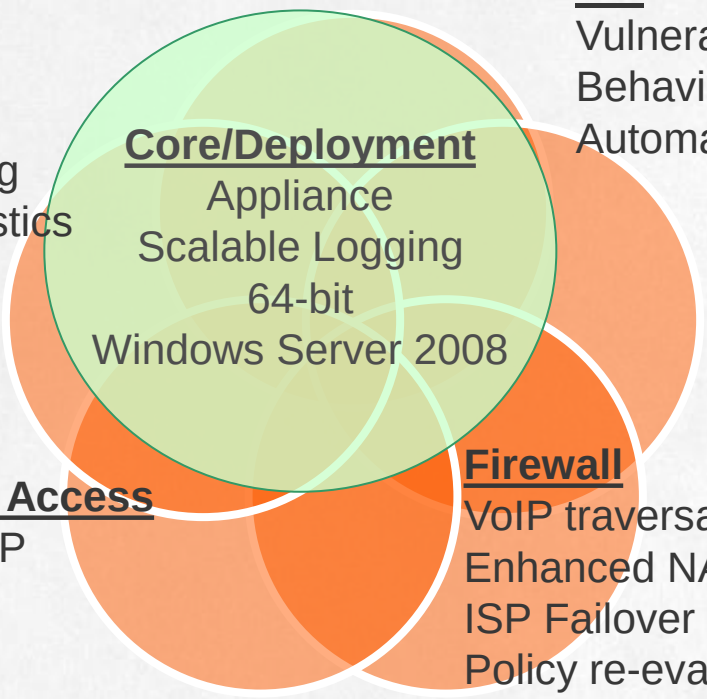
TMG 2010

Client Protection
HTTP Anti-virus/spyware
URL Filtering
HTTPS forward inspection
E-mail AV/AS

Subscription Services

IPS
Vulnerability Signatures
Behavior-based detection
Automated responses

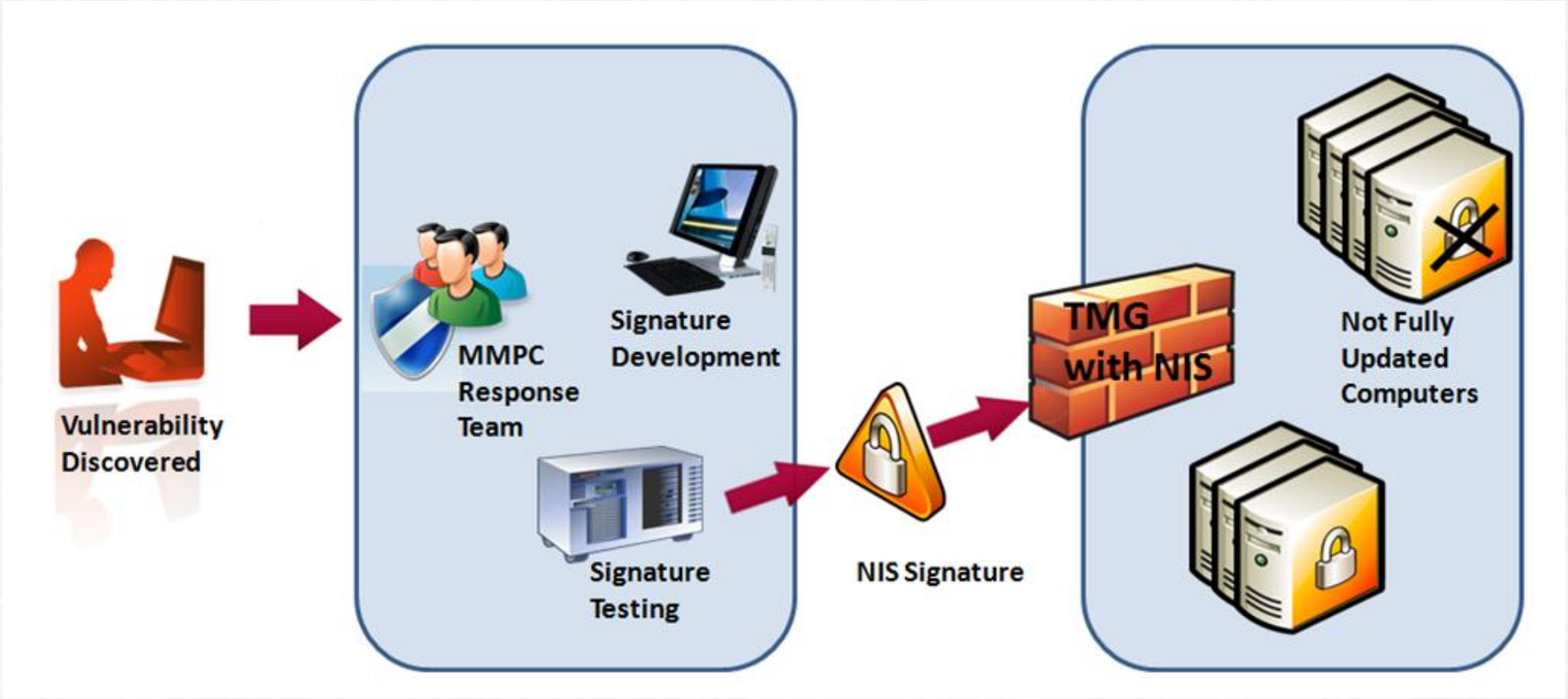
Management
EMS
Scenario Wizards
Enhanced reporting
Integrated Diagnostics



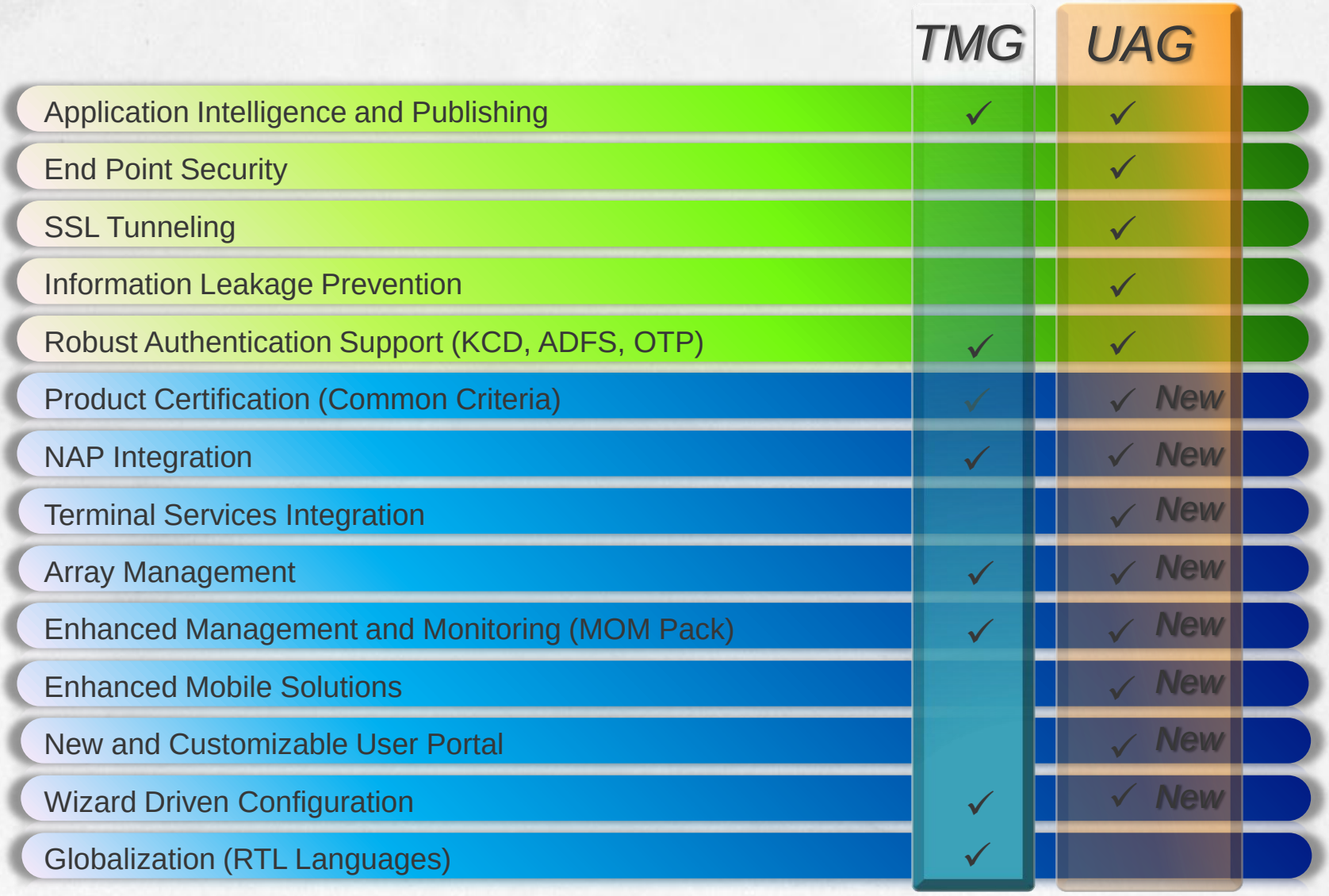
Remote Access
VPN/NAP
SSTP

Firewall
VoIP traversal (SIP)
Enhanced NAT
ISP Failover
Policy re-evaluation

Microsoft Forefront TMG - NIS

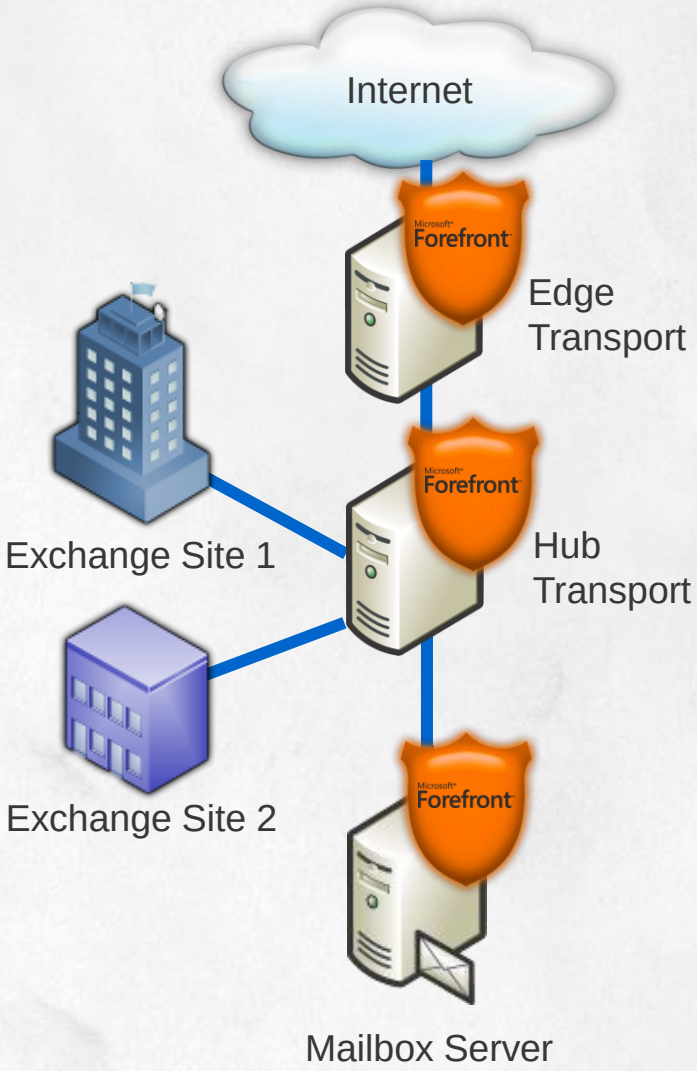


TMG versus UAG



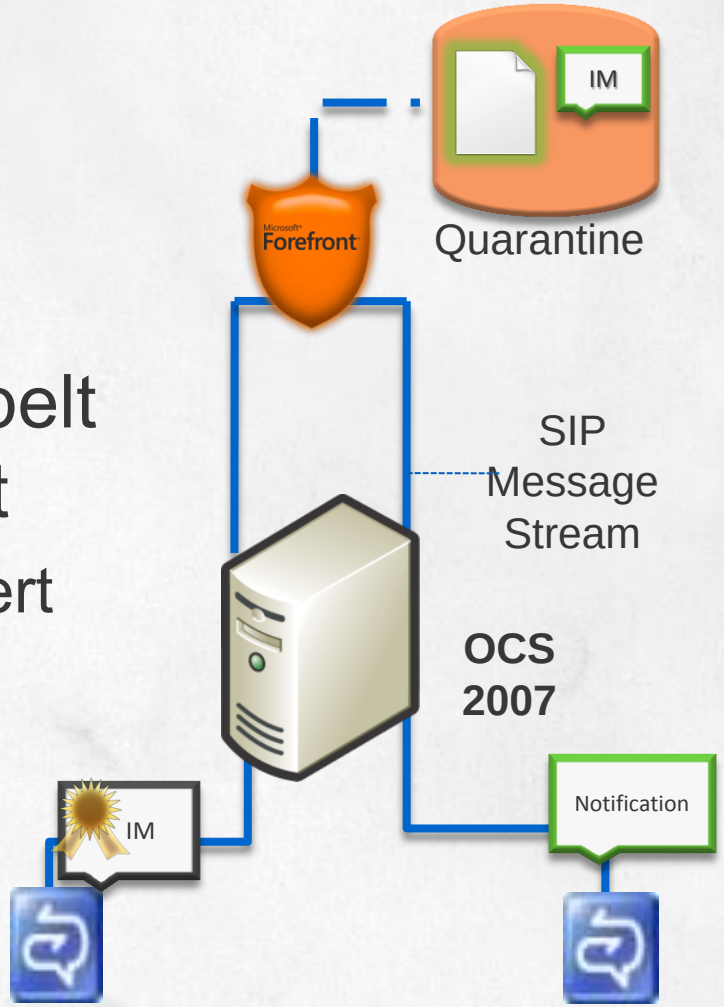
Forefront Security for Exchange Server

- Optimale Performance
  - Erkennung der Exchange-Rolle
  - AV-Stamping
  - Bias-Einstellung
- Maximale Sicherheit
  - Intelligentes Hintergrund-Scannen
  - Scan-On Scanner Update-Scanning
  - Proaktives Scanning
  - Echte Dateifiliterung
  - Premium-AntiSpam für Exchange



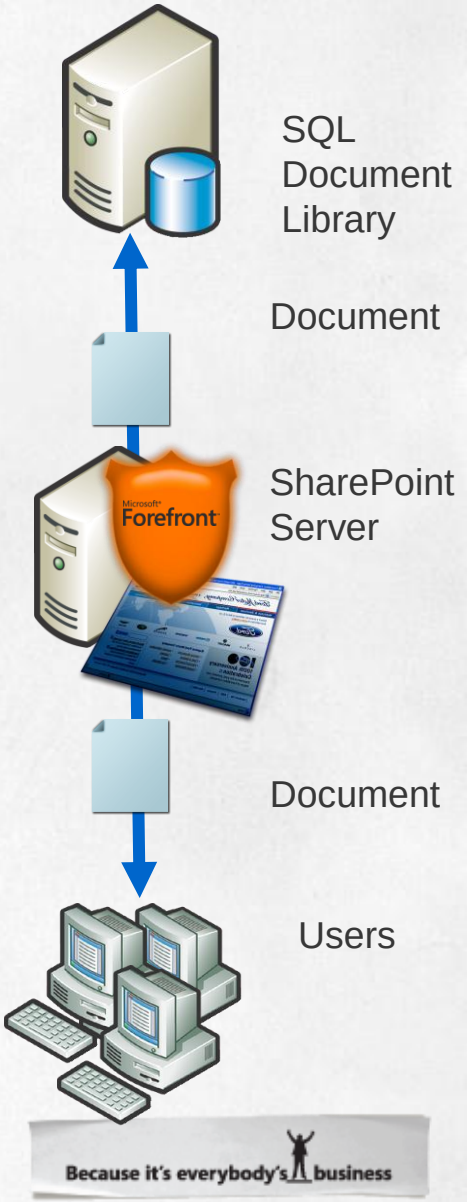
Forefront Security for OCS

- SIP-Nachrichtenstrom wird durch FSOCS geroutet
- Geprüfte Nachrichten und Filetransfers werden gestempelt und durch OCS weitergeleitet
  - Infizierte Dateien werden blockiert und/oder in Quarantäne gestellt
  - Benachrichtigung wird an den Administrator gesendet



