

TMG/UAG/FEP/FPE/FSSP/
FPSMC/FIM/FOPE/FPOCS
- Alles klar?

Marc Grote

grotem@it-training-grote.de

Twitter ??

Inhalt

- Was ist Forefront
- Forefront im Einsatz

Folie 2 von 609
(14,3 Folien pro Min.)

Wer bin ich?

- Marc Grote
- Baujahr 1972
- Seit 1989 hauptberuflich Itler
Seit 1995 Selbststaendig, vorher angestellt als
IT-Administrator und Teilzeitconsultant
- Schwerpunkte: Microsoft Forefront
TMG/UAG/FCS/FPE/FEP, Windows Server
Clustering und PKI, Exchange Server seit v5.0

Was ist Forefront?

Die haeufigsten Fragen auf der CeBIT, meiner Kunden, Tched und Technet Foren

- Habe Forefront-Server installiert...
- Zeigen Sie mir mal den neuen Forefront
- Mein Forefront macht Probleme



Meine Antwort

- Welchen Forefront haetten Sie denn gern?
- Forefront ist kein Produkt, sondern eine Produktfamilie

Forefront Produktfamilie

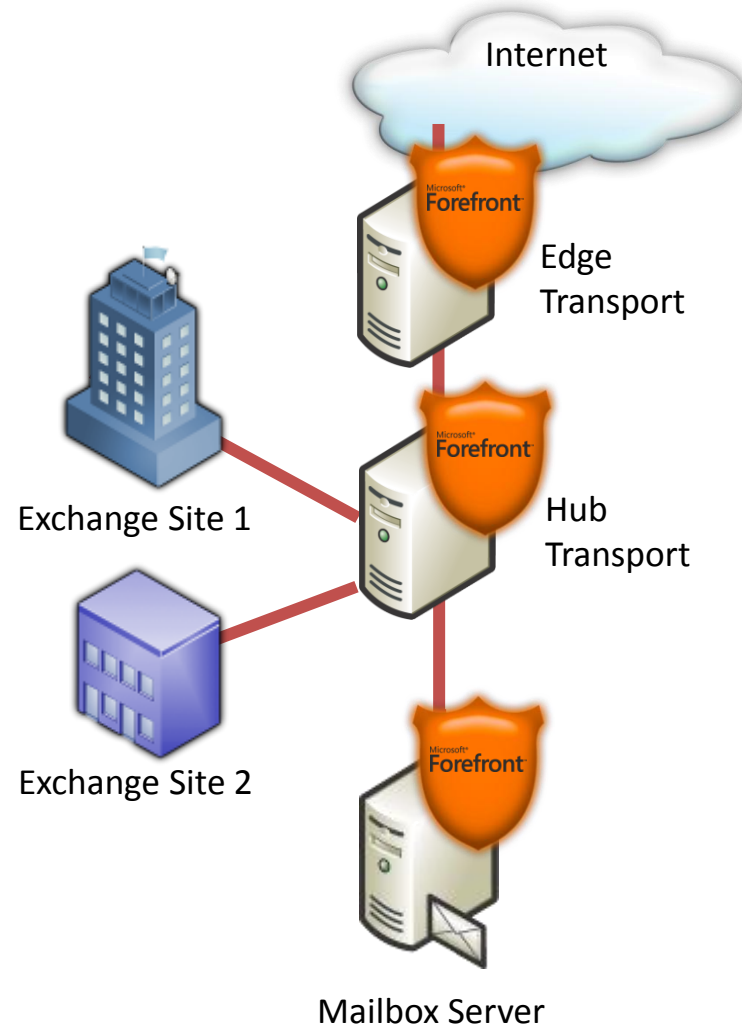
Bereich	Vorgänger	Aktuell	Beschreibung
Management	Microsoft Identity Lifecycle Manager 2007 (ILM)	Forefront Identity Manager 2010 (FIM)	Zentrale Verwaltung von Benutzeridentitäten und den dazugehörigen Berechtigungen
Management	Forefront Server Security Management Console (FSSMC)	Forefront Protection Server Management Console 2010 (FPSMC)	Zentrale Management und Monitoring Konsole für FPE und FPS
Protection	Forefront Client Security (FCS)	Forefront Endpoint Protection 2010 (FEP)	Antiviren-Lösung für den Desktop
Protection	Forefront Security for Exchange Server (FSE)	Forefront Protection 2010 for Exchange Server (FPE)	Antiviren- und Antispam-Lösung für den Exchange Server
Protection	Forefront Online Security for Exchange (FOSE)	Forefront Online Protection for Exchange (FOPE)	Antiviren- und Antispam-Lösung für den Exchange Server in der Cloud
Protection	Forefront Security for SharePoint (FSSP)	Forefront Protection 2010 for SharePoint (FPSP)	Antiviren-Lösung für den SharePoint Server
Protection		Forefront Security for Office Communications Server (FSOCS)	Antiviren-Lösung für den Office Communications Server
Edge	Microsoft Internet Security & Acceleration Server 2006 (ISA)	Forefront Threat Management Gateway 2010 (TMG)	Firewall, Proxy, Cache, Deep-Inspection, Secure Webgateway
Edge	Microsoft Intelligent Application Gateway 2007 (IAG)	Forefront Unified Access Gateway 2010 (UAG)	SSL-VPN mit Portalbildung, sowie prädestiniert für DirectAccess

