

FOREFRONT THREAT MANAGEMENT GATEWAY



Marc Grote

IT TRAINING GROTE

****ice:2008**

intelligent communities for europe

30.08.2008 :: Lingen/Ems

Inhalt




- Überblick über die Microsoft Forefront Produktfamilie
- Unterschiede ISA – TMG
- TMG Funktionen
- TMG praktisch
- Integration mit Microsoft Stirling
- Ausblick Microsoft Forefront UAG

Wichtiger Hinweis

- Die in diesem Vortrag gezeigte TMG Version ist eine oeffentlich verfuegbare Beta Version
- Nicht oeffentlich verfuegbare Versionen sind fuer einen geschlossenen Benutzerkreis verfuegbar
- Alle Angaben ohne Gewaehr
- Die gezeigten Funktionen koennen jederzeit geaendert werden



Microsoft Forefront Produktfamilie

• Client And Server OS	• Server Applications	• Network Edge
 <p>Microsoft® Forefront™ Client Security</p>	 <p>Microsoft® Forefront™ Security for Exchange Server</p> <p>Microsoft® Forefront™ Security for SharePoint®</p>	 <p>Jetzt</p> <p>Microsoft® Internet Security & Acceleration Server 2006</p> <p>Intelligent Application Gateway 2007</p>

Bald Microsoft Forefront Threat Management Gateway
Microsoft Forefront Unified Access Gateway



Microsoft Forefront Client Security

Proactive

Ausführung nur erlaubter / gewünschter Anwendungen

Reduzierte Angriffsfläche

Beschränkung, was Anwendungen ausführen dürfen

Blocken bekannter und unbekannter Gefahren

Minimieren oder Verhindern der Zero Day Exploits

Blockieren, entfernen und bereinigen von Malicious Software

Reactive

Software Restriction Policies

Vulnerability Assessments

Host Firewall

Vulnerability Remediation

HIPS (GAPA)

Antivirus/
Antispyware



Microsoft Forefront Server Security

- **Multi Engine Antivirus** Verbesserte Virenerkennung
- **Premium Anti-spam** Verbesserte Erkennungsraten
- **Spyware scanning (MSAV engine)** Spyware Erkennung
- **Heuristic Detection** Erkennt Zero-Day Attacken
- **Malicious and Phishing URL Filtering** Setzt e-mails in Quarantaene, welche URLs enthalten, welche auf Malware oder Phishing Links zeigen
- **Support fuer die naechste Exchange und Sharepoint Version**
 - Erweitert Exchange 2007, SharePoint 2007 und WSS 3.0 Unterstuetzung
- **Content Filtering and Confidential Information Scanning**
Schuetzt gegen elektronischen Datendiebstahl



Microsoft Forefront Produktfamilie

Heute

Microsoft®
**Internet Security &
Acceleration Server 2006**

**Network
Protection**

**Intelligent Application
Gateway 2007**

**Network
Access**

Bald

Microsoft®
Forefront™
Threat Management Gateway

***Integrated and
comprehensive protection
from Internet-based threats***

Microsoft®
Forefront™
Unified Access Gateway

***Unified platform for all
enterprise remote access
needs***



Microsoft Forefront TMG Funktionen

- Integrierte „All in one“ Firewall, VPN, Proxy, Cache und Anti Malware Loesung
- Verbesserte Integration in die Microsoft Forefront Produktfamilie
- Vereinfachte Verwaltung mit Hilfe von Assistenten
- Subscription Services fuer Anti Malware etc.



Comprehensive



Integrated



Simplified



Microsoft Forefront TMG Szenarien



Control Network Policy Access at the Edge (Firewall)

- Enable admins to control which network traffic is allowed in & out of their organization



Protect users from Web browsing threats (Web Client Protection).



Protect desktops and servers from Intrusion attempts (IPS)

- Securely connect corporate resources to the Internet while protecting from intrusion attempts.