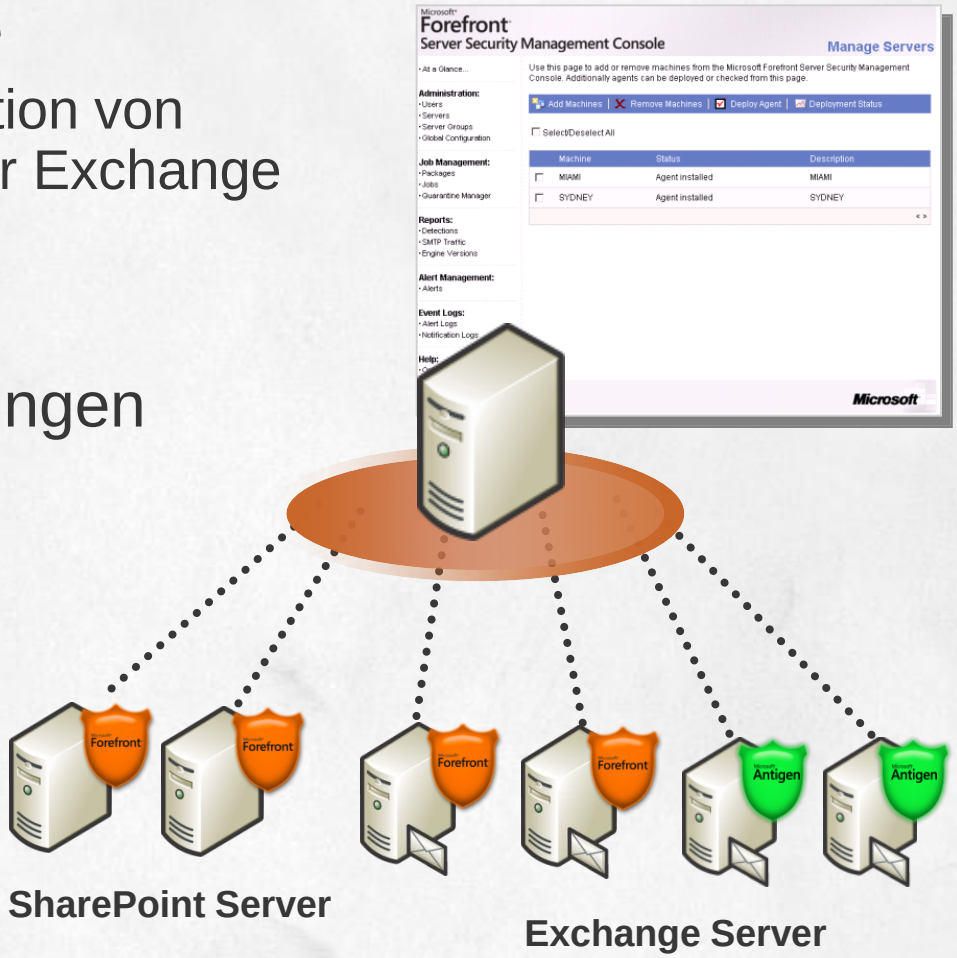
Forefront Security SharePoint Server

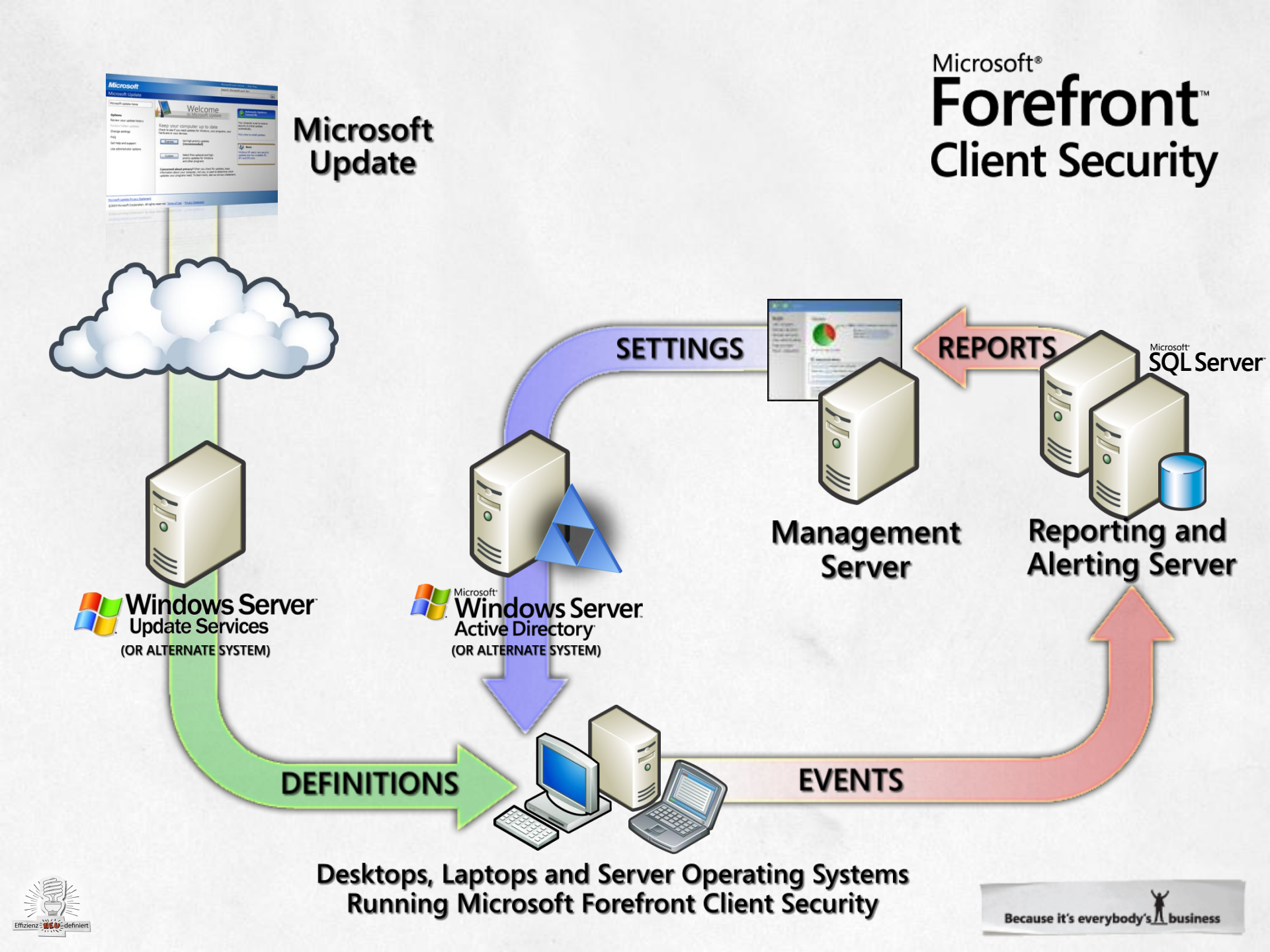
- Virenschutz für die Dokumenten-Bibliothek
  - Echtzeitschutz beim Up-und Download von Dokumenten in die SQL-Datenbank
  - Manuelle und zeitgesteuerte Scans
- Durchsetzen von inhaltlichen Richtlinien
  - Dateifilter können auf Basis von Dateinamen, Dateiendung und Dateityp angewendet werden
  - Filterung nach ungewollten Inhalten ist auch innerhalb von Dokumenten möglich



Forefront Server Security Management Console

- Zentrale Verwaltungskonsole
  - Bereitstellung und Konfiguration von Forefront/Antigen Security for Exchange und SharePoint Server
- Automatisiert die Aktualisierungen im gesamten Netzwerk
- Ermöglicht umfangreiches Reporting und Festlegung von Outbreak Alerts
- Erweiterungen mit SP1 erwartet (Multiserverbetrieb)



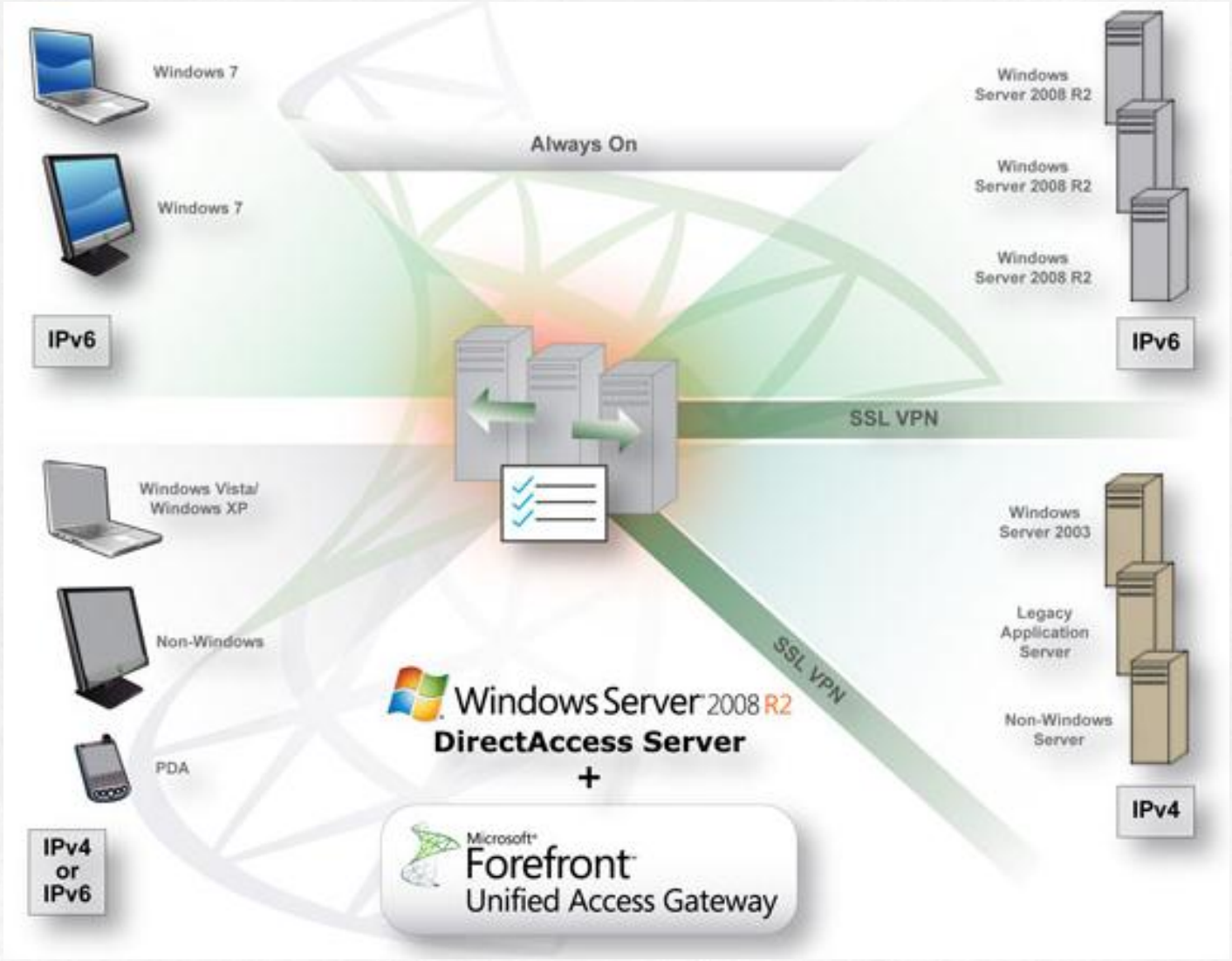

Microsoft Update
Microsoft® Forefront™ Client Security
SETTINGS
REPORTS
Microsoft SQL Server
Management Server
Reporting and Alerting Server
Windows Server Update Services
(OR ALTERNATE SYSTEM)
Microsoft Windows Server Active Directory
(OR ALTERNATE SYSTEM)
DEFINITIONS
EVENTS
Desktops, Laptops and Server Operating Systems
Running Microsoft Forefront Client Security
Effizienz – NEU – definiert
Because it's everybody's business

Forefront Client Security

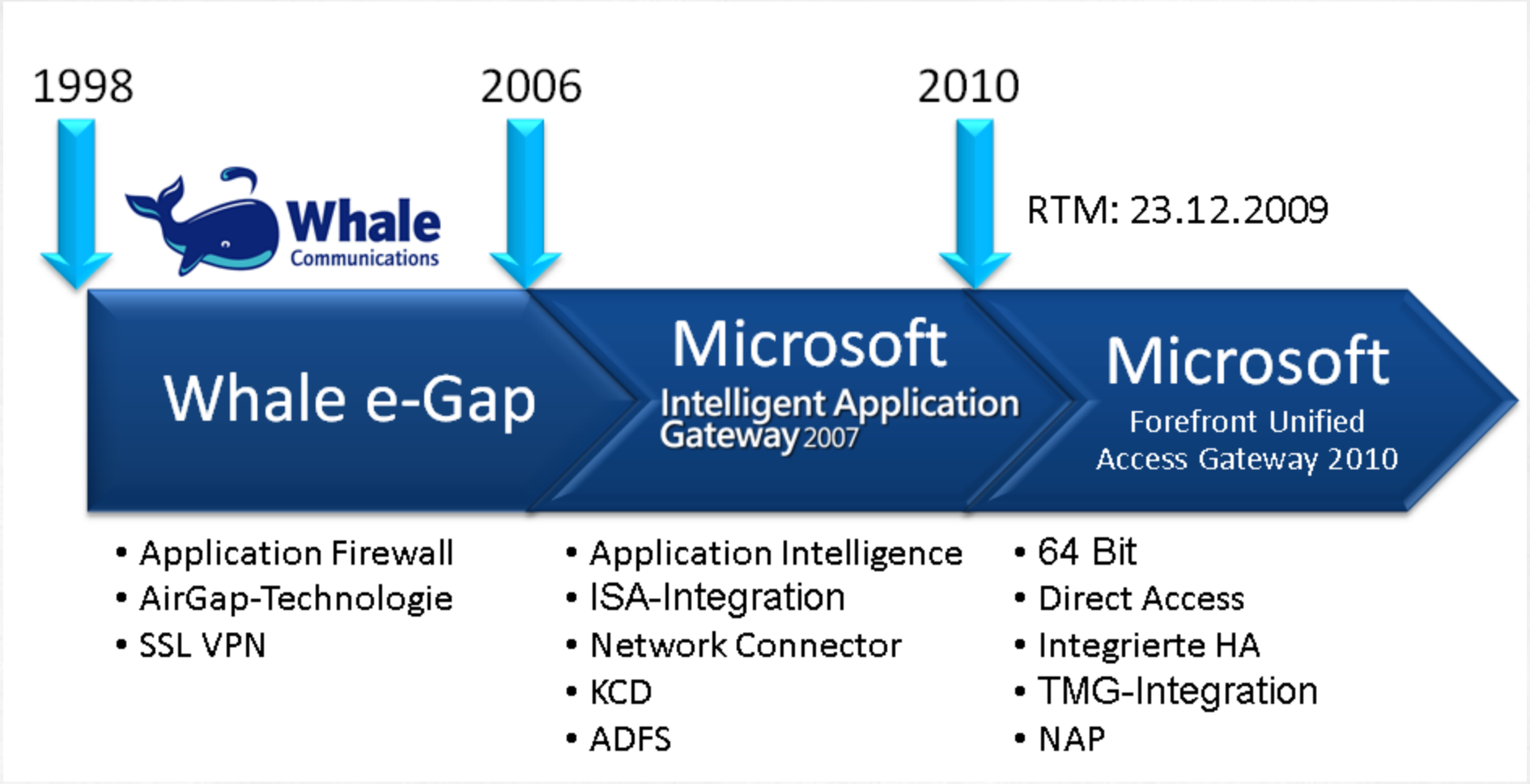
Anti-Malware-Schutz der Client- und Server-Betriebssysteme

Einheitlicher Schutz	Eine Lösung für Viren- und Spyware-Schutz Überwachung des Systemzustands Eigene Research- & Response-Zentren
Vereinfachte Verwaltung	Eine Konsole für einfache, zentrale Verwaltung Leichte Signatur- und Richtlinien-Verteilung Integriert sich in bestehende Infrastrukturen
Überblick & Kontrolle	Ein Cockpit bietet kompletten Überblick Aussagekräftige Berichte (z.B. täglich per Email) Stets auf dem aktuellen Stand &Trends sichbar

Forefront UAG



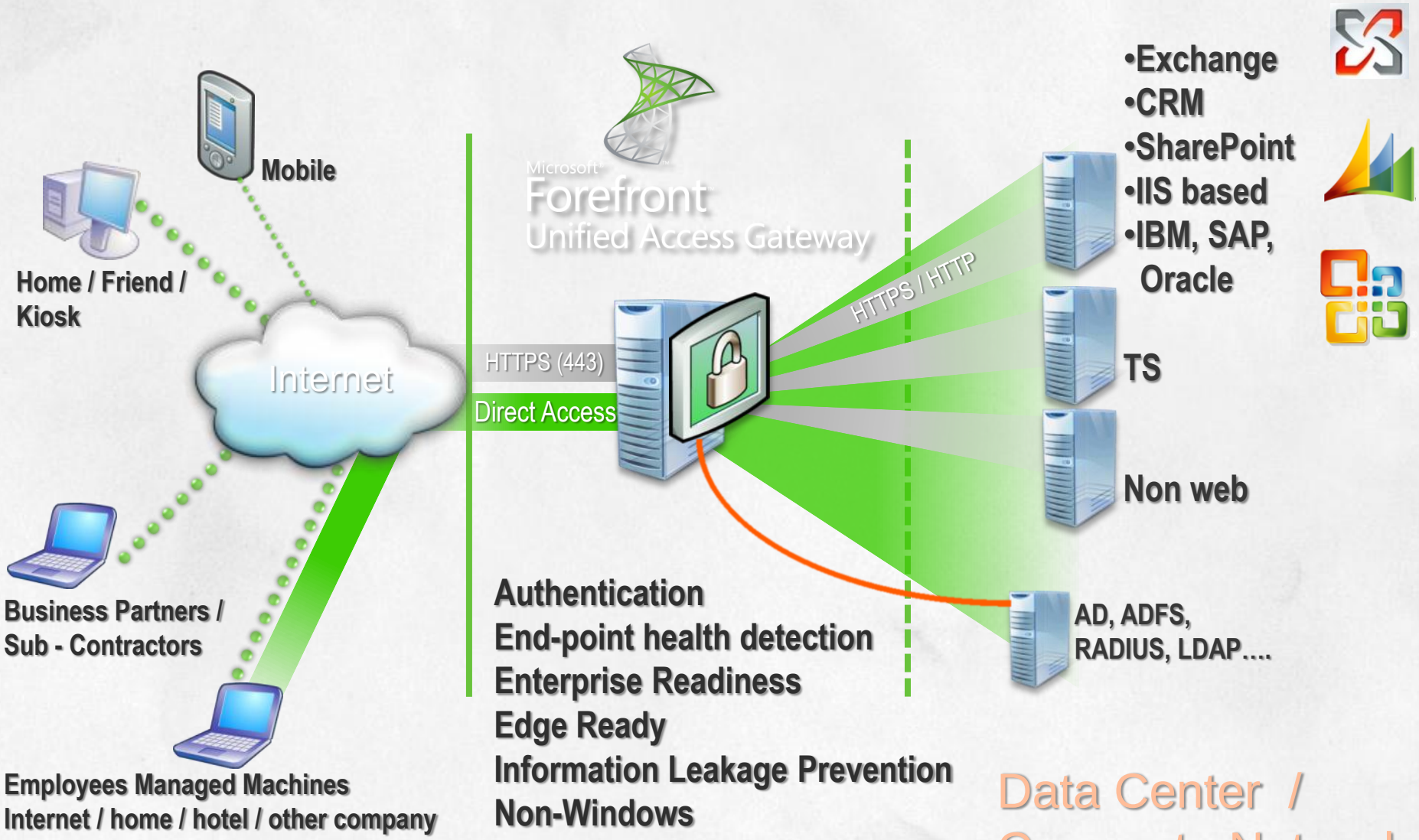
Forefront UAG



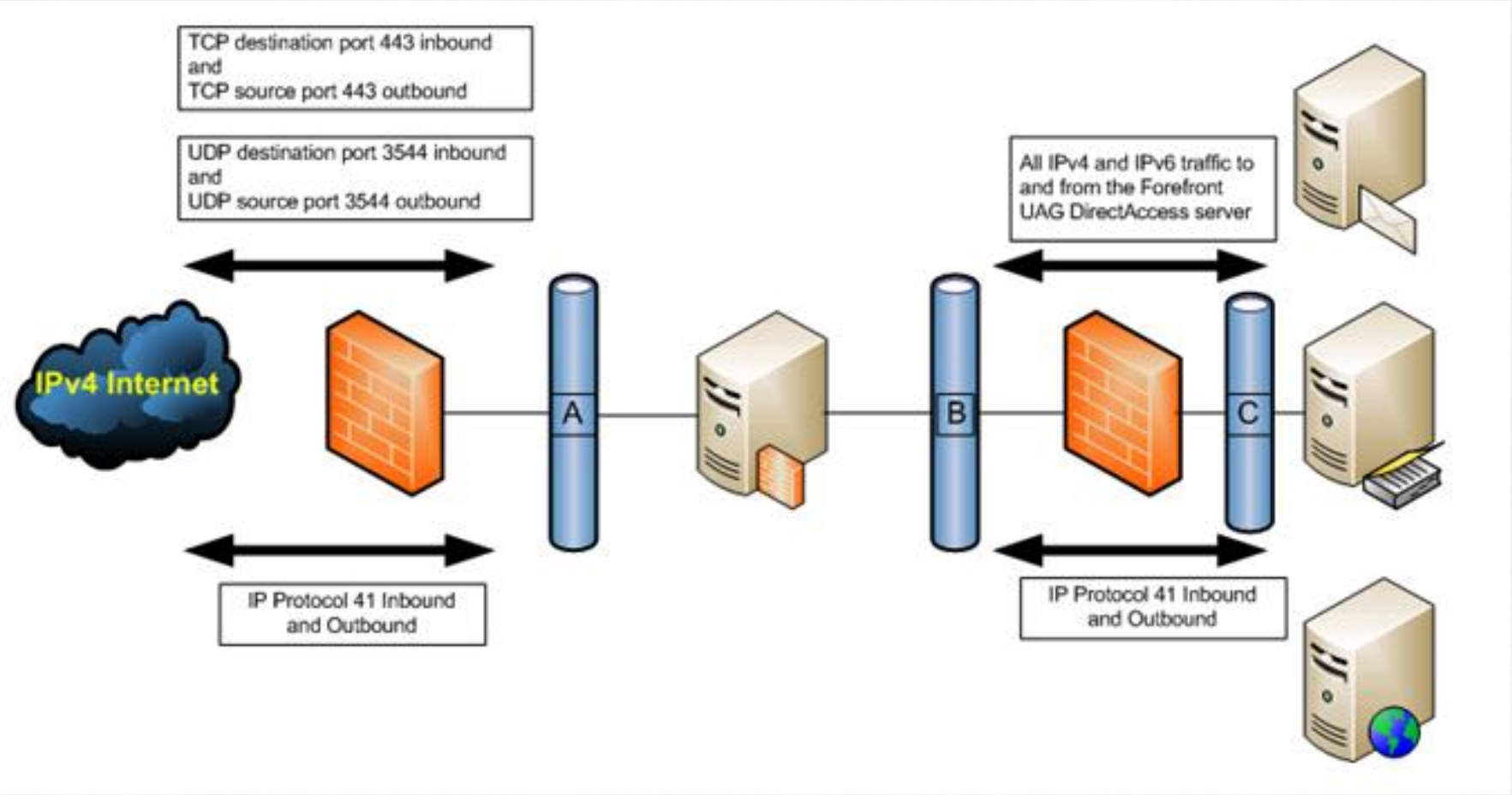
Forefront UAG im Ueberblick

- 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.