Das ist Forefront ...



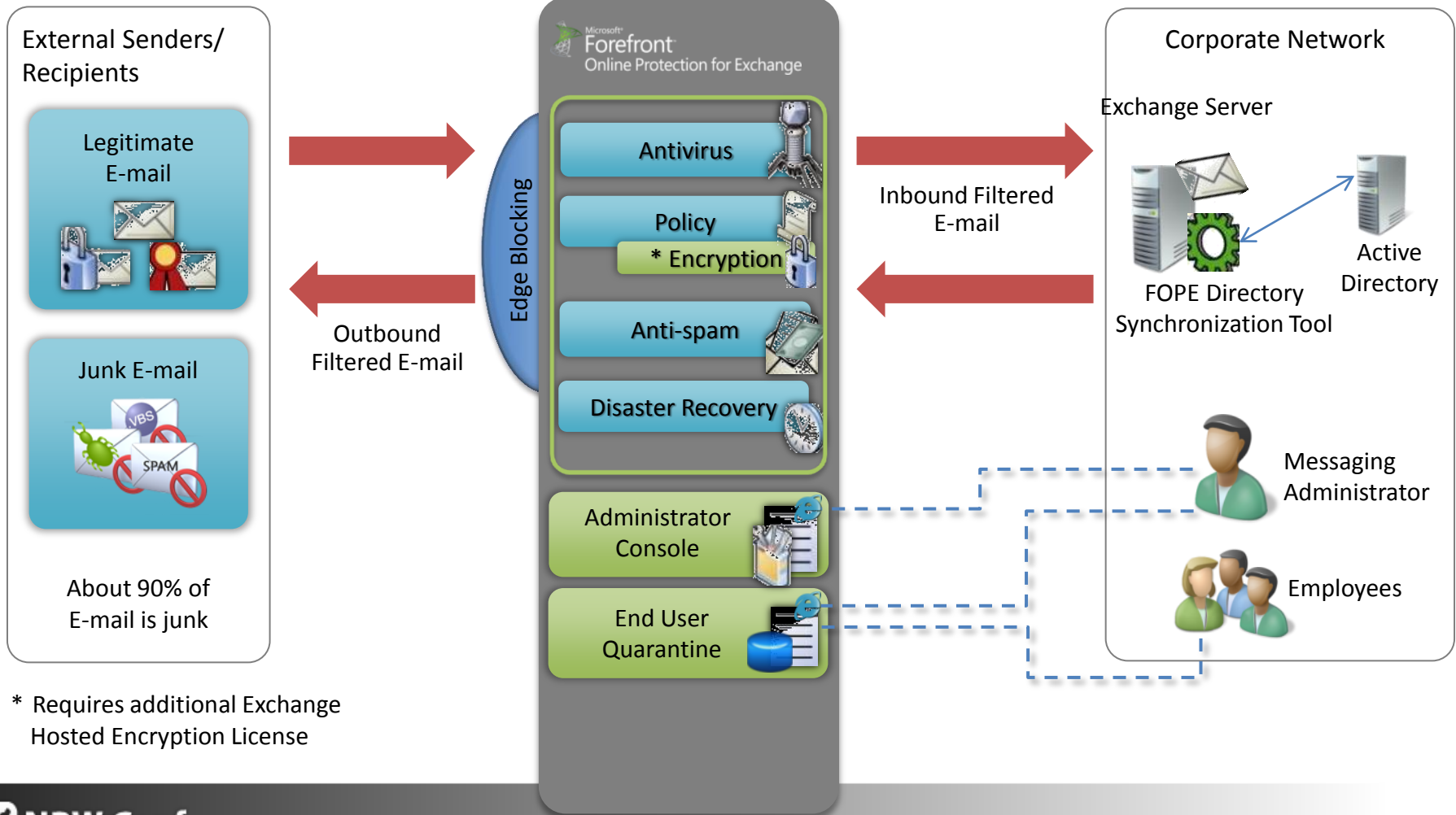
FPE

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



FOPE

Multilayer Antispam + Antivirus und Durchsetzung von Filterregeln



TMG und UAG

Gestern

Microsoft®
Internet Security &
Acceleration Server 2006

Protection

... keep the bad guys out!

