

ICE2005
Intelligent Communities for Europe

Microsoft Internet Security & Acceleration Server 2004

Einführung und Funktionen

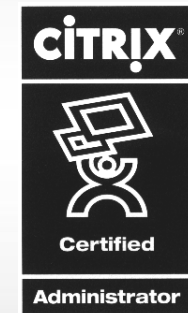


Agenda

- **Vorstellung IT TRAINING GROTE**
- **Firewallgrundlagen**
- **ISA Server 2004 Versionen**
- **ISA Server 2004 Leistungsmerkmale**
- **ISA Server 2004 Mehrfachnetzwerke**
- **ISA Server 2004 Übersicht - GUI klicken**
- **ISA Server 2004 Basis-Einrichtung**
- **ISA Server 2004 Monitoring**
- **ISA Server 2004 VPN**
- **ISA Server 2004 Enterprise**
- **Zukunft**
- **Werbung**
- **ISA Server 2004 Tech@Night**
- **Lust auf Links?**

IT TRAINING GROTE – I

Mehr Schein als Sein



Berufserfahrung ist aber auch nachweisbar:

17 Jahre in der IT

Davon 10 Jahre Trainer / 7 Jahre Consulting

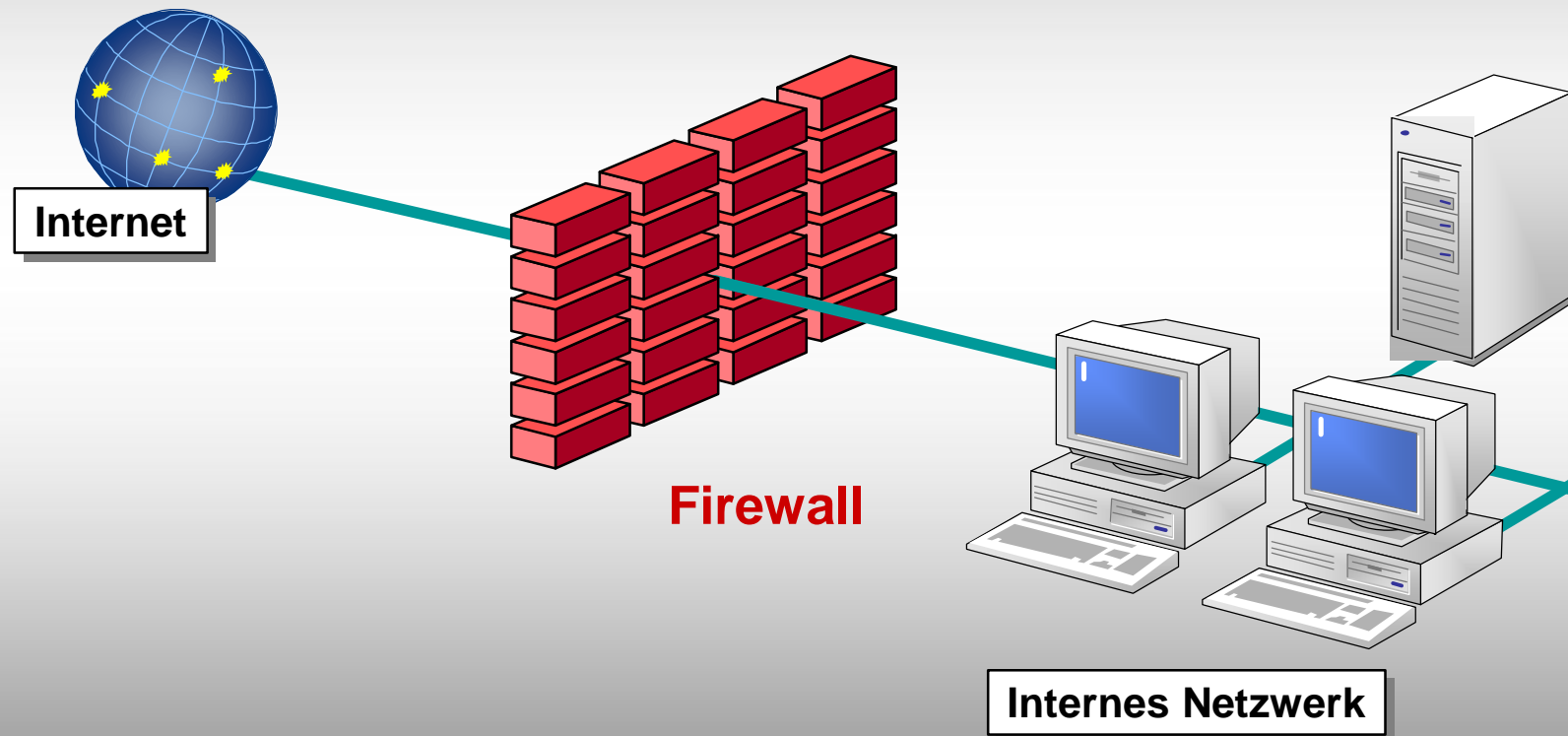
IT TRAINING GROTE – II

(Die letzte Beweihräucherung)