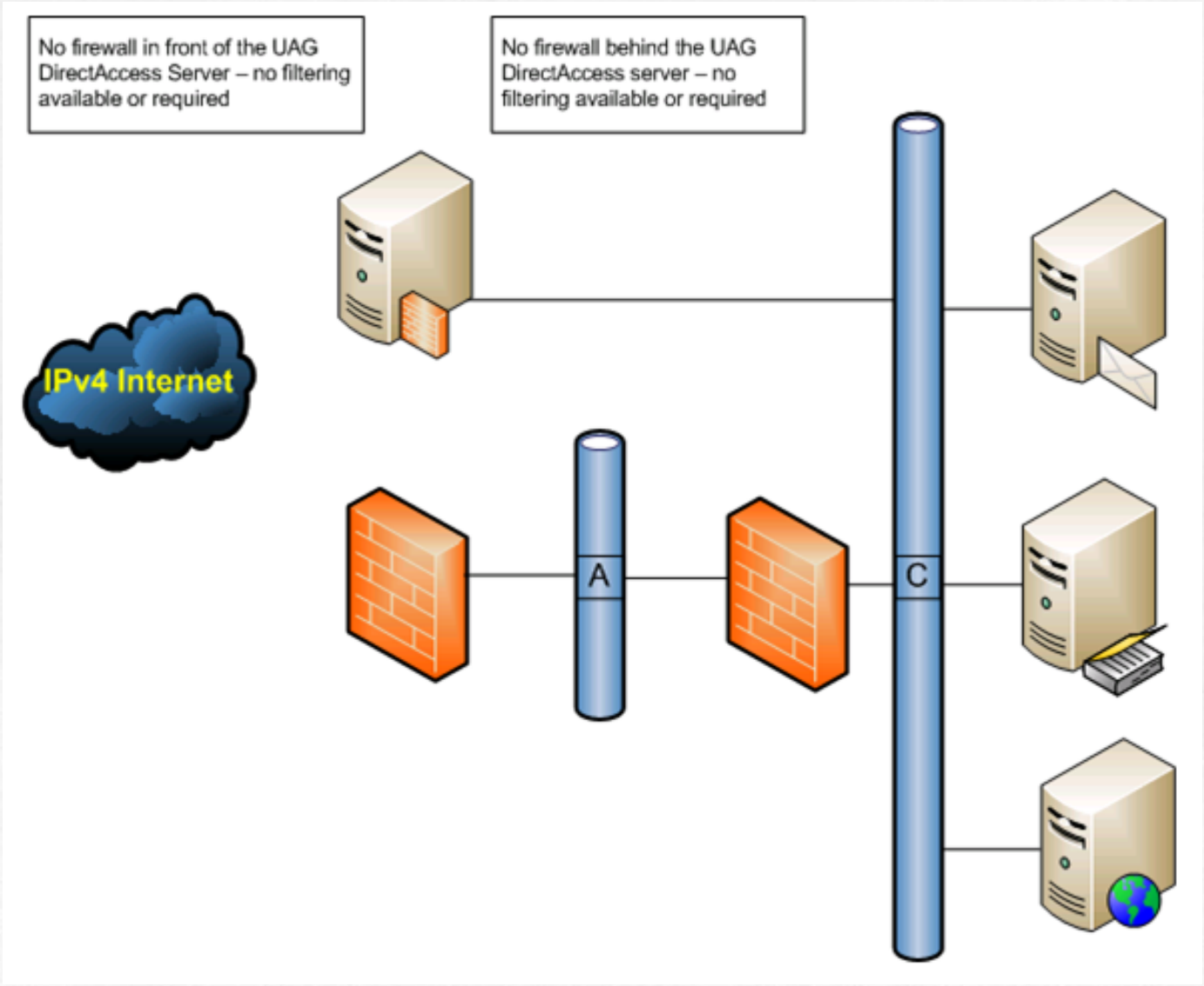
Forefront UAG im Ueberblick



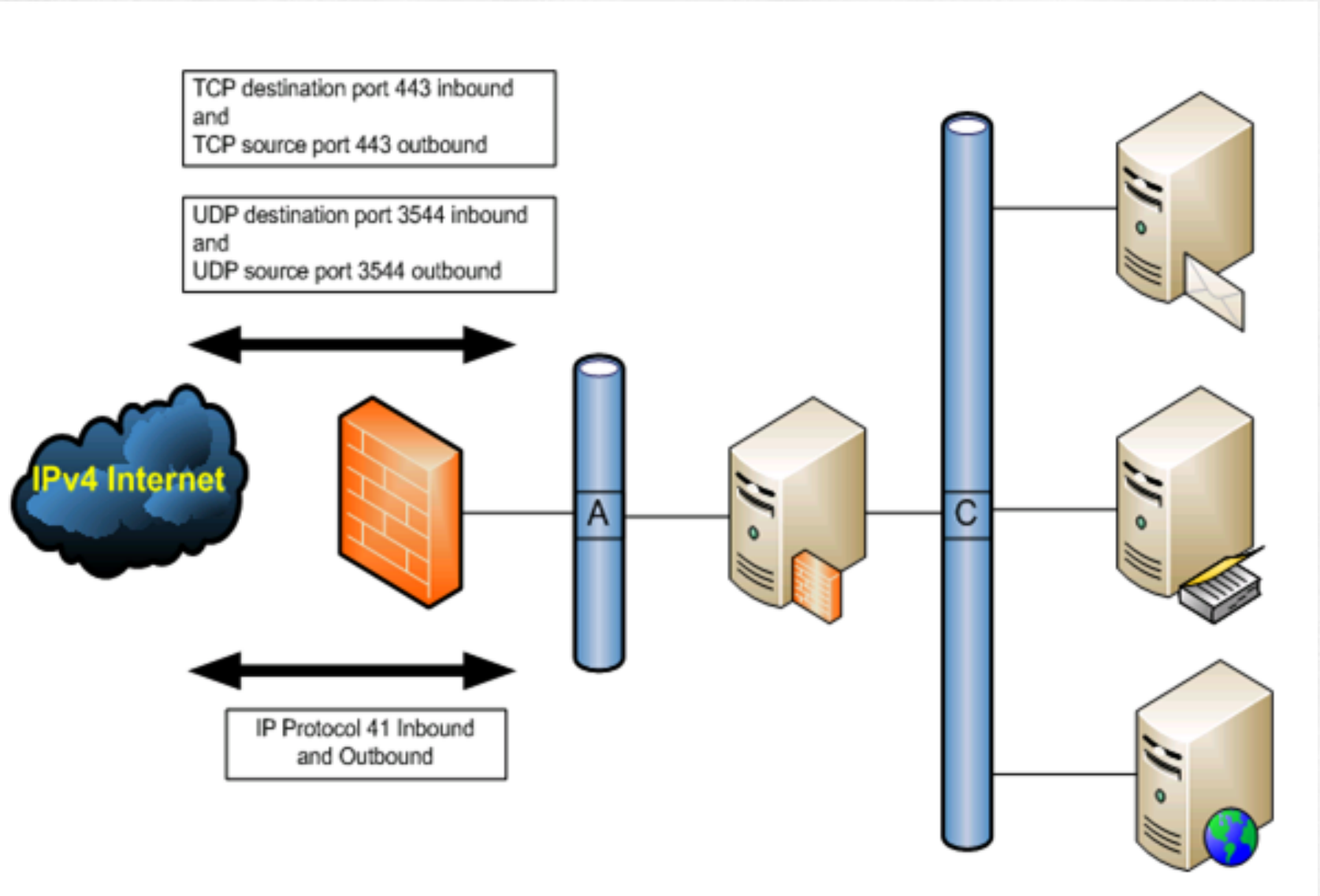
UAG Placement



UAG Placement



UAG Placement



Einschraenkungen von UAG im Zusammenspiel mit TMG

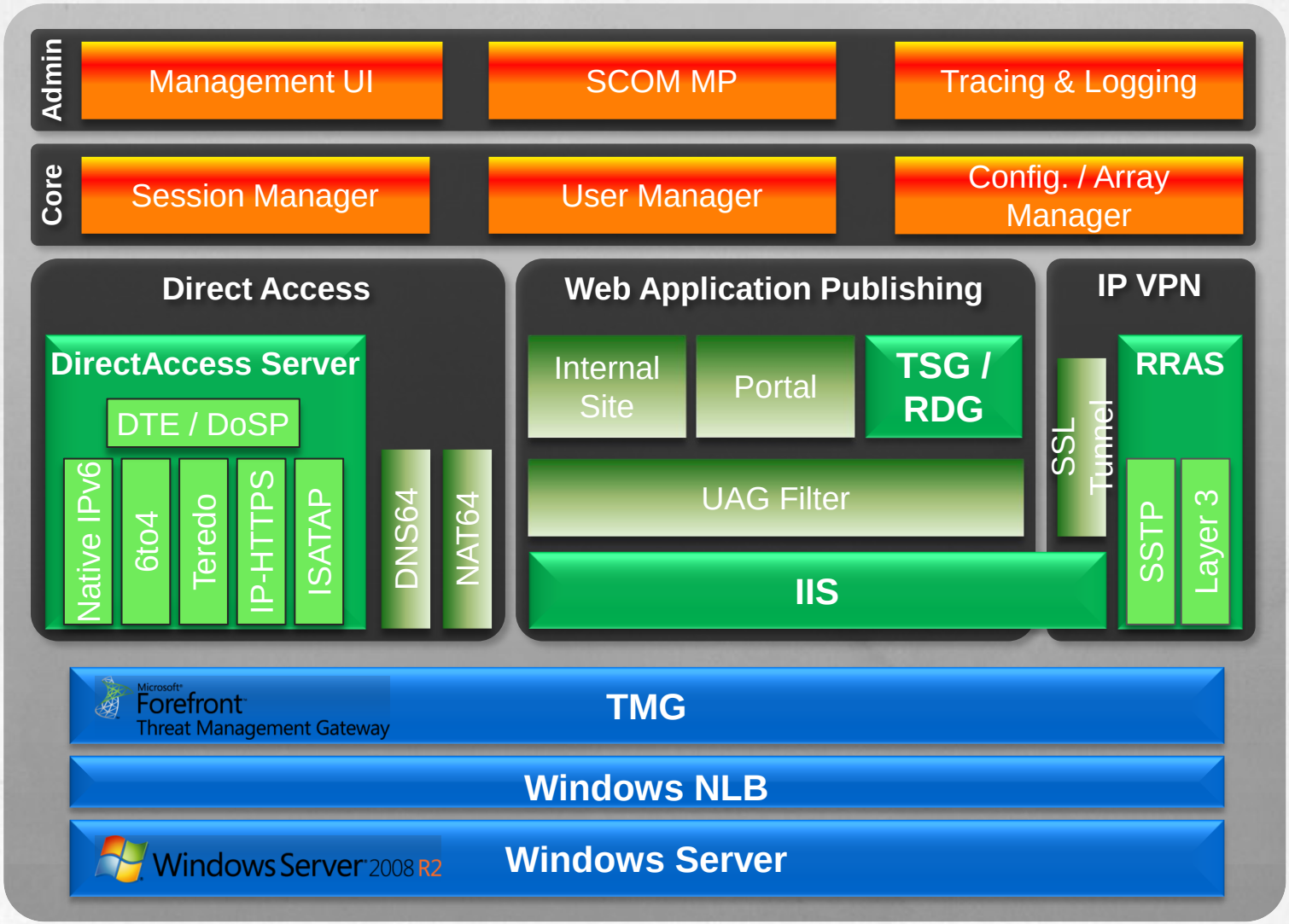
- Forefront TMG is installed automatically during Forefront UAG Setup, and removed automatically if Forefront UAG is uninstalled. Installing and uninstalling only Forefront TMG is not supported
- (YES) Forefront TMG as a forward proxy for outbound Internet access
- (YES) Forefront TMG application publishing, except for the publishing scenarios listed in the Supported Forefront TMG configurations section that follows
- (NOT) Forefront TMG as a site-to-site VPN
- (NOT) Forefront TMG as an intrusion protection system
- (NOT) Forefront TMG as a network perimeter firewall. Forefront TMG running on Forefront UAG is only intended to protect the Forefront UAG local host server
- (YES) Publishing Forefront TMG via Forefront UAG

Support boundaries
http://technet.microsoft.com/en-us/library/ee522953.aspx

Supported Configuration TMG und UAG

- Monitoring with the Forefront TMG Management console.
- Limiting users, groups, sources and destinations on Forefront TMG system policy rules, with the purpose of enabling access to corporate servers and remote management to and from the Forefront UAG local host server.
- You can publish the following applications via Forefront TMG:
    - Exchange SMTP/SMTPS
    - Exchange POP3/POP3S
    - Exchange IMAP/IMAPS
    - Office Communications Server (OCS)

Forefront UAG Architektur



Forefront UAG Systemanforderungen

- 2,66 Ghz Dual Core Prozessor oder schneller
- 4 GB RAM
- 30 GB HD freier Platz
- 2 Netzwerkkarten (3 empfohlen fuer Intraarray Traffic)
- Windows Server 2008 R2
- Forefront TMG wird waehrend der UAG Installation installiert
- Installation als Child Partition in Hyper-V ist supported

Forefront UAG Installation

Windows Server 2008 R2
Alle Windows Patches
UAG
UAG Update 1
Folgende NLB Updates
    KB977342
    KB980674
    KB980374 (wenn nicht TMG SP1)
TMG SP1
UAG „Getting Started Wizard“
UAG Array bauen
NLB aktivieren

Forefront UAG Update 1

- Remote Desktop access from Windows Vista and Windows XP: Client endpoints running Windows Vista and Windows XP can now access RemoteApps and Remote Desktops published through Forefront UAG
- Support for Microsoft SharePoint Server 2010
- Forefront UAG now supports the Office Forms Based Authentication protocol
- Forefront UAG now supports the use of site cookies for non-alternate access mapping applications, in addition to domain cookies.
- Forefront UAG now supports CustomUpdate files up to 1.5 GB in size.
- Changes in Group Policy Object (GPO) provisioning for DirectAccess clients: Update 1 fixes an issue that caused the export script that creates GPO objects to fail, and an issue that caused the GPO to be applied to all authenticated users in the domain (including computer accounts), instead of to DirectAccess clients only.
- Forefront UAG help - A new help file (UAG_Help.chm) is provided for Forefront UAG Update 1. To update the help file on the Forefront UAG server, download the UAG_Help.chm file and save it in the …\Microsoft Forefront Unified Access Gateway\common\help folder

UAG und TMG Best Practice Analyzer

Microsoft Forefront Unified Access Gateway (UAG) 2010 Best Practices Analyzer Tool
http://www.microsoft.com/downloads/details.aspx?FamilyID=d24994ef-8670-4324-957a-805d35f1244e&displayLang=en
Microsoft Forefront Threat Management Gateway Best Practices Analyzer Tool
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=8aa01cb0-da96-46d9-a50a-b245e47e6b8b

Zertifikatgrundlagen

Anwendungsbereiche

- Verschluesselung von Webseiten mittels SSL
- Verschluesselung von Daten über einen IPSec-VPN-Tunnel
- Authentifizierung von Benutzern und Geraeten
- Smartcard-Anmeldung
- Netzwerkzugriffssteuerung mit 802.1x
- Verschlüsselung von Dateien auf Datentraegern mit EFS
- Signierung von Dateien und Softwarecode
- Gesicherte E-Mail-Kommunikation mit S/MIME

Was ist eine PKI?

Als Public-Key-Infrastruktur (PKI, engl.: public key infrastructure) bezeichnet man in der Kryptologie und Kryptografie ein System, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Die innerhalb einer PKI ausgestellten Zertifikate sind meist auf Personen oder Maschinen festgelegt und werden zur Absicherung computergestützter Kommunikation verwendet.

Quelle: http://de.wikipedia.org/wiki/PKI

Bestandteile einer PKI

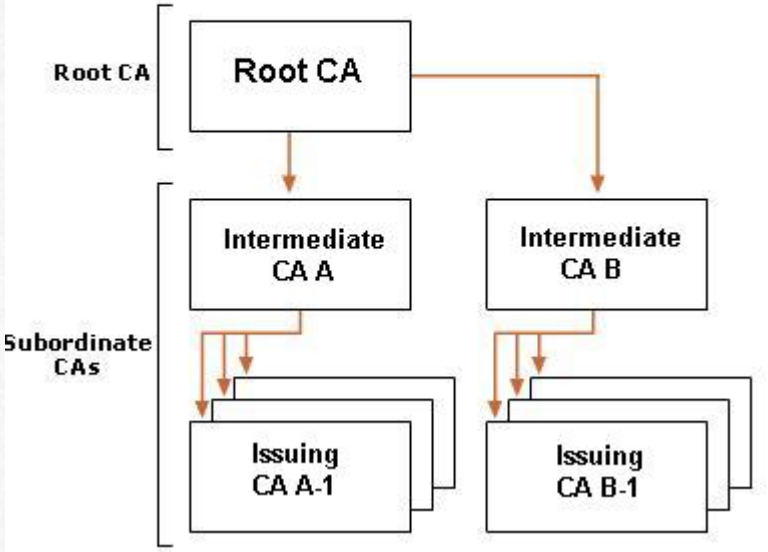
Wesentliche Bestandteile einer (minimalen) PKI sind:

Digitale Zertifikate:
Digital signierte elektronische Daten, die sich zum Nachweis der Echtheit von Objekten verwenden lassen.
Certification Authority:
Organisation, welche die Bereitstellung von Zertifikaten übernimmt.
Registration Authority:
Organisation, bei der Personen und Maschinen Zertifikate beantragen können.
Certificate Revocation Lists:
(Sperrliste) Listen mit zurückgezogenen, abgelaufenen und für ungültig erklärten Zertifikaten.
Verzeichnisdienst:
Ein durchsuchbares Verzeichnis welches ausgestellte Zertifikate enthält, meist ein LDAP-Server, seltener ein X.500-Server.
Validierungsdienst:
Ein Dienst, der die Überprüfung von Zertifikaten in Echtzeit ermöglicht.

Zertifikatgrundlagen

Schlüssel	Beschreibung
PCKS #12	Privater Informationsaustausch
.PFX	Privater Informationsaustausch
.P12	Privater Informationsaustausch
PCKS #7	Syntaxstandard kryptografischer Meldungen
.P7B	Syntaxstandard kryptografischer Meldungen
.SST	Microsoft serieller Zertifikatsspeicher
.CER	DER-kodiert-binär X.509 Base-64-codiert-X.509
.PFX	Privater Informationsaustausch PCKS #12
.CRL	Certification Revocation List
.P7C	Digitale ID-Datei
.P7M	PCKS #7 MIME-Nachricht
.P7R	PCKS #7 Zertifikat
.P7S	PCKS #7 Signatur

- RootCA
- IntermediateCA
- IssuingCA



Zertifikatgrundlagen

Zertifizierungsstelle
Stellt die Basisfunktionen einer Zertifizierungsstelle zur Verfügung.
Zertifizierungsstellen-Webregistrierung
Dieser Rollendienst stellt eine Weboberfläche zur Verfügung, über die Zertifikate von der Zertifizierungsstelle beantragt werden können.
Online-Responder
Ueber diesen Rollendienst wird die Funktion der Online-Prüfung von Zertifikaten mit dem Protokoll OCSP bereit gestellt
Registrierungsdienst für Netzwerkgeräte
Netzwerkkomponenten, wie zum Beispiel eine Cisco ASA 5505, können über diesen Rollendienst direkt ein Zertifikat von der Zertifizierungsstelle anfordern. Notwendig ist dieser Rollendienst vor allen, wenn die Netzwerkkomponenten nur über eine Kommandozeile (CLI) konfiguriert werden können. Für diesen Rollendienst ist die Enterprise Edition von Windows Server 2008 notwendig.
Webdienst für Zertifikatsregistrierung
Dieser Rollendienst ermöglicht es Benutzern und Computern die nicht Mitglied der Domäne sind oder sich derzeit in einem anderen Netzwerk befinden trotzdem Zertifikate zu beantragen beziehungsweise zu erneuern. Dieser Rollendienst erfordert zusätzlich den Rollendienst Webdienst für Zertifikatsregistrierungsrichtlinie.
Webdienst für Zertifikatsregistrierungsrichtlinie
Über diesen Rollendienst werden die Richtlinien zur Beantragung oder Erneuerung von Zertifikaten für Benutzer und Computer die nicht Mitglied der Domäne sind oder die sich aktuell in einem anderen Netzwerk befinden vergeben. Dieser Rollendienst erfordert zusätzlich den Rollendienst Webdienst für Zertifikatsregistrierung.