Intelligent Application
Gateway 2007

Access

... let the good guys in!

Heute

Microsoft®
Forefront™
Threat Management Gateway

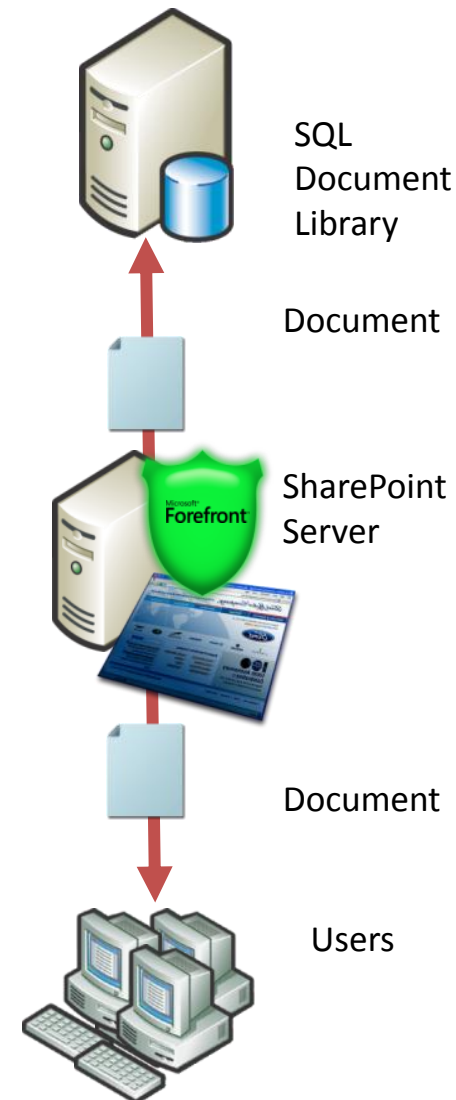
**Unfassender Schutz vor Web-
basierten Bedrohungen**

Microsoft®
Forefront™
Unified Access Gateway

**Universale Plattform für alle
Remote Access Bedürfnisse**

FSSP

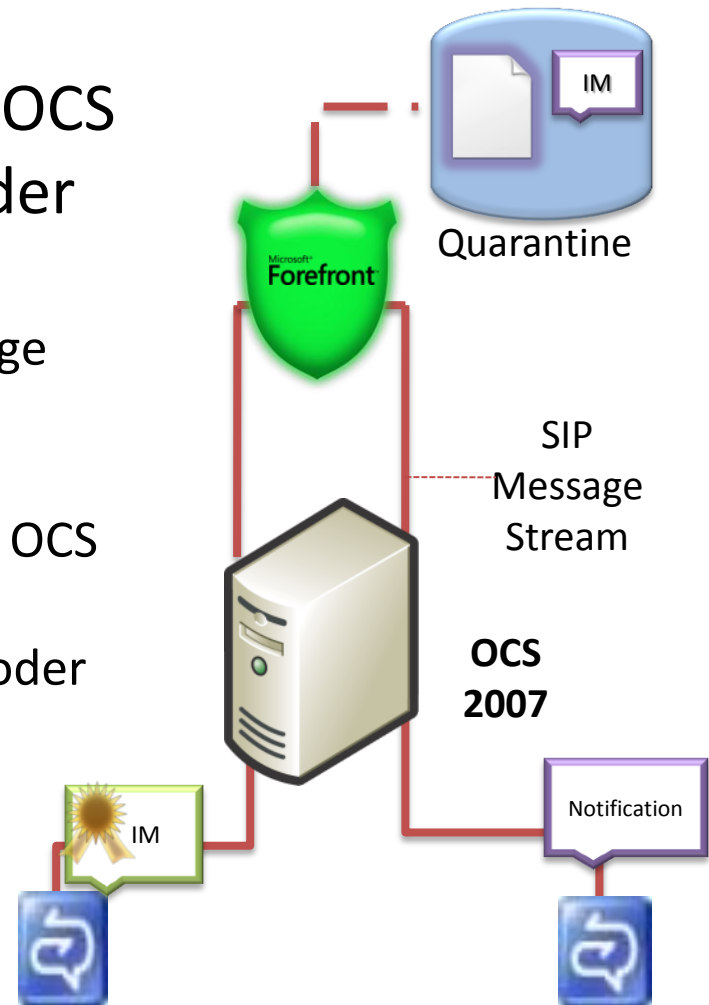
- Virenschutz für die Dokumenten-Bibliothek, nutzt VSAPI
 - Echtzeitschutz beim Up-und Download von Dokumenten in die SQL-Datenbank
 - Manuelle und zeitgesteuerte Scans
- Durchsetzen von inhaltlichen Richtlinien
 - Dateifilter können auf Basis von Dateinamen, Dateiendung und Dateityp angewendet werden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