Enable Users to Remotely Access Corporate Resources (VPN, SWP)

- Securely connect to the corporate resources and applications from remote.



Simple Deployment & Management

- Easily deploy & configure the different scenarios

Firewall

- Erweitertes NAT (Weitere Informationen in Kuerze)
- Firewall-Aenderungsnachverfolgung (ab ISA 2006 SP1)
- Edge Ready – Gehaertet von Anfang an
- Verschiedene Anwendungs- und Webfilter
- Weitere neue Filter – Lassen Sie sich ueberraschen
- TFTP-Filter



Web Client Schutz

- HTTP Proxy und Cache
- Edge Malware Schutz
 - Microsoft Antivirus
 - Schutz nicht verwalteter Clients
- Neuerungen im Bereich HTTPS Inspection
- Weitere Filtermoeglichkeiten



RAS / VPN / SWP

- Roaming Client Zugriff
 - IPSEC und SSTP (Secure Socket Tunneling Protocol)
- VPN Quarantaene (NAP)
- Standort zu Standort VPN
- Sichere Webserververoeffentlichung
- Erweiterte Loesung durch das UAG
 - Portal basierend
 - Verfeinerter Remote Zugriff
 - Endpunkt-Schutz



Genug der Worte

Demo



Diverses

- Subscription Services
 - Anti Malware Signaturen (Web- und E-Mail)
 - URL Filterung
 - IPS Signaturen
- Telemetry
 - Erweiterte Erkennung und Verwaltung von Signaturen durch das Senden proaktiver Informationen an Microsoft
- Plattform-Änderungen
 - Ausschliesslich 64 Bit Plattform
 - Basiert auf Windows Server 2008
 - Voraussichtlich verfügbare als Appliance



Microsoft®

Forefront™

Code Name "Stirling"

An Integrated Enterprise Security System that delivers comprehensive, coordinated protection with simplified management and critical visibility across clients, servers, and the network edge

Comprehensive Protection

- Integrated protection across clients, server & edge
- Dynamic responses to emerging threats
- Next generation protection technologies

Simplified Management

- Manage from a single role-based console
- Asset and policy centric model
- Integrates with your existing infrastructure

Critical Visibility

- Know your security state in real-time
- View insightful reports
- Investigate & remediate security issues