Zertifikatgrundlagen

Zertifkattypen

Normal (Single)
- webmail.trainer.de

Wildcard (*.domain.tld)
- *.trainer.de

SAN (Ein Zertifikat mit mehreren alternativen Namen (CN = Common Name))
- webmail.trainer.de
- owa.trainer.de
- UAG.trainer.intern
- autodiscover.trainer.intern
- autodiscover.trainer.de

Forefront UAG Auth. Support

- Active Directory
- LDAP
- TACACS
- RADIUS
- RSA
- KCD
- FBA
- Smart Card
- Certificates
- uvm. …

UAG Endpoint Security

- Installation bei Portal Aufruf (Online)
- Offlinekomponente verfuegbar
  - Keine ActiveX Install Permission (aber Admin User)
  - Installation File fuer Non Admin User (Inst. Durch Admin)
- Endpoint Session Cleanup
- Endpoint detection
- SSL Application Tunneling
- Socket Forwarding
- SSL Network Tunneling (Network Connector)
- SSL Network Tunneling (SSTP)
- Endpoint Quarantine Enforcement
- Clients
  - Mac OS 10.4+, Linux 32 Bit (RPM), Iphone 3.0
  - Windows Mobile 5+, Diverse Nokia
  - Windows XP-Windows 7 (Vista+7 = 64 Bit
  - Windows Server 2008 R2
- Verschiedene Sprachen (DE, EN, FR, IT usw.)
- Browser
  - Internet Explorer (6+), Firefox (3+), Safari (3.2+)
- Quelle: http://technet.microsoft.com/en-us/library/dd920232.aspx

UAG Endpoint Security

Endpoint Component Manager component

Downloads, installs, manages, and removes all the endpoint components. ActiveX and Java Applet.

Endpoint Session Cleanup component

Bereinigt alle lokal gespeicherten Daten (Coockies, Applikationsdaten, Offline Folder etc.)

Endpoint Detection

Stellt das NAP Enforcement und Compliance sicher

SSL Application Tunneling component

ActiveX and Java Applet. The Java applet provides SSL tunneling functionality only, and does not enable any of the other feature that are enabled by the endpoint components, such as client endpoint detection, Endpoint Session Cleanup, Socket Forwarding, or SSL Network Tunneling

Socket Forwarding component

Application aware (Allow and Block Lists)

Winsock2 Layered Service Provider (LSP) and Name Service Provider (NSP).

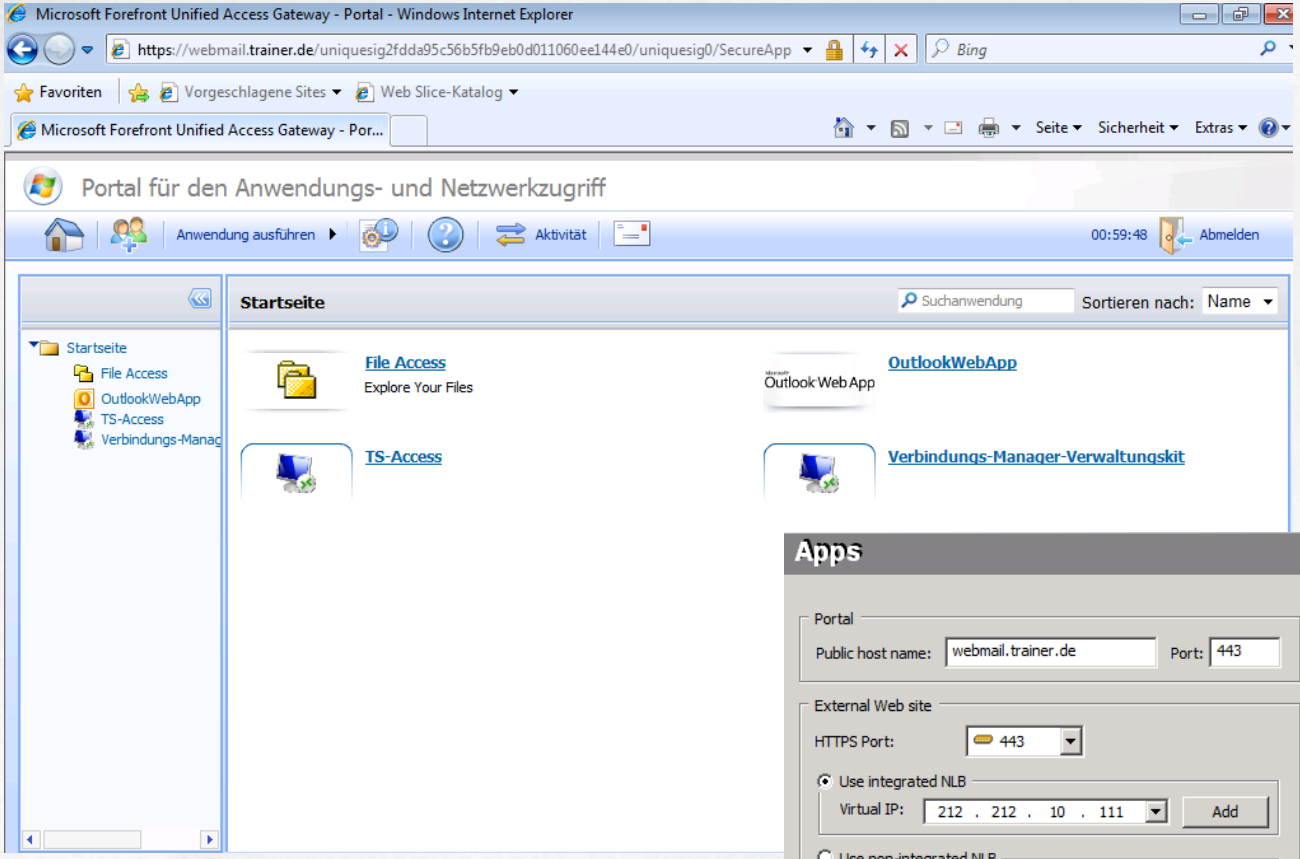
SSL Network Tunneling component

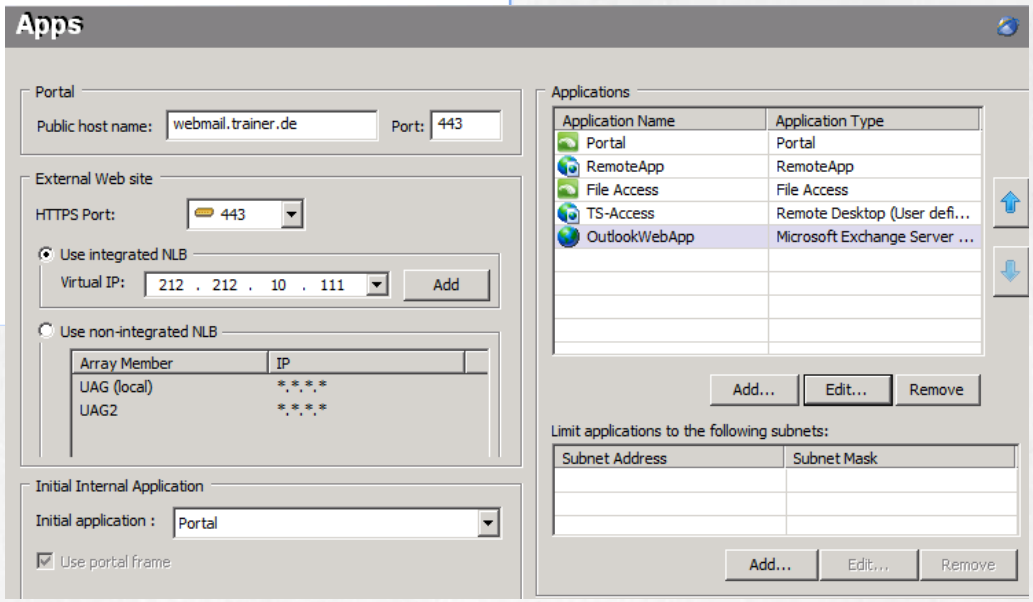
SSL Tunneling (UAG Network Connector (32 Bit OS) oder SSTP (64 Bit)

Socket Forwarding Helper component

Used for support purposes.