FSOCS

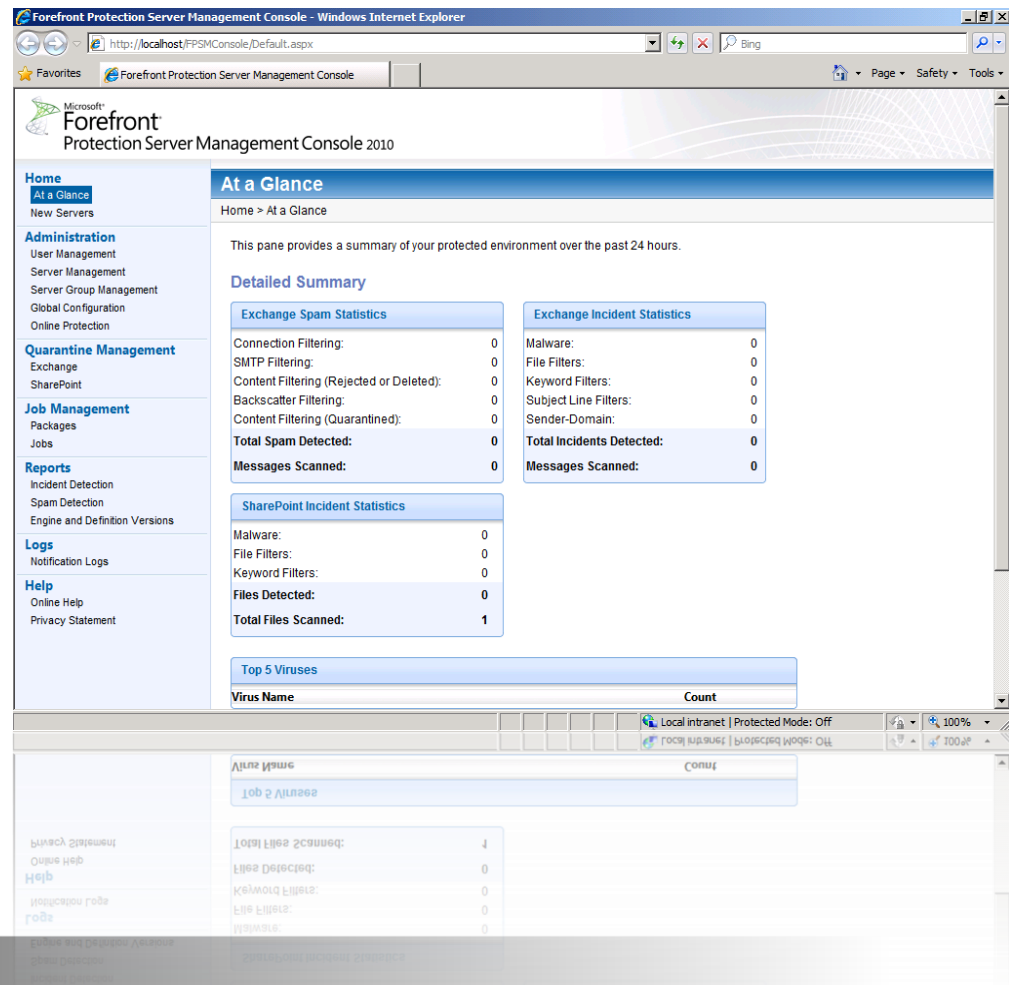
SIP-Nachrichtenstrom wird durch FSOCS geroutet, Forefront hängt dabei an der VSAPI von OCS.