Microsoft Forefront Stirling

Enterprise Security Assessment

Information Sharing

Coordinated Defense

Adaptive Investigation

Microsoft®
Forefront™
Client Security

vNext

**Antivirus
Antispyware**

Host Firewall

**Host Intrusion
Prevention System**

Device Control

Software Restriction

**Vulnerability
Assessment &
Remediation**

Microsoft®
Forefront™
Security for Exchange Server

vNext

**Geheim –
NDA!**

Microsoft®
Forefront™
Security for SharePoint®

vNext

**Geheim –
NDA!**

Microsoft®
Forefront™
Threat Management Gateway

NEW

Firewall

Web (URL) Filtering

HTTP/FTP AV

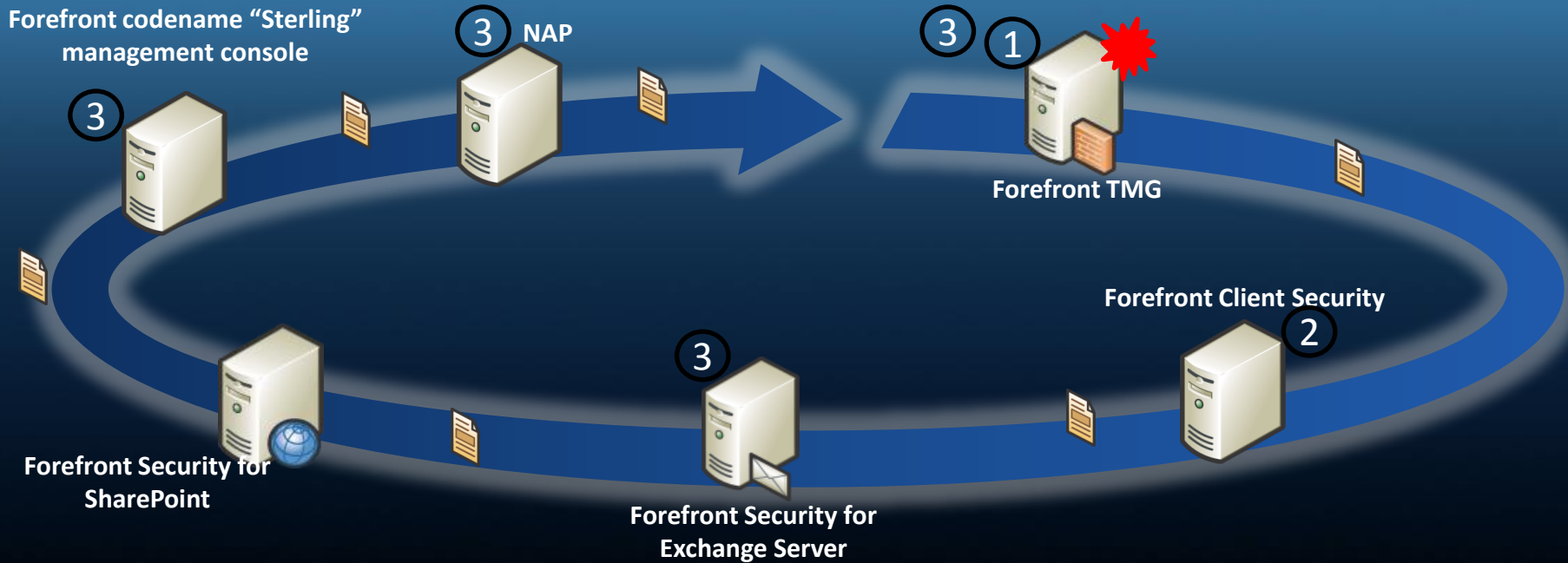
**Network Intrusion
Prevention**

Remote Access

**Network Access
Protection**

**Active Directory
Protection**

Integration aller Komponenten



Geheim – NDA!

Daher keine weiteren Informationen



TMG / Stirling Integration

- Informationen noch nicht(alle) oeffentlich verfuegbar

**Geheim –
NDA!**

Beta Version verfuegbar:

[http://technet.microsoft.com/de-de/evalcenter/cc339029\(en-us\).aspx](http://technet.microsoft.com/de-de/evalcenter/cc339029(en-us).aspx)

Microsoft Forefront UAG

- Microsoft Forefront Unified Access Gateway
- Nachfolger des Microsoft IAG (Intelligent Application Gateway 2007)
- SSL basierter VPN Zugriff
- Integrierte Portal Loesung
- NAP Integration



Microsoft Forefront UAG

- Zentrale Array Verwaltung
- Terminaldienste Integration
- Erweiterte Verwaltung und Management (SCOM Pack)
- Erweiterte Mobility Loesungen
- Assistenten gefuehrte Konfiguration



TMG versus 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)	✓	

www.msisafaq.de

- Betreiber Dieter Rauscher
- Nach Microsoft die meistbesuchte Webseite zum Thema ISA Server / TMG
- Deutschsprachige Anleitungen und weitere Informationen zu ISA Server 200x und (in Zukunft) Microsoft Forefront TMG und UAG
- Coautoren Christian Groebner und Marc Grote



Die deutschen Microsoft Forefront MVP



Marc Grote –

Grotem@it-training-grote.de

Blog:

<http://www.it-training-grote.de/blog>



Im ATE Bereich

Dieter Rauscher –

Dieter.Rauscher@msisfaq.de

Blog:

<http://msmvps.com/blogs/rauscher>



Im ATE Bereich

Christian Gröbner –

Newsgroups@groeby.net



com for children



Fragen?



Das Ende

Vielen Dank fuer Ihre Aufmerksamkeit