UAG Portalloesungen





Remote Desktop Services Publishing

RemoteApp

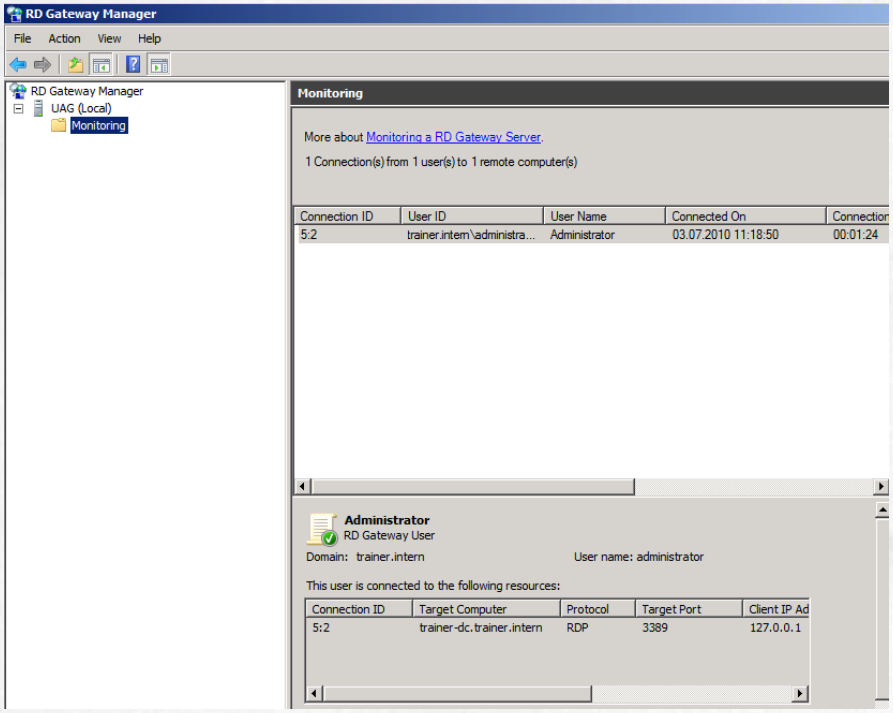
- Import TSPUB File vom RD Session Host

RemoteDesktop

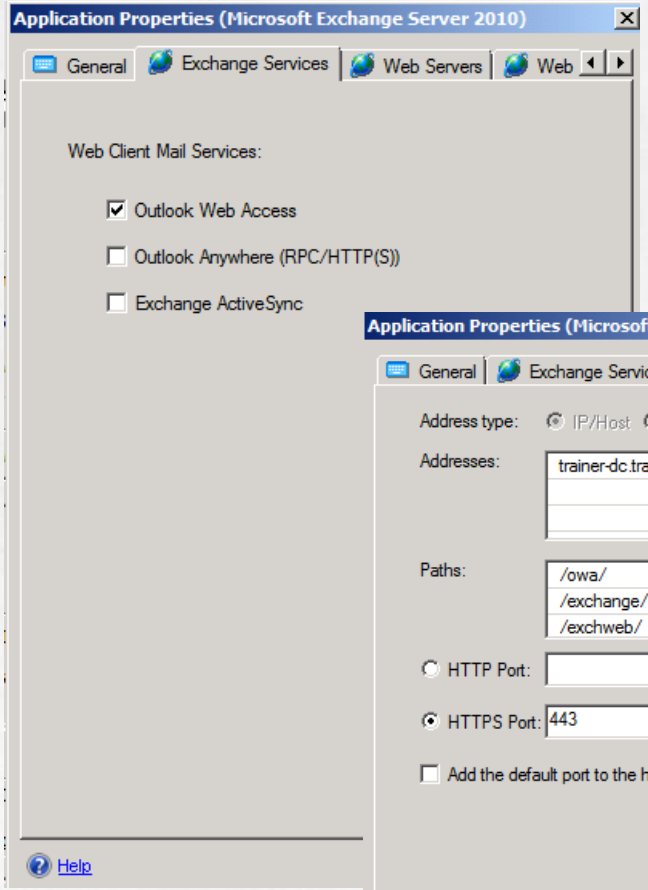
- UAG fungiert als RD Gateway

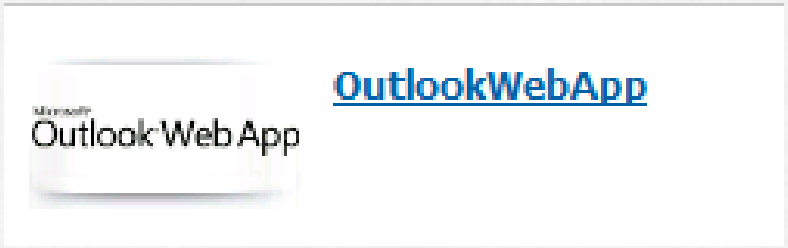
TS Client Tunneling

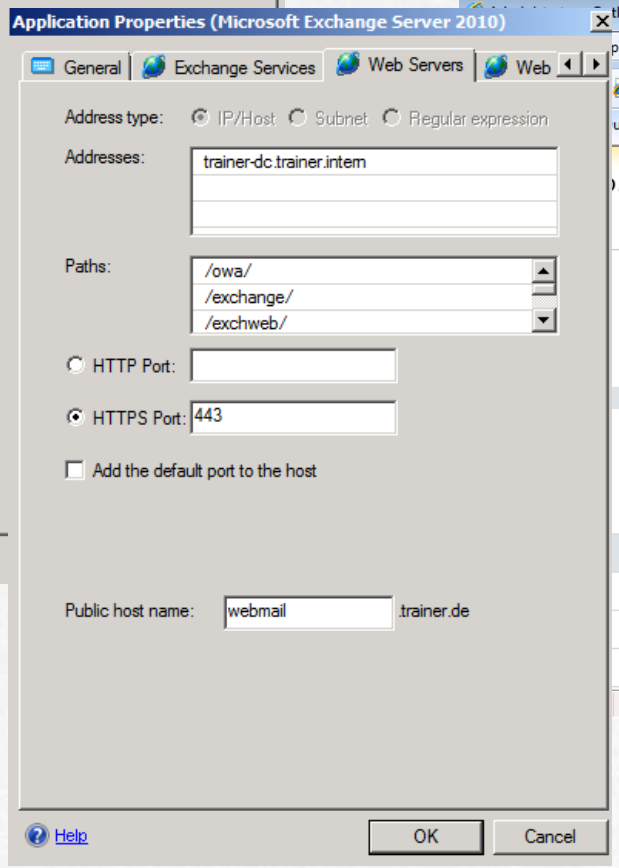
TS Web Client Tunneling

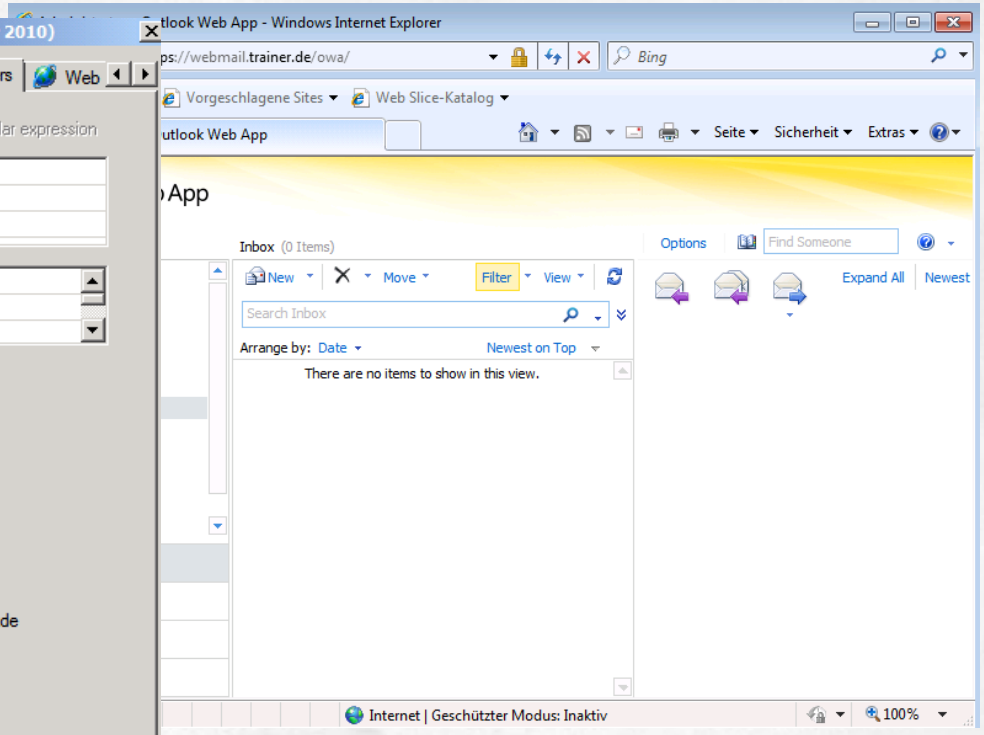


Exchange Publishing

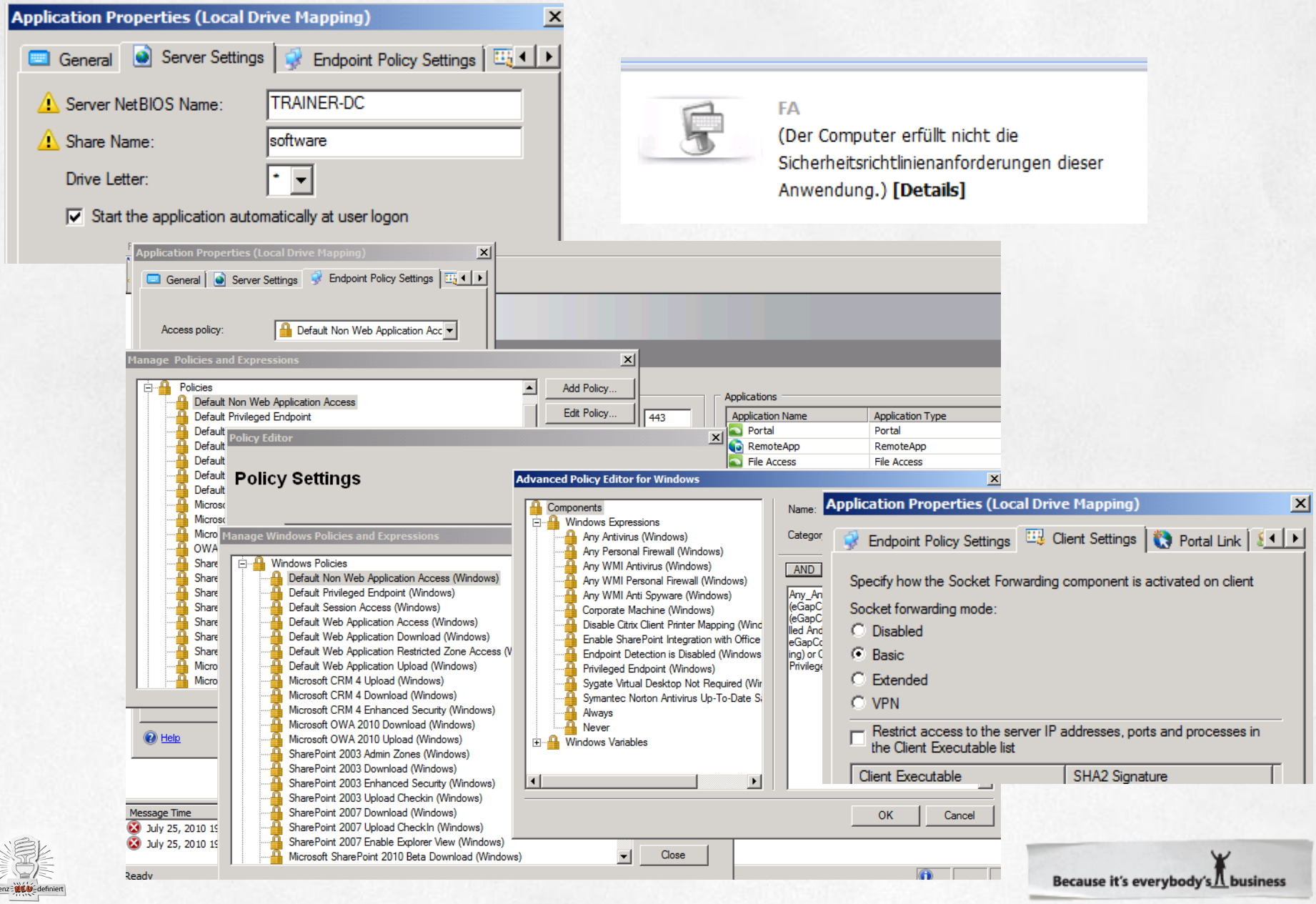








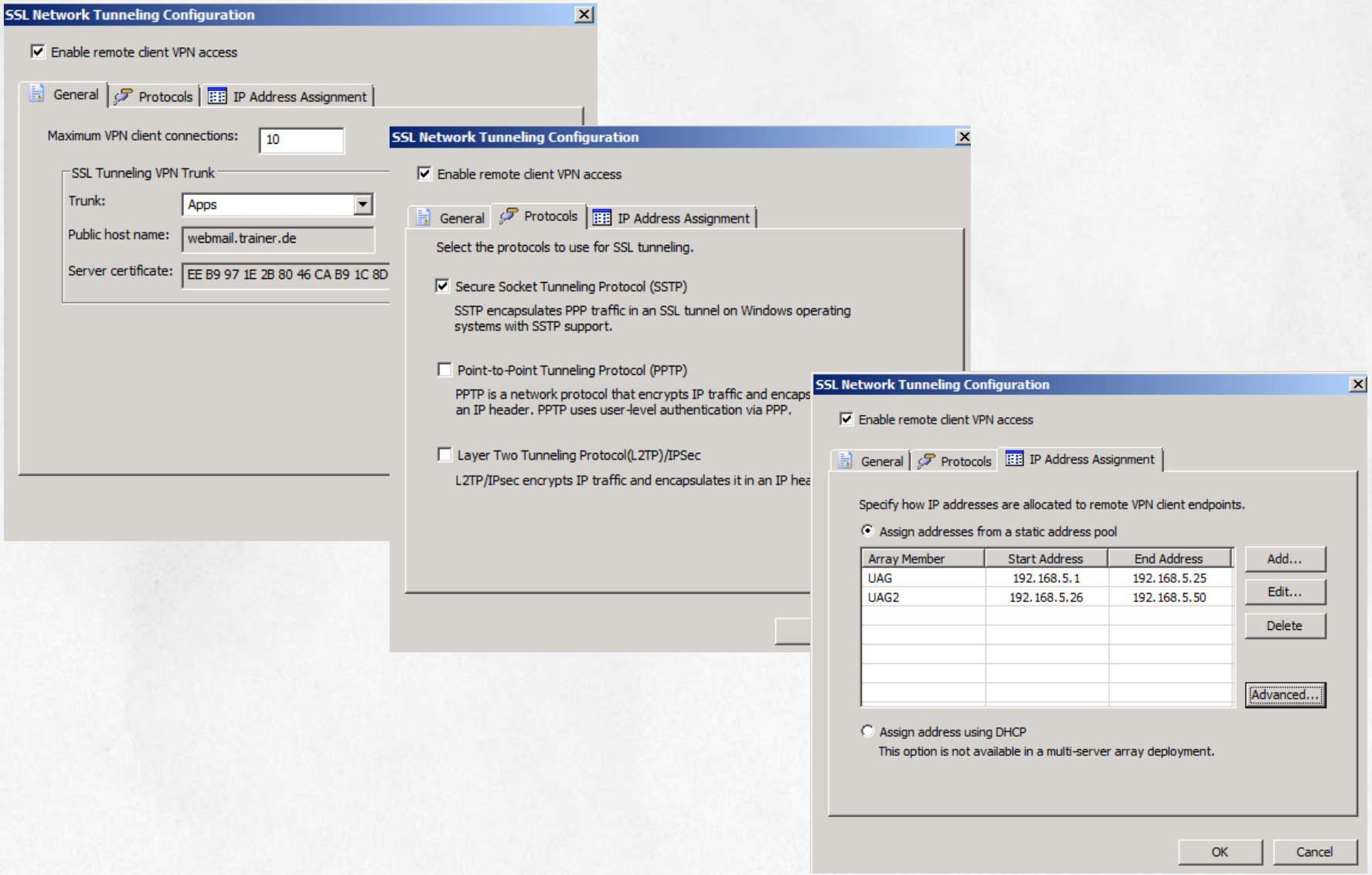
File Access



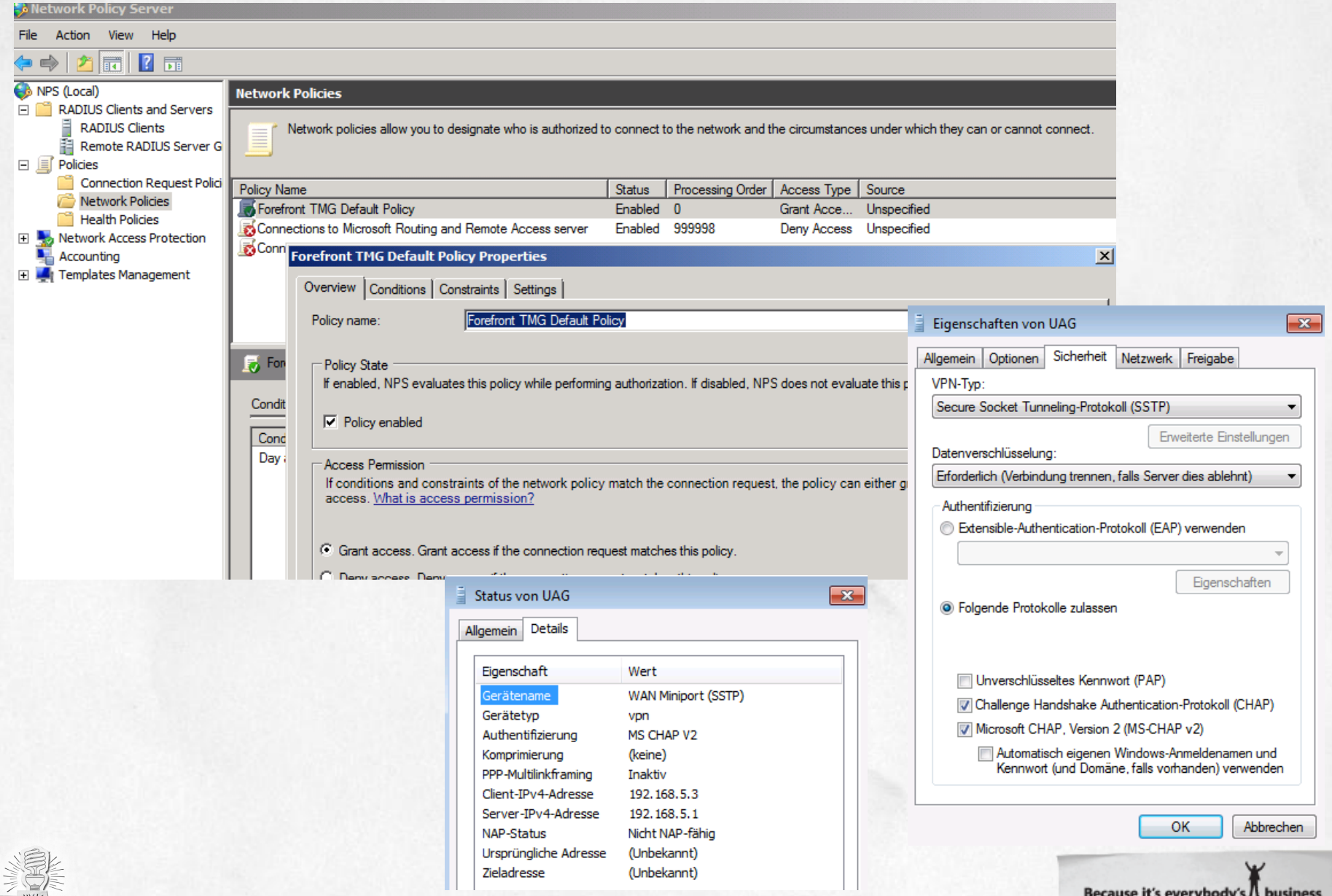
Effizienz – NEO – definiert

Because it's everybody's business

SSL VPN



SSL VPN



SSL VPN

CRL Check ausschalten:
NoCertRevocationCheck
Registry: HKEY_LOCAL_MACHINE\System\
CurrentControlSet\Services\Sstpsvc\Parameters
REG_DWORD: NoCertRevocationCheck
Wert: 1 Disable CRL Check, 0 Enable CRL Check

http://support.microsoft.com/kb/947054/en-us

NAP in UAG

Installing an NPS
Configuring Forefront UAG as an NPS client
    Vendor MS – NAP capable - PSK
Configuring NAP health policies
Configuring NAP network policies
    Vendor 77, allow clients without negotiating an auth…
    Perform machine Health Policies only
    NAP enforcement
Defining NPS servers in Forefront UAG
Source: http://technet.microsoft.com/en-us/library/ee809068.aspx

Monitoring und Troubleshooting

UAG Activation Monitor
- Array Sync
- Sync mit TMG Storage
- ProgramData\Microsoft\UAG\Logs - Monitor-tmp*.log

Windows Eventlogs

UAG Logs

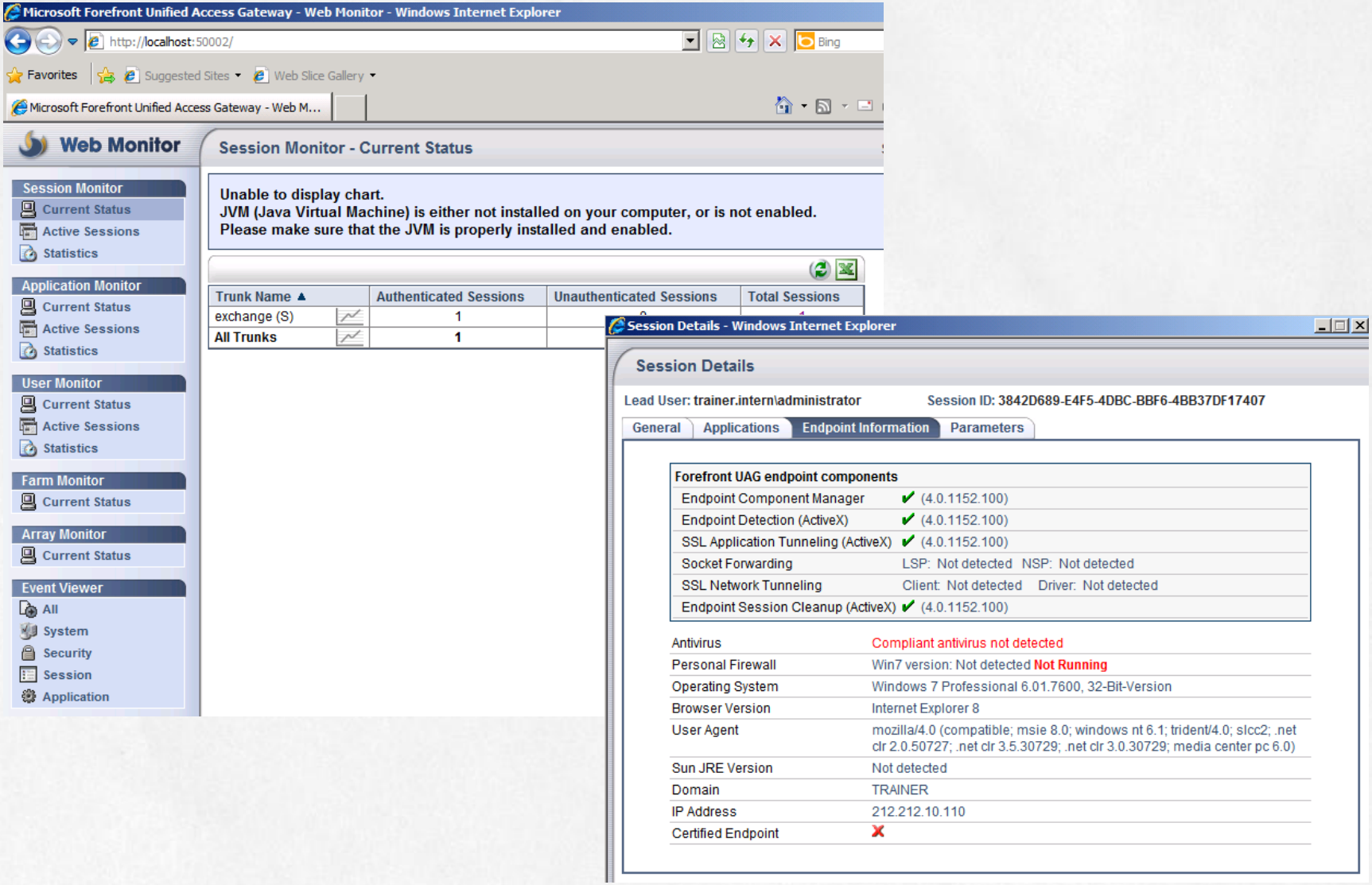
UAG Webmonitor

Forefront UAG Services

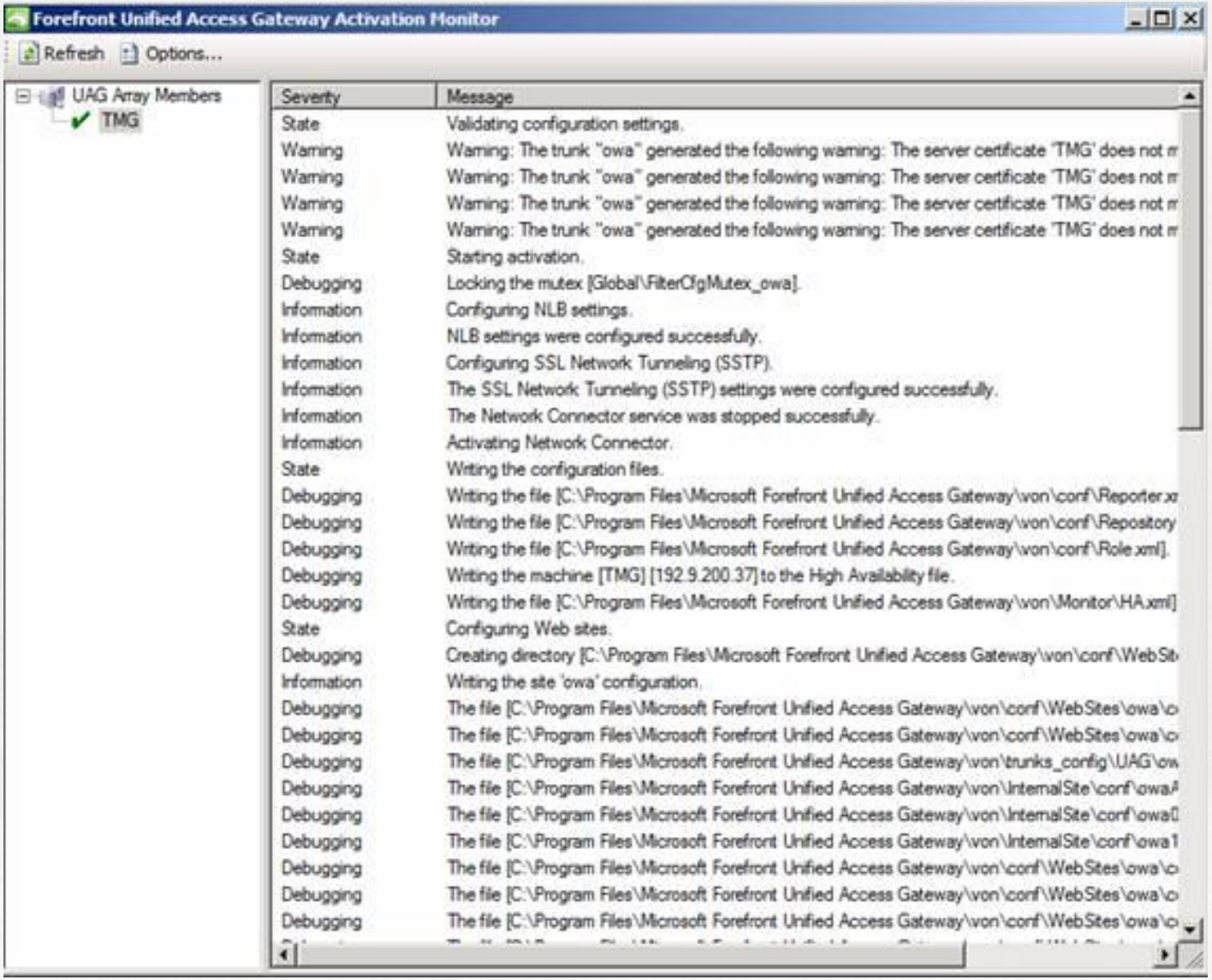
Perfmon
- mehr als Man(n) braucht

SCOM Management Pack

UAG Webmonitor



UAG Activation Monitor



UAG Debugging

Built in Tracing

Delete ForeFront_UAG.bin from ..\windows\debug folder

Navigate to \Programfiles\MicrosoftForefrontUnifiedAccessGateway\common\bin\tracing

Open LaunchHta.vbs

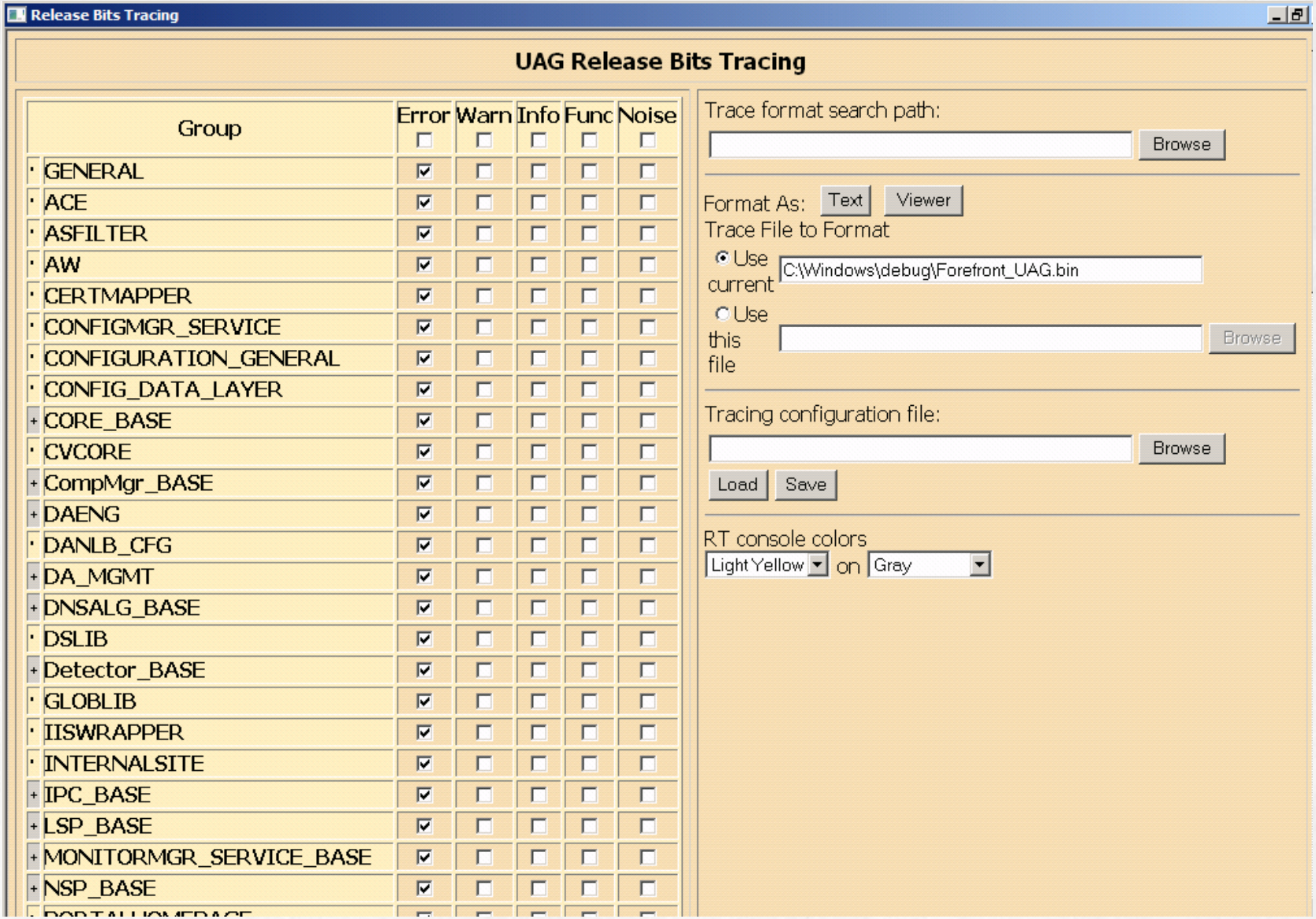
Under Group, select the component named DA_ENG, DA_MGMT, DANLB_CFG, check all 4 checkboxes, click on the Button Go.