- Identische AV-Engines und Filterwerkzeuge wie Forefront Protection für Exchange
- Geprüfte Nachrichten und Filetransfers werden gestempelt (AV-Stamp) und durch OCS weitergeleitet
- Infizierte Dateien werden blockiert und/oder in Quarantäne gestellt
- Benachrichtigung wird an den Administrator gesendet
- IM Sender / Empfänger werden informiert



FPSMC

- Verwaltet Forefront Protection für Exchange und SharePoint Server
- Web-basiert
- Zentrale Verteilung von Server-Konfigurationen
- Engine- und Signatur-Updates
- Monitoring und Reports
- Konsolidierte Quarantäne inkl. Release (auf „original“ Server)



FEP



Desktop Administrator

- Uses SCCM to perform daily tasks
- "What's the deployment status of FEP?"

Interactive
Experience



Security Administrator

- Be informed in case of an incident
- Audit Security Compliance

Typically daily/
weekly / monthly

Dashboard



Operational State Monitoring:

- ✓ FEP Client Deployment (and Health)
- ✓ FEP Policies Distribution Status
- ✓ FEP AM Activity Status (Security)
- ✓ FEP Compliance Baselines

Design Principles

- ✓ Integrated within SCCM Console
- ✓ Using DCM Checks to ensure Compliance
- ✓ Use SCCM Dynamic Collections to ensure Policy adherence through targeting specific Computer groups

Alerts



Security Incidents Notification:

- ✓ "Malware Outbreak"
- ✓ Malware Activity on sensitive Computers

Design Principles

- ✓ Admin configurable thresholds
- ✓ Subscription based forward by Email
- ✓ Alert issued within a few minutes from incident in nominal traffic periods

Reports



Security and Compliance Reporting:

- ✓ Protection status and Trend
- ✓ Security Incidents (Malware Detections)
- ✓ Alerts History

Design Principles:

- ✓ Match FCS v.1 capabilities (6-8 reports)
- ✓ Using SQL Reporting Services
- ✓ Subscription based Reports by Email
- ✓ Public Schema for Customization

FIM



Lizenzierung

- Einzelprodukte der Forefront-Familie als User Subscription License (pro User o. Device)
- Einzelproduktsuiten oder CAL's über alle Volumen Lizenz Programme erhältlich; Software Assurance

<i>Produkte</i>	<i>Enterprise CAL **</i>	<i>Exchange Enterprise CAL</i>	<i>Forefront Protection Suite</i>
Forefront Protection for Exchange	✓	✓	✓
Forefront Protection for Sharepoint	✓		✓
Forefront Security for OCS	✓		✓
Forefront Endpoint Protection	✓*		✓*
Forefront Online Protection for Exchange	✓	✓	✓
Exchange UM + Compliance	✓	✓	
Other Server CALs	✓	✓	
<i>Forefront TMG AM-/URL-Filtering</i>	✓		✓
<i>Forefront UAG (CAL)</i>	✓		
<i>Forefront Identity Manager</i>	✓		

****** Enterprise CAL enthält außerdem Core CAL Komponenten, RMS, MOM: Desktop OML, SPS EE, Exchange UM, und LCS
***** Management Console separat (mit oder ohne SQL 2005 EE) für Management/Reporting zu lizenzieren

Und was kann ich nun mit Forefront
machen?

Demo

Demo Szenarien

User Zugriff aus Internet auf UAG Portal mit Exchange

- UAG im Einsatz
- FPE im Einsatz
- FPSMC im Einsatz

User Zugriff aus Intranet Zugriff auf Internet ueber TMG

- TMG im Einsatz

Client Virenschutz

- FEP im Einsatz

Lust auf Links



- Microsoft Forefront Webseite
 - <http://www.microsoft.com/forefront/en/us/default.aspx>
- Forefront TMG Webseite Karsten Hentrup & Marc Grote
 - <http://www.forefront-tmg.de/>
- ISA Server FAQ (Dieter Rauscher + Coautor Christian Groebner und Marc Grote)
 - <http://www.msisafaq.de/>
- ISA Server Org
 - <http://www.isaserver.org/>
- Forefront Blog Deutsch
 - <http://www.forefront-blog.de/>
- Forefront Team Blog
 - <http://blogs.technet.com/b/forefront/>

Fragen?



Kontakt

- **Marc Grote**
- E-Mail: grotem@it-training-grote.de (7*16*365)
- Web: <http://www.it-training-grote.de>
- Blog: <http://blog.it-training-grote.de>
- XING:
[https://www.xing.com/profile/Marc Grote2](https://www.xing.com/profile/Marc_Grote2)
- Mobile: 0176/23380279 (manchmal)
- MSN: Was ist das? ☺
- Twitter: Nicht mit mir
- Facebook: Was bitte?