Close the HTA file, reproduce the issue, file will be generated under windows\debug file will be named Forefront_UAG.bin

Forefront UAG Tracing Symbol File:

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=fc052e67-2a04-4058-b326-9d92aa67b2c4

UAG Debugging



IPv6

- Vergrößerung des Adressraums von 2x32 (≈ 4,3 Milliarden = 4,3·109) bei IPv4 auf 2x128 (≈ 340 Sextillionen = 3,4·1038)
- Vereinfachung und Verbesserung des Protokollrahmens (Kopfdaten)
- zustandslose automatische Konfiguration von IPv6-Adressen
- Mobile IP sowie Vereinfachung von Umnummerierung und Multihoming
- Implementierung von IPsec innerhalb des IPv6-Standards
- Unterstützung von Netztechniken wie Quality of Service und Multicast

Unterschiede IPv4 zu IPv6

	IPv4	IPv6
Quell- und Zieladressen	32 Bits (4 Bytes) lang	128 Bits (16 Bytes) lang
IPsec-Unterstützung	Optional	Erforderlich
ARP	Broadcast-ARP-Anforderungsframes lösen die IPv4-Adresse in die Verbindungsschichtadresse auf	ARP-Anforderungsframes werden durch Multicast-Nachbaranfragen-achrichten ersetzt
Internet Group Management Protocol	Verwaltet die Gruppenmit-gliedschaft für lokale Subnetze	IGMP wurde durch MLD-Nachrichten ersetzt.
ICMP-Routererkennung	Bestimmt die IPv4-Adresse des Standardgateways	Wurde durch ICMPv6-Routeranfrage- und Routerankündigungsnachrichten ersetzt
Broadcastadressen	Sendet Datenverkehr an alle Knoten in einem Subnetz	Verwendet eine Multicastadresse mit verbindungslokalem Bereich für alle Knoten statt einer IPv6-Broadcastadresse
Konfiguration	Manuell oder durch DHCP konfiguriert	Keine manuelle Konfiguration oder DHCP erforderlich
Ressourceneinträge	Verwendet **A**-Ressourceneinträge in DNS zum Zuordnen von Hostnamen zu IPv4-Adressen	Verwendet **AAAA**-Ressourceneinträge in DNS zum Zuordnen von Hostnamen zu IPv6-Adressen

Quelle: Microsoft MOC Course 6742A

IPv6 Adressierung

Adresssyntax:

- **128-Bit-Adresse im Binärformat:**

```
0010000000000001000011011011100000000
0000000000000010111100111011
0000001010101010000000001111111111111
1110001010001001110001011010
```

- **128-Bit-Adresse unterteilt in 16-Bit-Einheiten:**

```
0010000000000001  0000110110111000
0000000000000000  0010111100111011
0000001010101010  0000000011111111
1111111000101000  1001110001011010
```

- **Die einzelnen 16-Bit-Blöcke konvertiert in HEX (base 16):**

```
2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A
```

- **Weitere Vereinfachung durch Entfernen führender Nullen:**

```
2001:DB8:0:2F3B:2AA:FF:FE28:9C5A
```

Nullauslassung:

- **Einige Adresstypen können eine Vielzahl von Nullen enthalten**
- **Eine zusammenhängende Sequenz von 16-Bit-Blöcken, die auf 0 festgelegt sind, kann mit einem doppelten Doppelpunkt „::“ verkürzt werden**
- **Verbindungslokal:**

```
FE80:0:0:0:2AA:FF:FE9A:4CA2
```

  - **Kann verkürzt werden zu:**

```
FE80::2AA:FF:FE9A:4CA2
```

- **Multicast:**

```
FF02:0:0:0:0:0:0:2
```

  - **Kann verkürzt werden zu:**

```
FF02::2
```

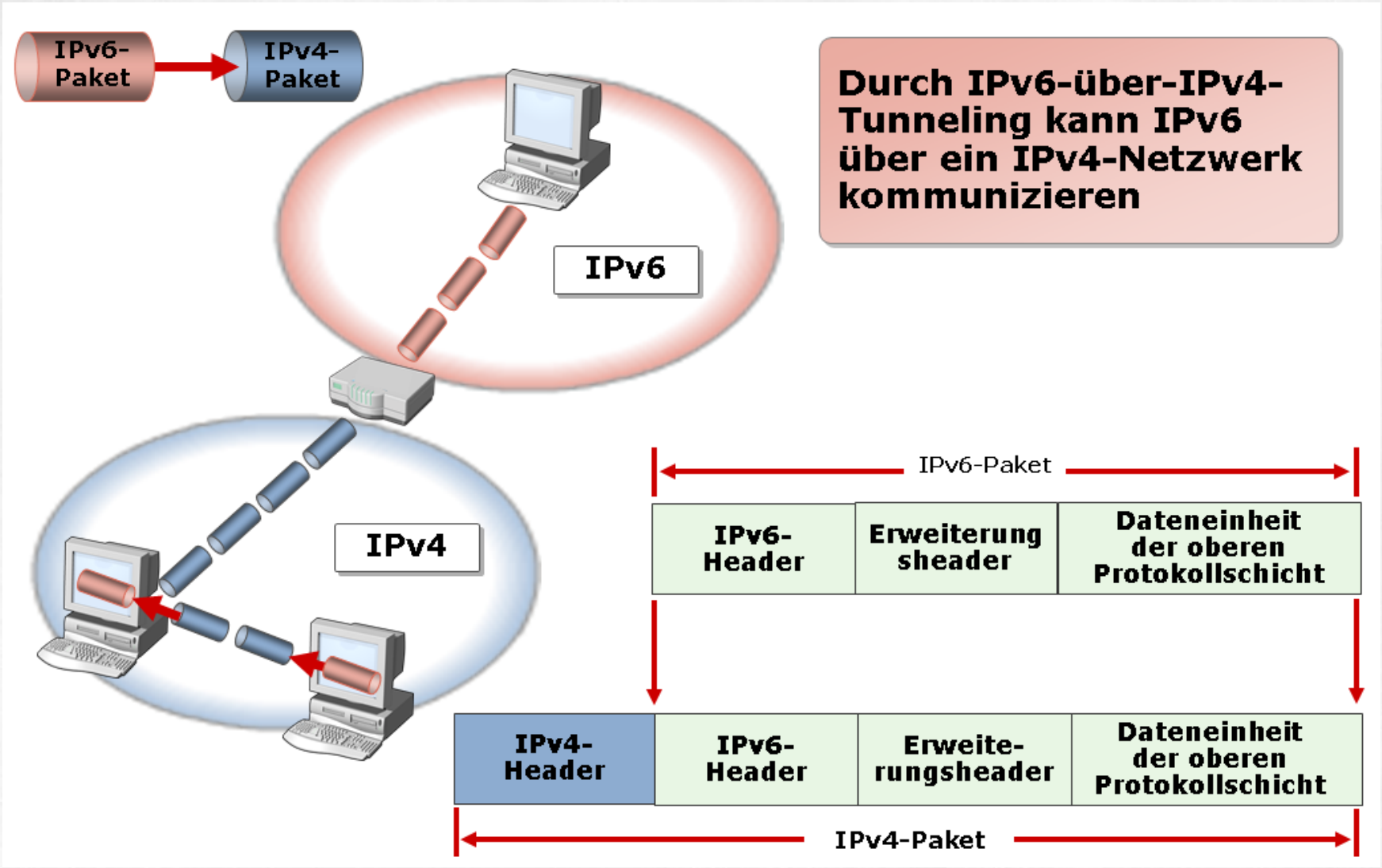
Quelle: Microsoft MOC Course 6742A

IPv6 Praefixe

Zuweisung	Binärwert für Formatpräfix	Hexadezimalwert für Formatpräfix	Teil des Adressraums
Reserviert	0000 0000	-	1/256
Reserviert für NSAP-Zuweisung	0000 001	-	1/128
Aggregierbare globale Unicastadressen	001	2 oder 3	1/8
Verbindungslokale Unicastadressen	1111 1110 10	FE8	1/1024
Standortlokale Unicastadressen	1111 1110 11	FEC0	1/1024
Multicastadressen	1111 1111	FF	1/256

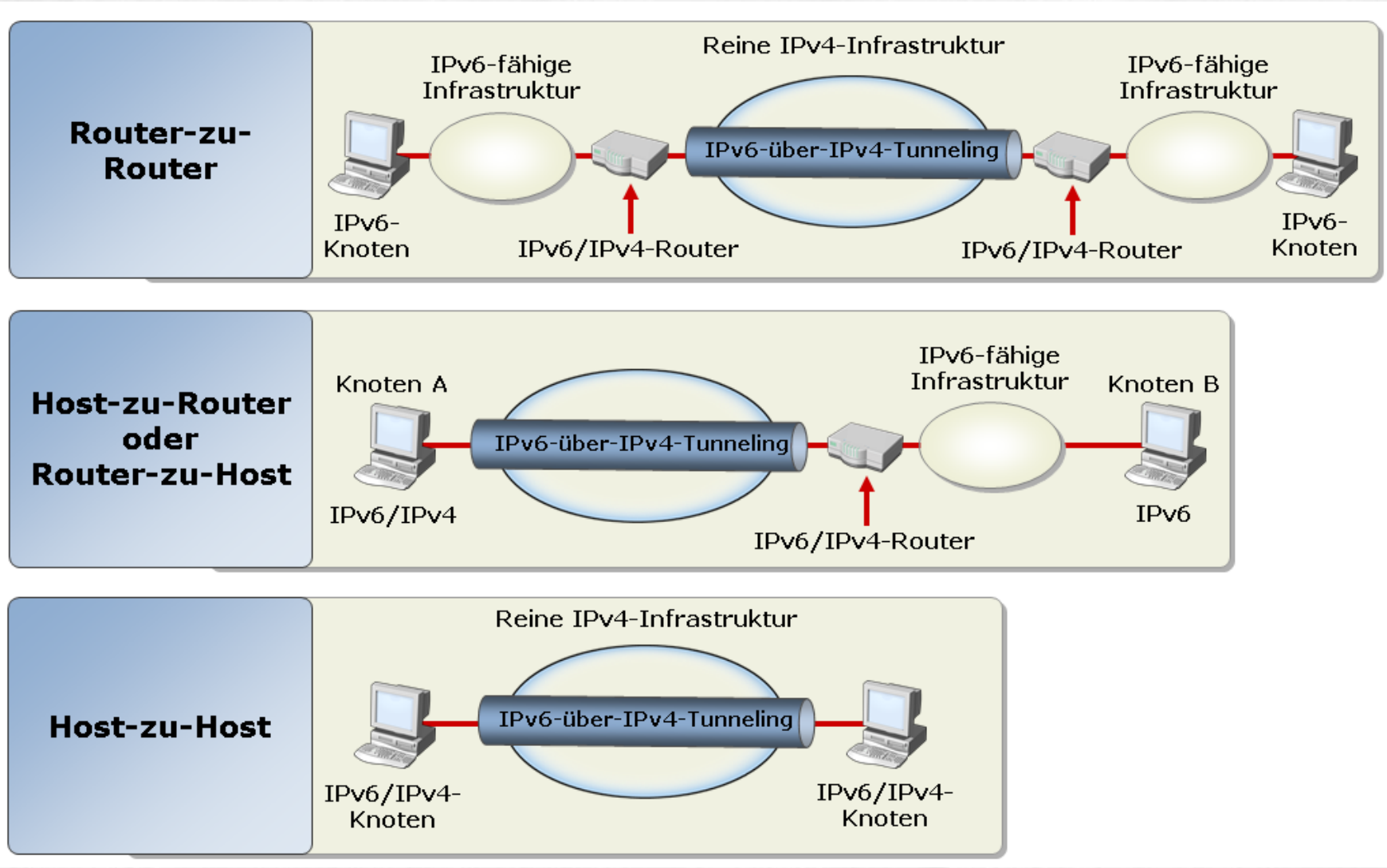
Quelle: Microsoft MOC Course 6742A

IPv6 zu IPv4 Tunneling



Quelle: Microsoft MOC Course 6742A

Tunnelblick



Quelle: Microsoft MOC Course 6742A

IPv6

ISATAP – stands for the Intrasite Automatic Tunnel Addressing Protocol. The UAG DA server will set itself up automatically as an ISATAP router and provide your IPv6 aware hosts IPv6 addresses and routing information. ISATAP capable hosts include Windows Vista and above and Windows Server 2008 and above.

6to4 – is a IPv6 transition technology that the DA clients and UAG DA server can use to connect the DA client to the UAG DA server over the IPv4 Internet. 6to4 is used when the DA client is assigned a public IP address. The IPv6 packets are encapsulated in a IPv4 header and send over the 6to4 tunnel adapter to the DA server.

Teredo – is another IPv6 transition technology that enables the DA client to connect to the DA server over the IPv4 Internet. In this case, Teredo is used when the DA client is located behind a NAT device (either a NAT router or a NAT firewall) and the device allows outbound UDP port 3544. If the DA client has a private IP address and outbound access to UDP 3544, then the DA client uses Teredo to encapsulate the IPv6 messages from the DA client to the UAG DA server in an IPv4 header to send over the IPv4 Internet.

IPv6

IP-HTTPS – is yet another IPv6 transition technology that allows the DA client to connect to the UAG DA server over the IPv4 Internet. IP-HTTPS is a “last ditch” method to encapsulate the IPv6 packets in an IPv4 header. When the client is assigned a private IP address, and the NAT device or firewall is configured to allow only HTTP/HTTPS outbound, then the DA client falls back to IP-HTTPS.

NAT64/DNS64 – NAT64/DNS64 (pronounced NAT 6 to 4/DNS 6 to 4). NAT64/DNS64 accepts the connections from the DA client, automatically creates a IPv6 address for the name requested by the client, and then does a “NAT” kind of protocol transformation so that the IPv6 communication from the DA client is forwarded to the IPv4 only server on the network using IPv4.

http://blogs.technet.com/b/tomshinder/archive/2010/03/12/uag-directaccess-don-t-fear-the-reaper-or-ipv6.aspx

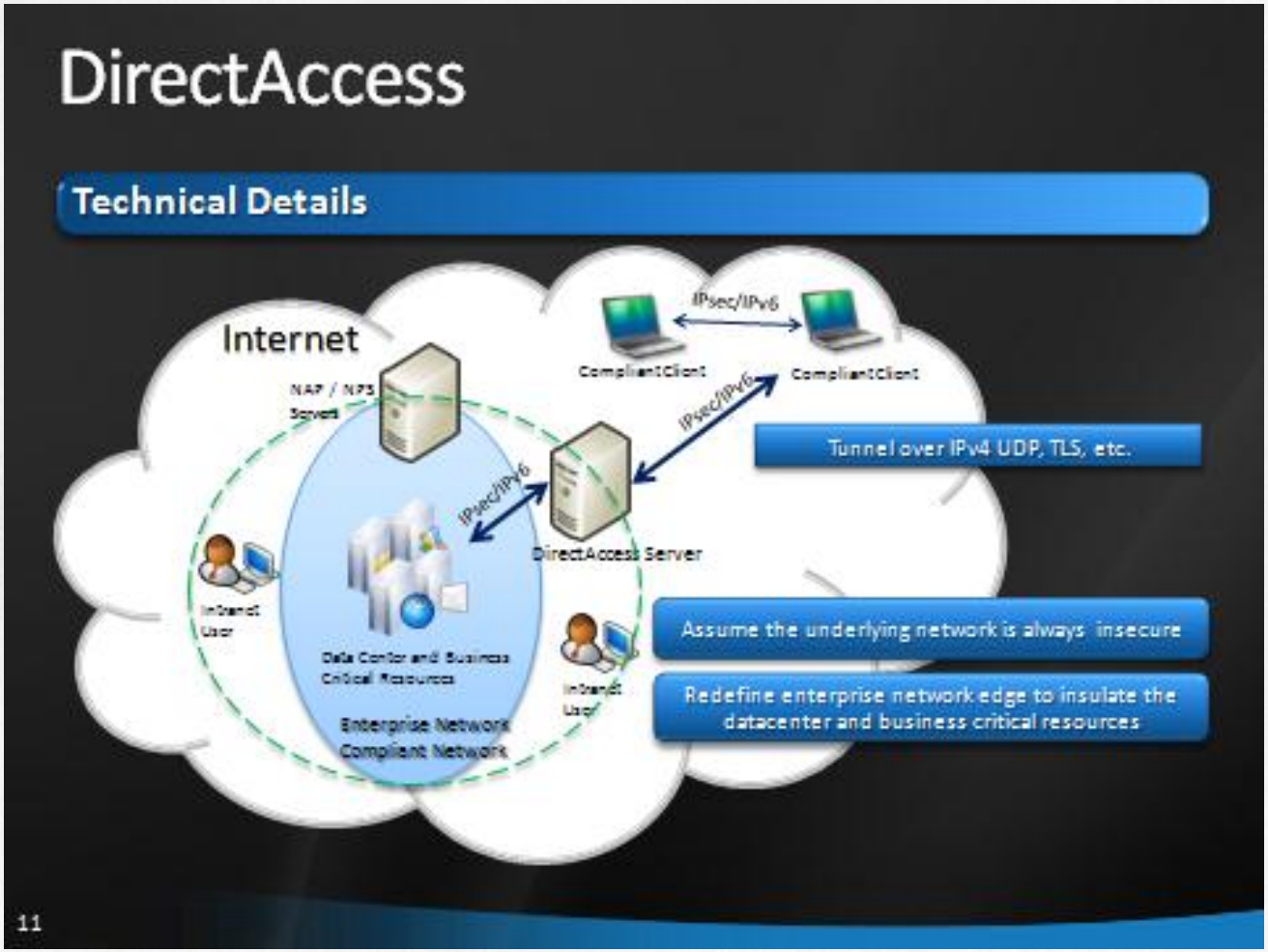
Tunneltechniken

Tunneling-technologie	Verwendung
ISATAP	• Lokale Intranets • Automatische Konfiguration auf Host • Ermöglicht IPv6-Knoten die Kommunikation über ein IPv4-Subnetz • Standardmäßig aktiviert
6to4	• IPv6-zu-IPv6-Netzwerke über das IPv4-Internet • Automatische Konfiguration auf Host • Standardmäßig aktiviert
Teredo	• IPv6-zu-IPv6 über IPv4-NAT • Standardmäßig deaktiviert

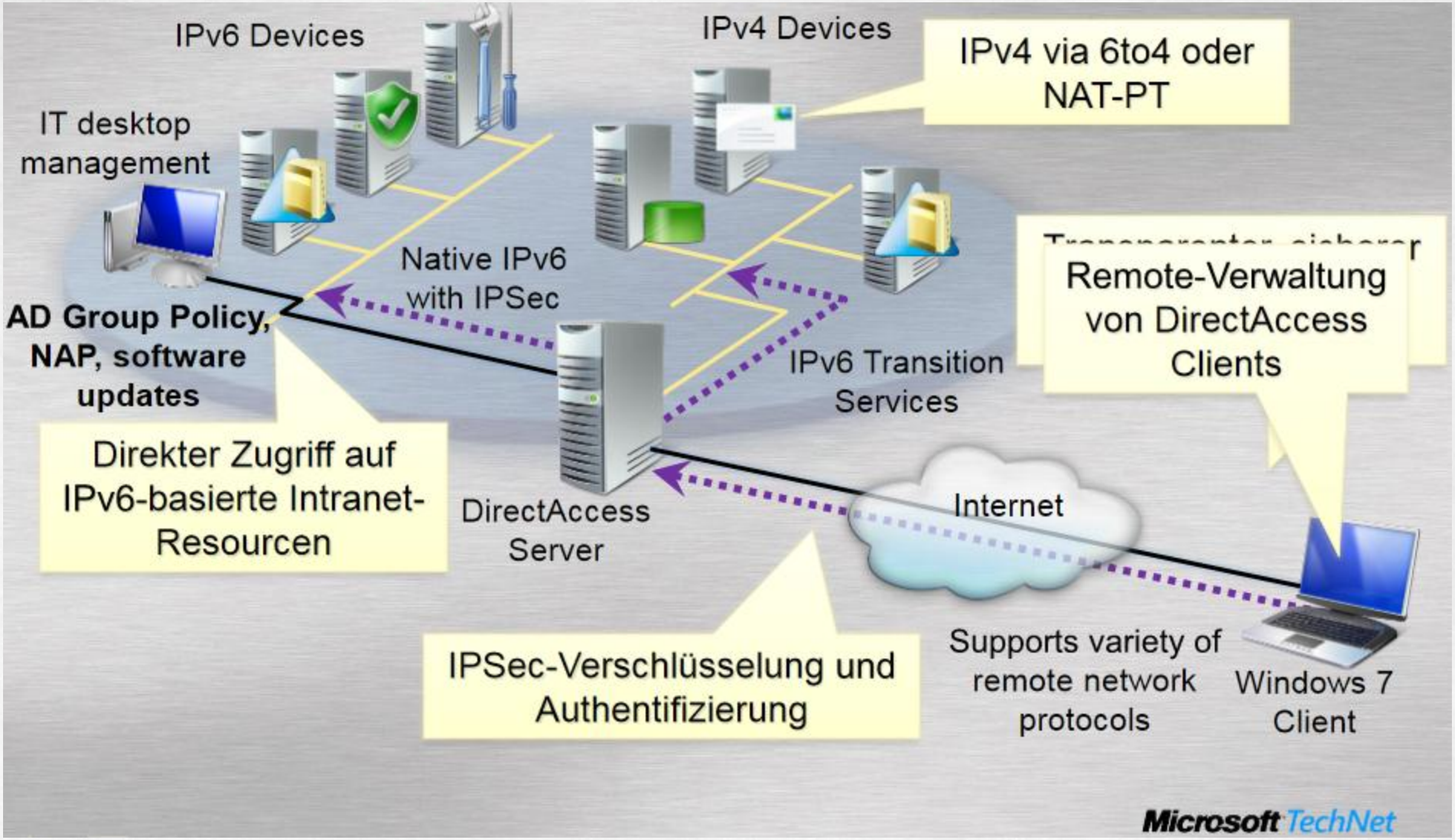
PortProxy vereinfacht die Kommunikation zwischen Knoten oder Anwendungen, die nicht über ein gemeinsames Internetschichtenprotokoll (IPv4 oder IPv6) eine Verbindung herstellen können

Quelle: Microsoft MOC Course 6742A

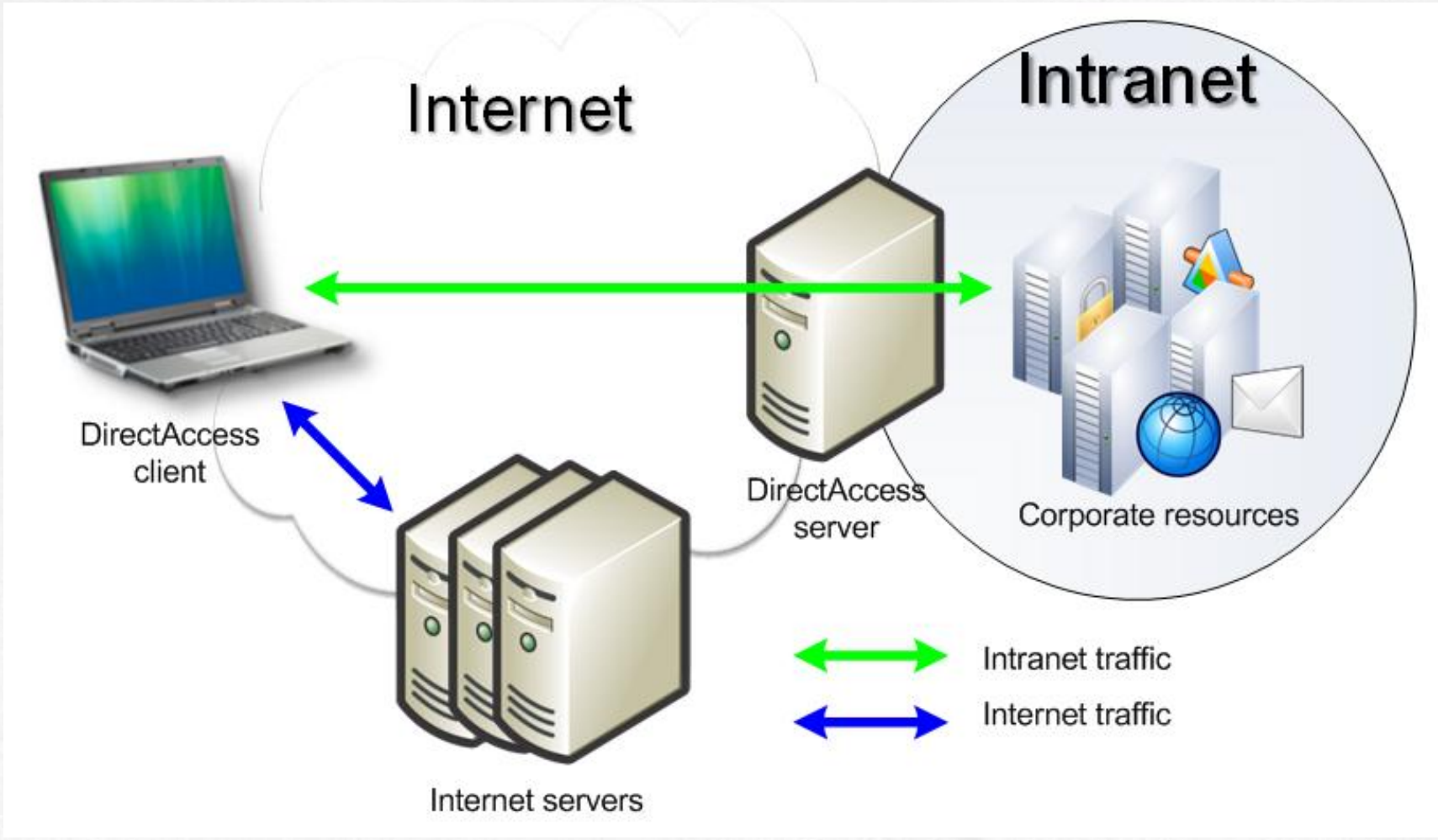
Direct Access



DirectAccess



Direct Access – Split Tunneling



Direct Access

System Requirements	Features List
• DirectAccess server running Windows Server 2008 R2 along with network adaptors for the Internet and the Intranet. • DirectAccess clients running Windows 7. • At least one domain controller and Domain Name System (DNS) server running Windows Server 2008 or Windows Server 2008 R2. • A public key infrastructure (PKI) to issue computer certificates, smart card certificates, and, for NAP, health certificates. For more information, see http://www.microsoft.com/pki. • IPsec policies to specify protection for traffic. For more information, see http://www.microsoft.com/ipsec. • IPv6 transition technologies available for use on the DirectAccess server: ISATAP, Teredo, and 6to4. • NAT-PT device to provide access to IPv4-only resources for DirectAccess clients.	• Always-on connectivity that requires no end-user steps to access corpnet. • Remote management, updating, and health maintenance of remote computers even when the end user is not logged on. • Granular policy controls for authorized access to corpnet resources and servers. • Tight integration with policy-based network access approach. • Support for multifactor authentication such as smart cards. • IPsec authentication and encryption. • Support for non IPsec and non-IPv6 environments (e.g., using IPv6-over-IPv4 tunneling with 6to4 or Teredo).

DirectAccess - Anforderungen

- Joined to an Active Directory domain
- Running Windows Server 2008 R2
- Have at least two physical network adapters installed
- Have at least two consecutive publicly addressable static IPv4 addresses that are externally resolvable through the Internet DNS
- Running Windows 7 Ultimate oder Enterprise
- NRPT
- Active Directory – ISATAP GlobalQueryBlocklistDisabled
- OU fuer User/ DA Client, GG/UG fuer DA-Access, DA Client Member)
- Windows 2008 / R2 Domain controller
- Public key infrastructure (PKI)
- Webservercertificate Public Name bound on first public IPv4 address
- All SSL certificates must have a certificate revocation list (CRL) that is reachable from a publicly resolvable fully qualified domain name (FQDN)
- IPsec policies
- IPv6 and IPv4 transition technologies – IPv6 and the transition technologies ISATAP, Teredo, and 6to4
- STEP BY STEP GUIDE: http://technet.microsoft.com/en-us/library/ee861169.aspx

CRL CA Pfad + Publish with TMG

1.On the CA computer, click Start, point to Administrative Tools, and then click Certification Authority.
2.In the console tree, right-click the name of the CA, and then click Properties.
3.Click the Extensions tab, and then click Add.
4.In Location, type the URL or UNC path for the CRL distribution point. For example, type http://crl.contoso.com/crld/.
5.In Variable, click <CAName>, and then click Insert.
6.In Variable, click <CRLNameSuffix>, and then click Insert.
7.In Variable, click <DeltaCRLAllowed>, and then click Insert.
8.In Location, type .crl at the end of the Location string, and then click OK.
9.Select Include in CRLs. Clients use this to find Delta CRL locations. and Include in the CDP extension of issued certificates, and then click OK
10. New IIS Virtual directory that points to the c:\windows\system32\certsrv\certenroll directory
11. Allow Directory Browsing
12. Allow HTTP or HTTPS access
13. Publish the CRL Directory with TMG

CRL CA Pfad

Alternativ:
Nur fuer Testumgebungen zu empfehlen:
CA properties
Extension tab
Specify locations for which users can obtain a certificate revocation list,
Check all locations of the CRL Distribution Point (CDP)
Authority Information Access (AIA), and verify that Publish CRLs to this location or Publish Delta CRLs to this location is not selected

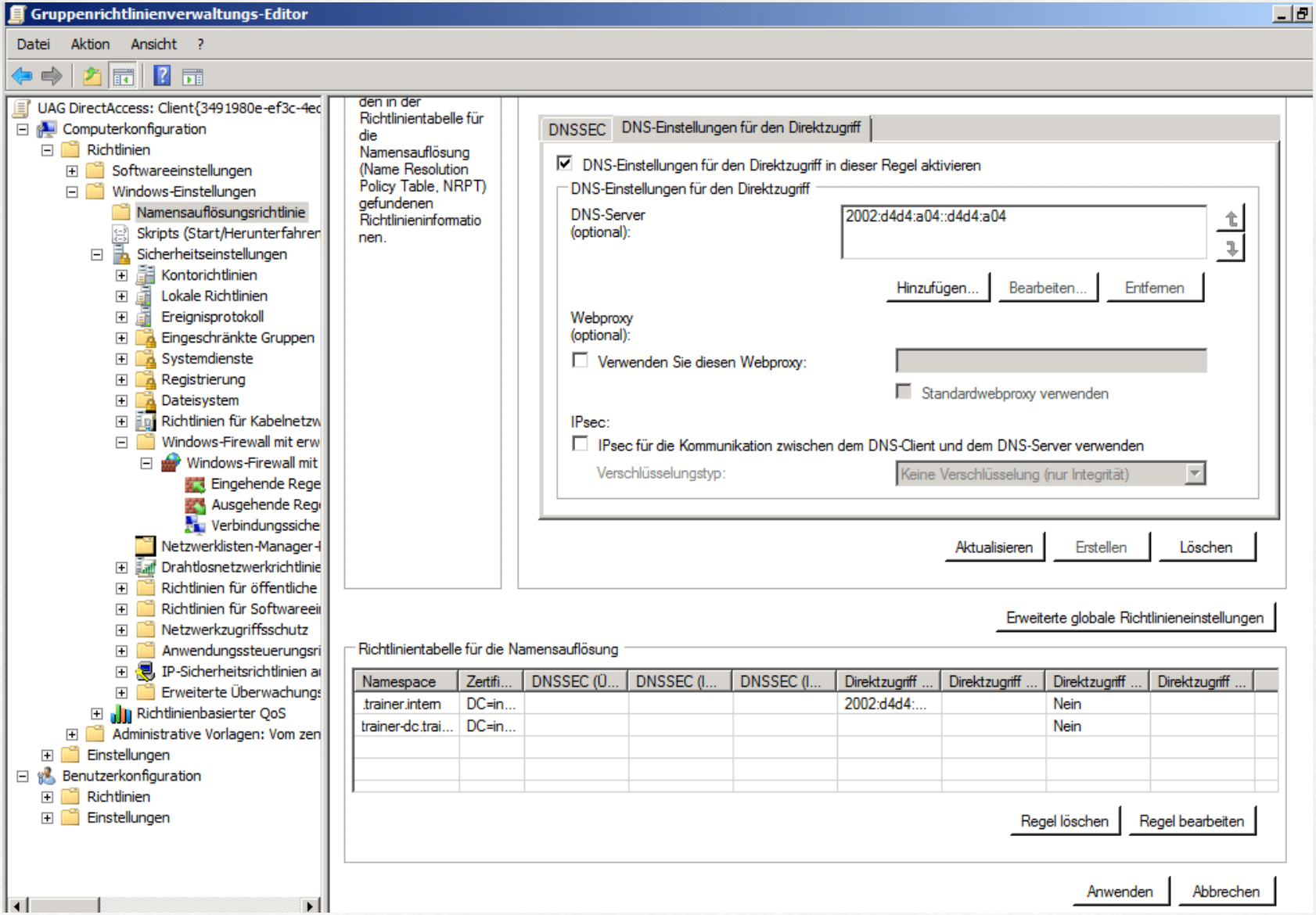
DirectAccess – Group Policies

UAG DirectAccess: AppServer {GUID} – these GPO settings are applied to machines that you include in the application servers groups, which are called out at the end of the UAG DA configuration wizard. These policies enable end to end IPsec protection between the DA client and the destination server.

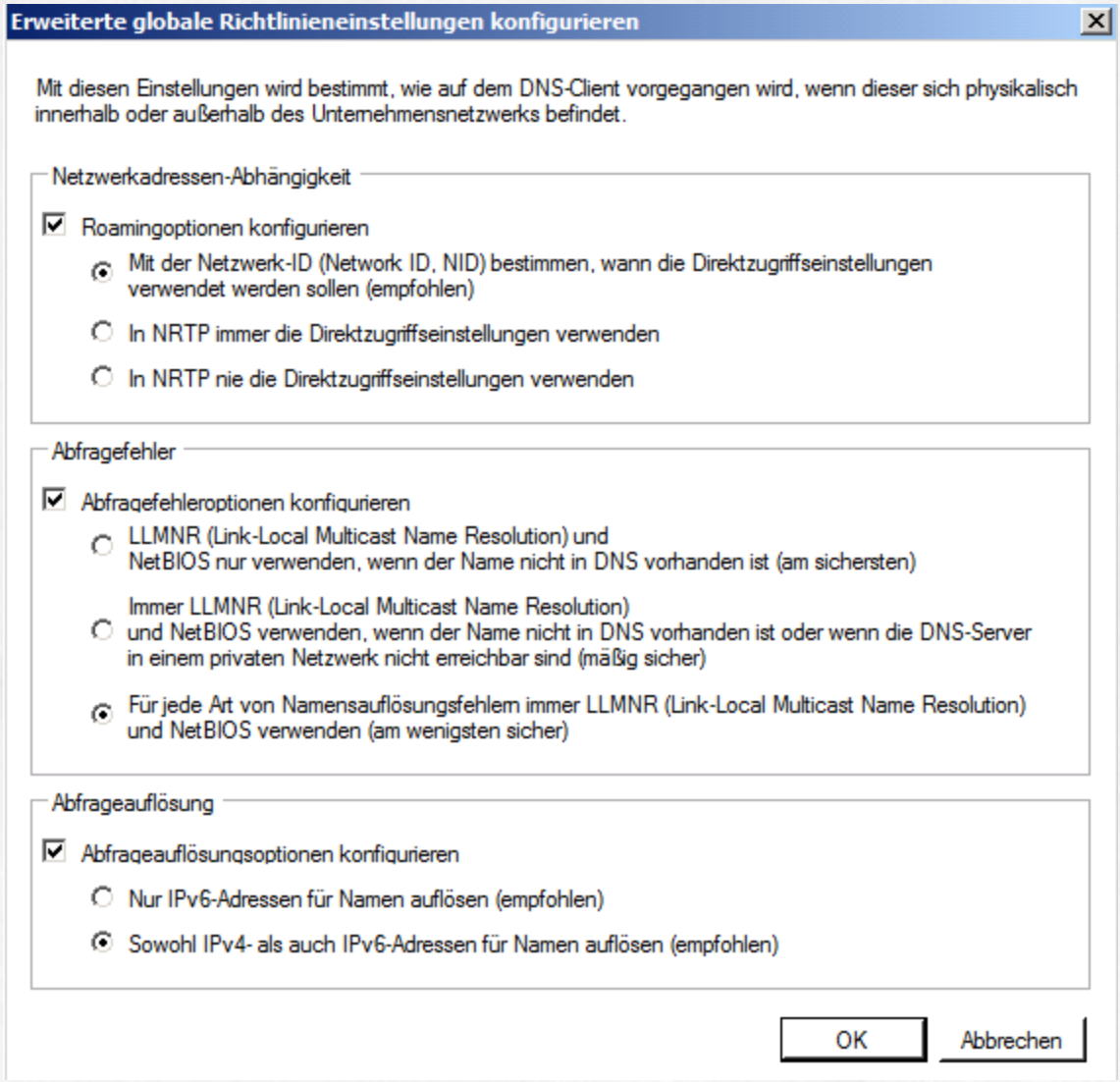
UAG DirectAccess: Client {GUID} – these GPO settings are applied to the DA clients. DA clients are assigned to a security group that you create when you configure the DA solution for your organization. There is no “built in” DA clients security group, you need to create this yourself.

UAG DirectAccess: DaServer {GUID} – these GPO settings are applied to the UAG DA servers themselves. If you have a single UAG DA server, then these settings will be applied to that server. If you have an array of UAG DA servers, then the GPO settings will be applied to each of the servers in the UAG DA server array.

NRPT



NRPT



NAT64 und DNS64

DirectAccess client sends a DNS name query to Forefront UAG DirectAccess server

Because DirectAccess clients have only IPv6 connectivity to the Forefront UAG, the DNS name query is an IPv6 AAAA request.

When the DNS64 gets the name query request, it sends two DNS name queries, an IPv4 query (A) and an IPv6 query (AAAA), to the corporate DNS configured on the Forefront UAG DirectAccess server.

The DNS64 gets a response from the corporate DNS, and decides which address to return to the DirectAccess client.

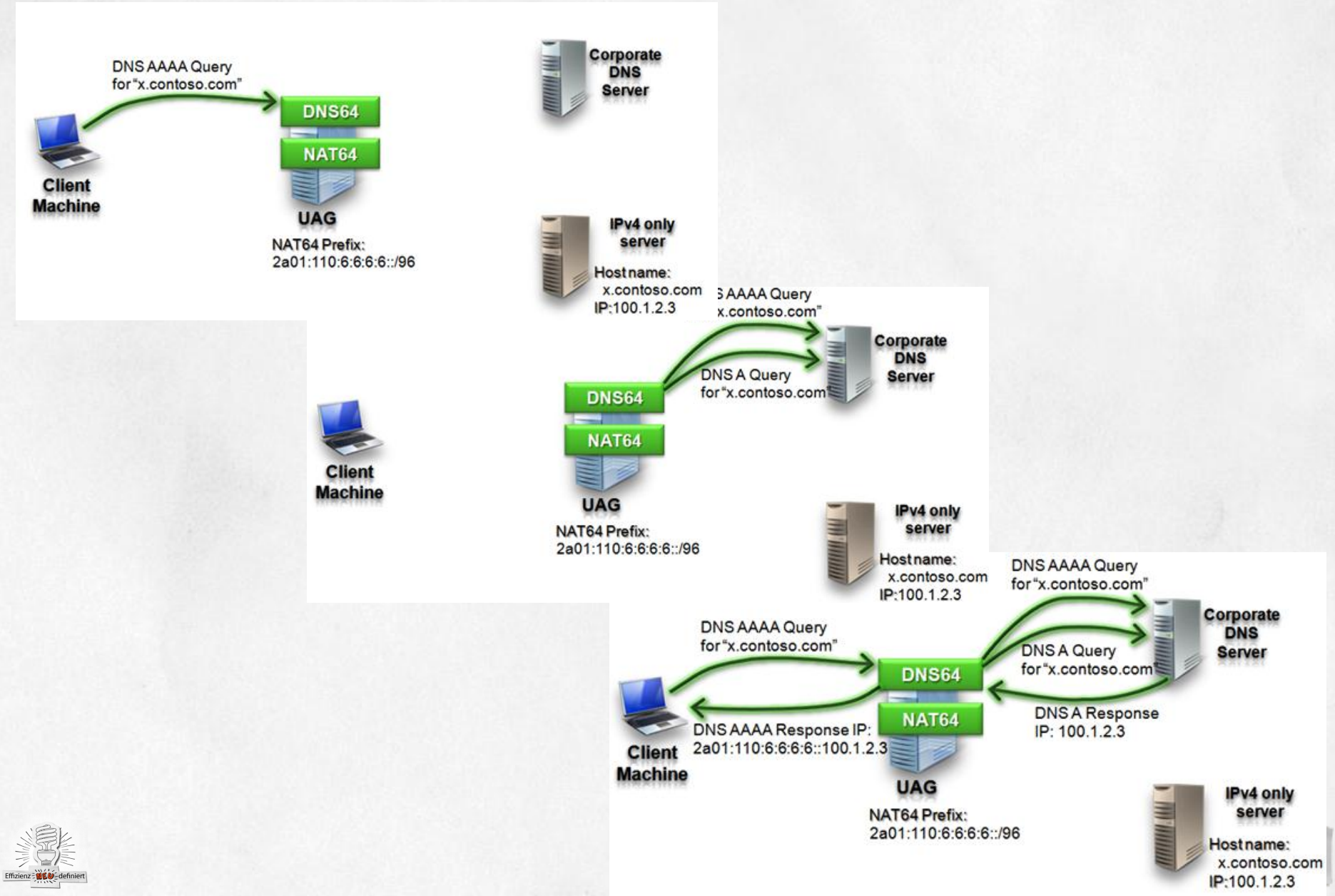
When the DNS64 receives an IPv6 address (AAAA record) response from the corporate DNS, the application server has IPv6 connectivity, and the IPv6 address is returned to the DirectAccess client.

When the DNS64 receives an IPv4 address (A record), the NAT64 acts as a bridge for the traffic. The generated IPv6 address is sent to the DirectAccess client.

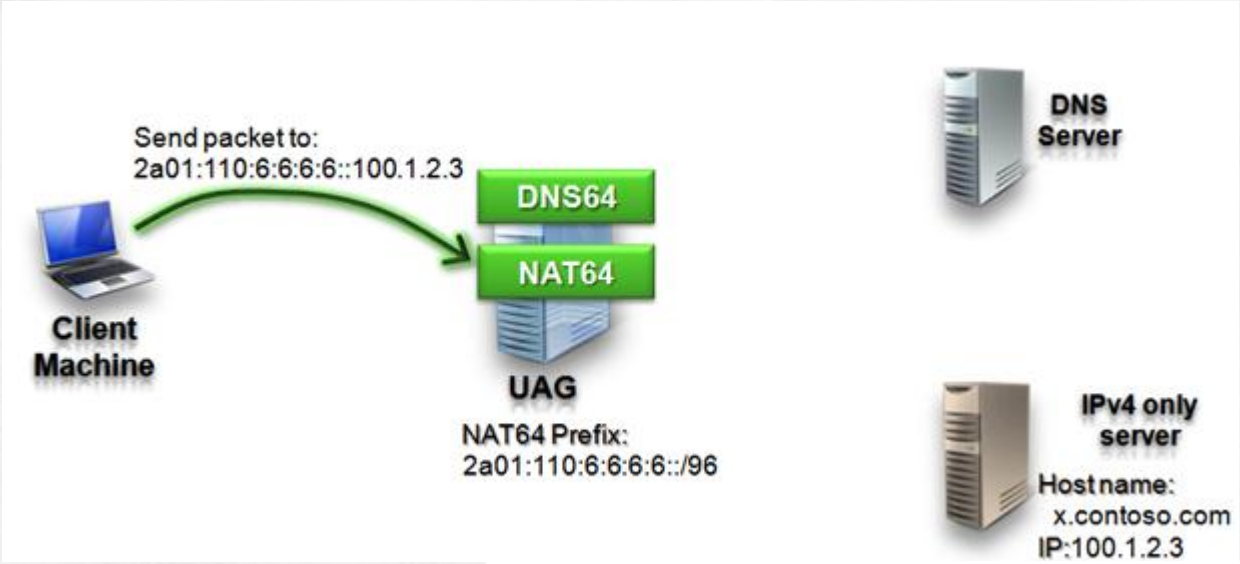
The DirectAccess client now has an IPv6 address for the application server. Traffic is sent directly to the Forefront UAG DirectAccess server's NAT64

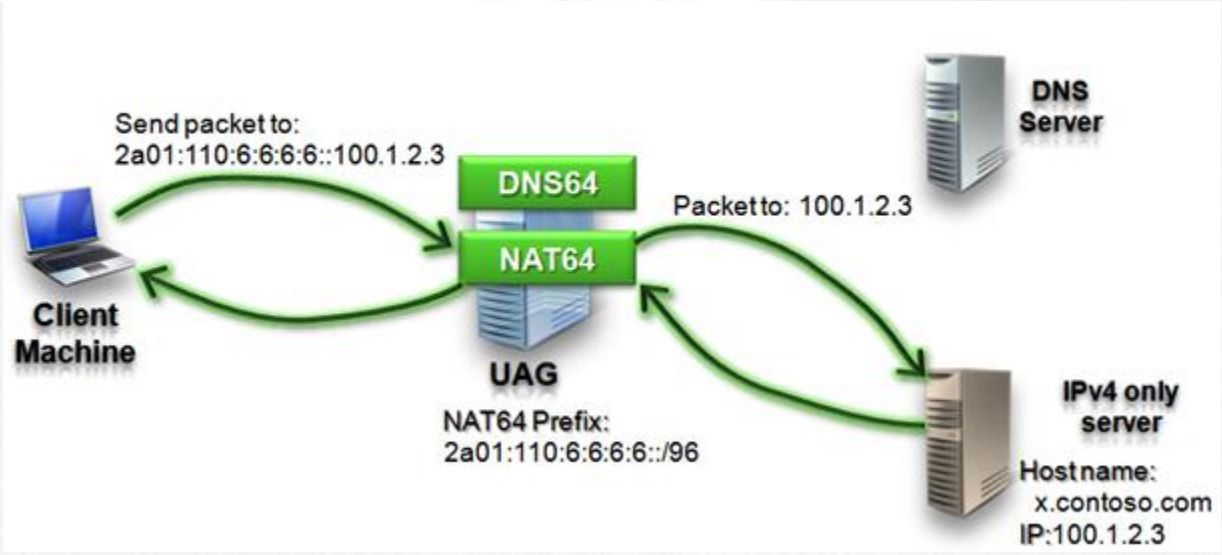
When the NAT64 receives the packet, it extracts from the IPv6 packet the IPv4 address associated with the destination IPv6 address, and transmits the data with an IPv4 header to the application server

DNS64 – NAT64


DNS AAAA Query
for "x.contoso.com"
DNS64
NAT64
Client
Machine
UAG
NAT64 Prefix:
2a01:110:6:6:6:6::/96
Corporate
DNS
Server
IPv4 only
server
Host name:
x.contoso.com
IP:100.1.2.3
DNS A Query
for "x.contoso.com"
DNS AAAA Response IP:
2a01:110:6:6:6:6::100.1.2.3
DNS A Response
IP: 100.1.2.3

DNS64 – NAT64





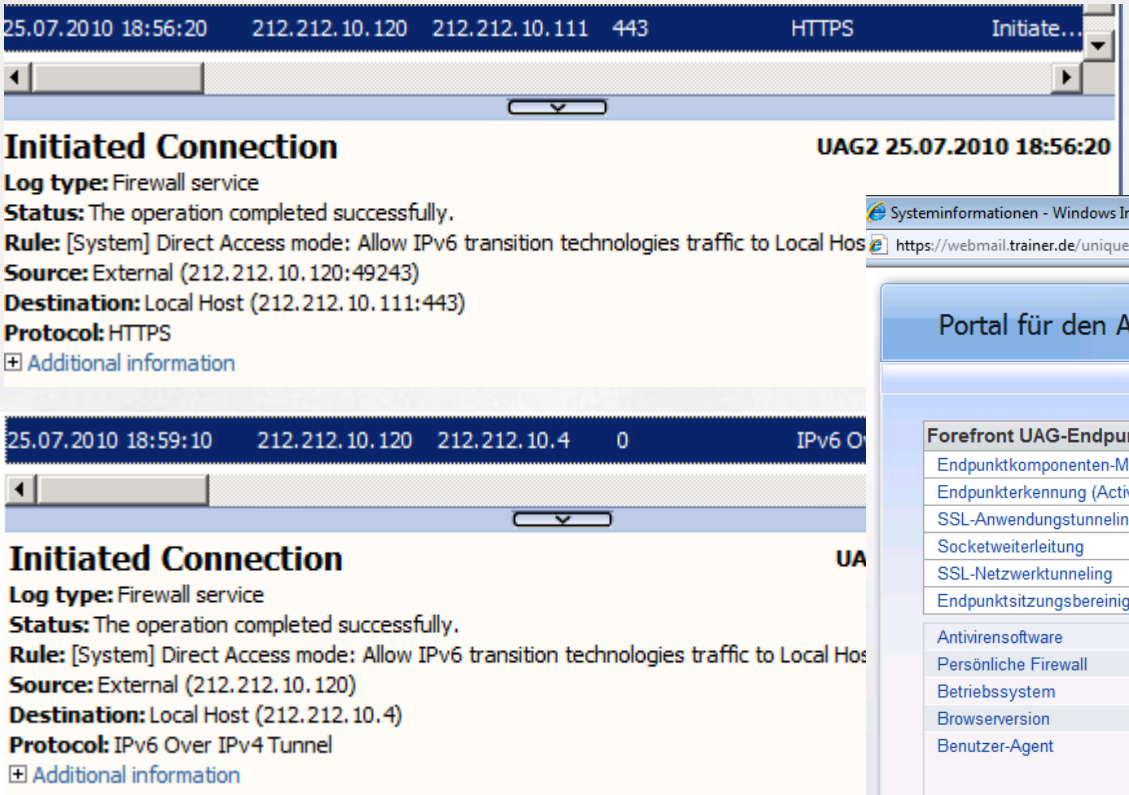
Wie prueft ein Direct Access Client den Netzwerkzugriff

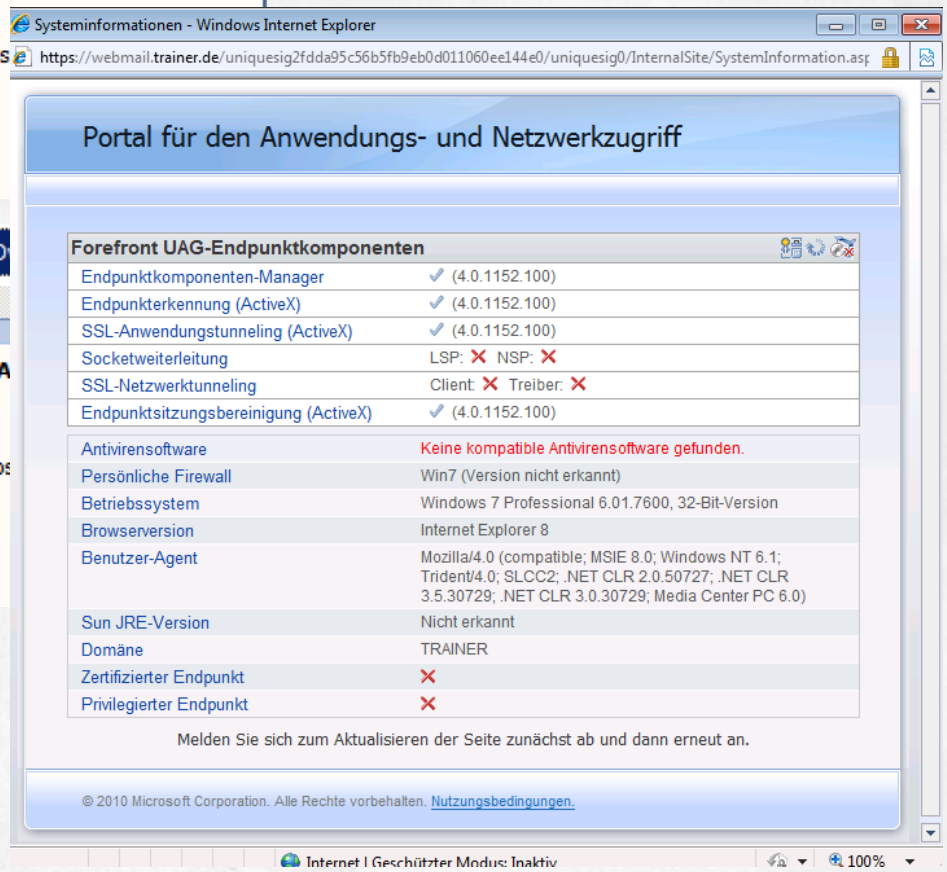
1. HTTPS Anfrage an den internen FQDN des NLS Server (im UAG DA Wizard angegeben und per GPO auf den Client gebracht)
2. Wenn die URL nicht erreicht werden kann, ist der Client nicht mit dem Intranet verbunden. Wenn die URL erreichbar ist wird NRPT abgeschaltet (netsh namespace show effectivepolicy)
3. Ist der DA Client im Internet / kein NAT: Verwendung von 6to4
4. Hinter NAT und UDP Zugriff ist moeglich: Verwendung von Teredo
5. Hinter NAT, und UDP ist blockiert:
Verwendung eines HTTPS-Tunnel über Port 443 TCP

IPv6 Transitionstechnologien pruefen

Command	Description	On client (C) or server (S)
ipconfig /all	Displays all IP configuration data, and should include global IP address.	C,S
Netsh interface teredo show state	Displays the current state of Teredo.	C,S
Netsh interface 6to4 show state	Displays the current state of 6to4.	C,S
Netsh interface isatap show state	Displays the current state of ISATAP.	S
Netsh interface httpstunnel show interface	Displays the current state of IP-HTTPS interface. This should not have a status of deactivated.	C,S

DirectAccess Monitoring





Hochverfuegbarkeit und Skalierbarkeit

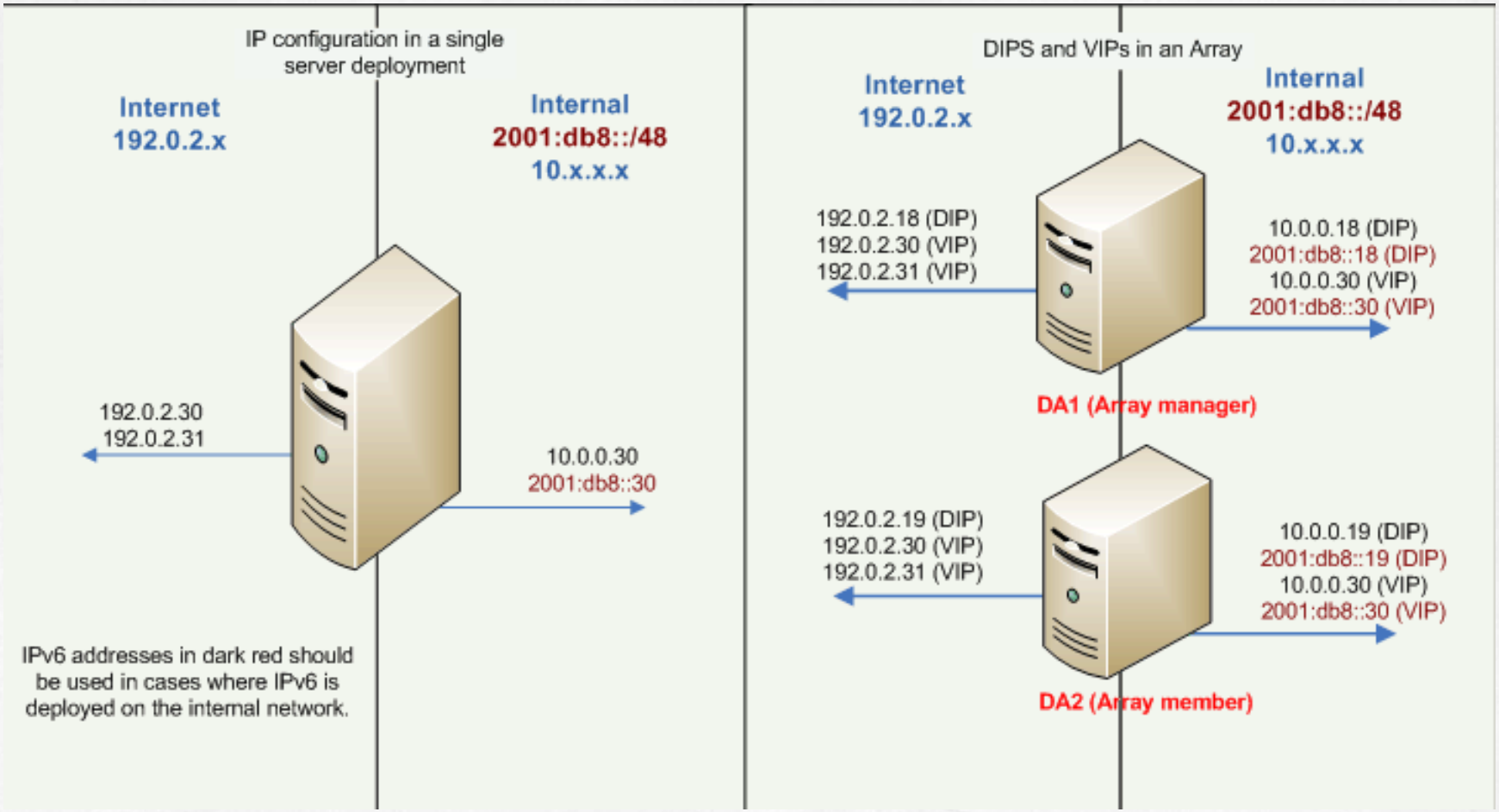
Bis zu 50 Server in einem Array
Bis zu 8 Server im NLB Array
Windows Server 2008 R2 NLB
In virtualisierten Umgebungen (MAC Address Spoofing aktivieren)
VIP = Virtual IP Address
DIP = Dedicated IP Address
Array Manager
Array Verwaltung
NLB Einrichtung
- Unicast
- Multicast
- Multicast IGMP

NLB fuer Trunks
UAG Verwaltung nur ueber Array Manager
Ueberwachung mit UAG Webmonitor oder TMG-Verwaltungskonsole
Hotfix erforderlich: http://support.microsoft.com/kb/977342/de

DirectAccess Step by Step

http://www.it-training-grote.de/download/FF-UAG-DA.pdf

Hochverfuegbarkeit und Skalierbarkeit



Migration von IAG zu UAG

Keine autmatische Migration
Voraussetzung IAG 3.7 SP2
Manuell nachbauen:

- Trunks and trunk settings
- Authentication and authorization server settings
- Client endpoint access policies
- File Access configuration
- Inspection rule sets
- Custom update files (in the CustomUpdate folders)
- Internal site customizations
- Custom hook files (in the commin\bin\CustomHooks folder)
- Endpoint component customizations
- Predefined IP addresses and ports stored in the .smf files (created in the Service Policy Manager console)
- ISA Server rules or settings you created manually
- Modified registry keys
- Custom IIS settings

Source: http://technet.microsoft.com/en-us/library/ee921426.aspx

Migration von IAG zu UAG

Ensure you have access to IAG 2007 servers and configuration settings.
On a separate server, install Forefront UAG, according to instructions described in the Installation guide.
Recreate required configuration settings.
Update network adapter IP address settings
Update certification authority (CA) settings, and certificates
If you publishing Exchange 2003 or Exchange 2007 ActiveSync or Outlook Web Access using IAG 2007 application trunks, recreate the publishing configuration according to the instructions described in Exchange services publishing solution guide.
Copy internal site customizations, and custom updates
Ensure that custom EPD scripts and policies created for IAG 2007 SP2 are adapter for Windows Server 2008 R2 before deploying on Forefront UAG.
Note that Forefront UAG endpoint components are compatible for access to both Forefront UAG and IAG 2007 resources.

Backup und Recovery von UAG

Forefront UAG Server Backup and Restore
Built-in log files
Forefront UAG export configuration files
Other vendor log files
Backing up the Forefront UAG DirectAccess configuration
Export in XML:

configmgrutil export filename.xml password comment

Import: UAG Konsole – File – Import –
Import von anderer UAG Maschine:
HKEY_LOCAL_MACHINE\Software\WhaleCom\e-Gap\Configuration – REG_DWORD
ImportFromOtherVersion, auf Wert = 1 setzen
Source: http://64.4.11.252/en-us/library/ff607447.aspx

Lust auf Links?

Forefront Team Blog
http://blogs.technet.com/edgeaccessblog
Microsoft Forefront UAG
http://www.microsoft.com/forefront/prodinfo/roadmap/uag.mspx
Forefront UAG FAQ
http://www.microsoft.com/forefront/prodinfo/roadmap/uag-faq.mspx
Forefront UAG Systemanforderungen
http://technet.microsoft.com/en-us/library/dd903051.aspx
Forefront IAG/UAG Foren
http://social.technet.microsoft.com/Forums/de-DE/forefrontedgeiag/threads

Marc Grote

Fragen??

Microsoft Forefront

www.forefront.de

www.microsoft.com/forefront