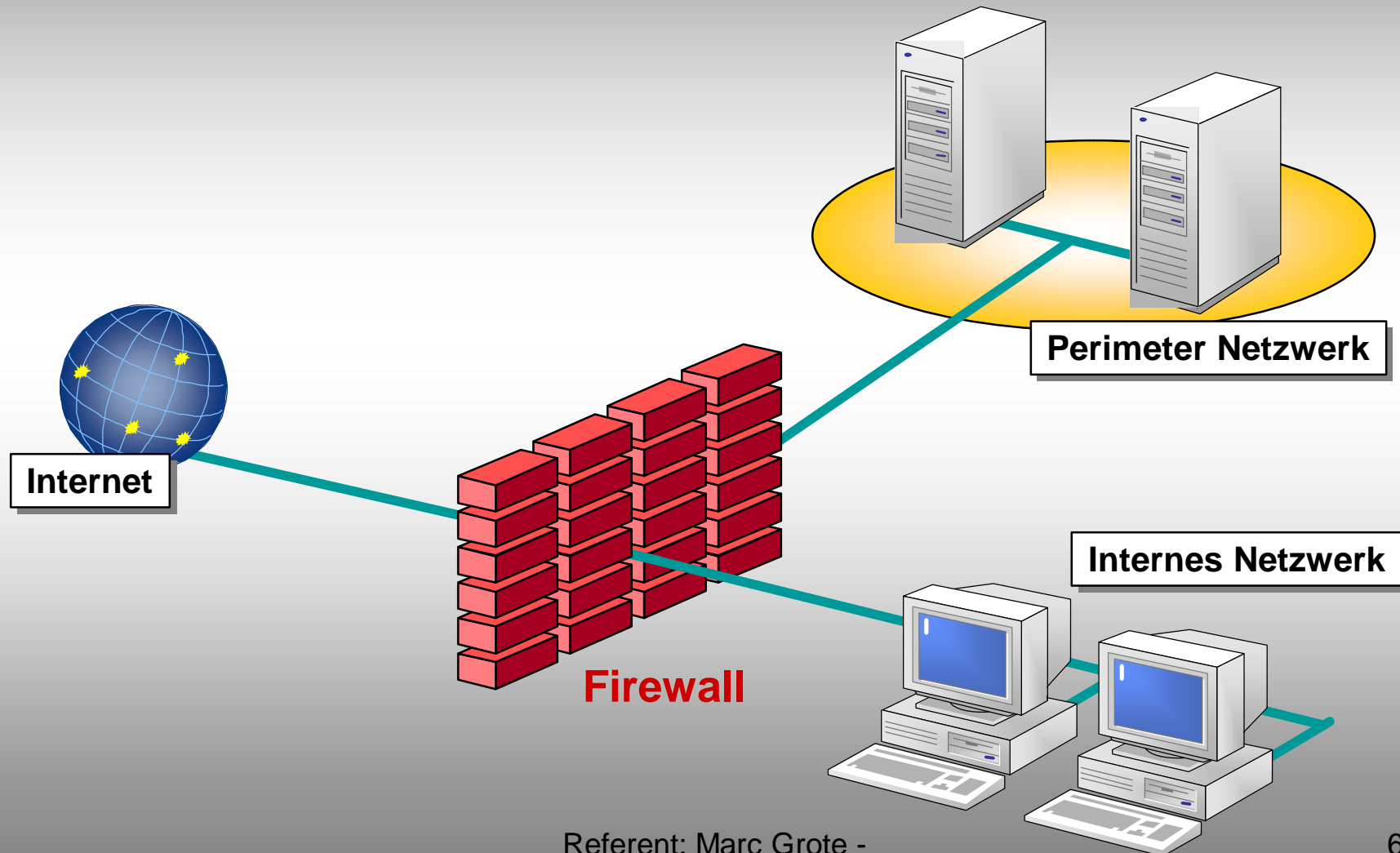
Warum sollte ich in meiner Firma einen ISA Server durch IT TRAINING GROTE implementieren lassen?

- Diverse ISA Server Projekte und Kundenimplementationen
- Microsoft ISA Server MVP
- Autor für www.msisafaq.de
- Microsoft Press Buch ISA Server 2004
- Tätigkeiten in diversen ISA Server Newsgroups (Pseudonym: Jens Baier)

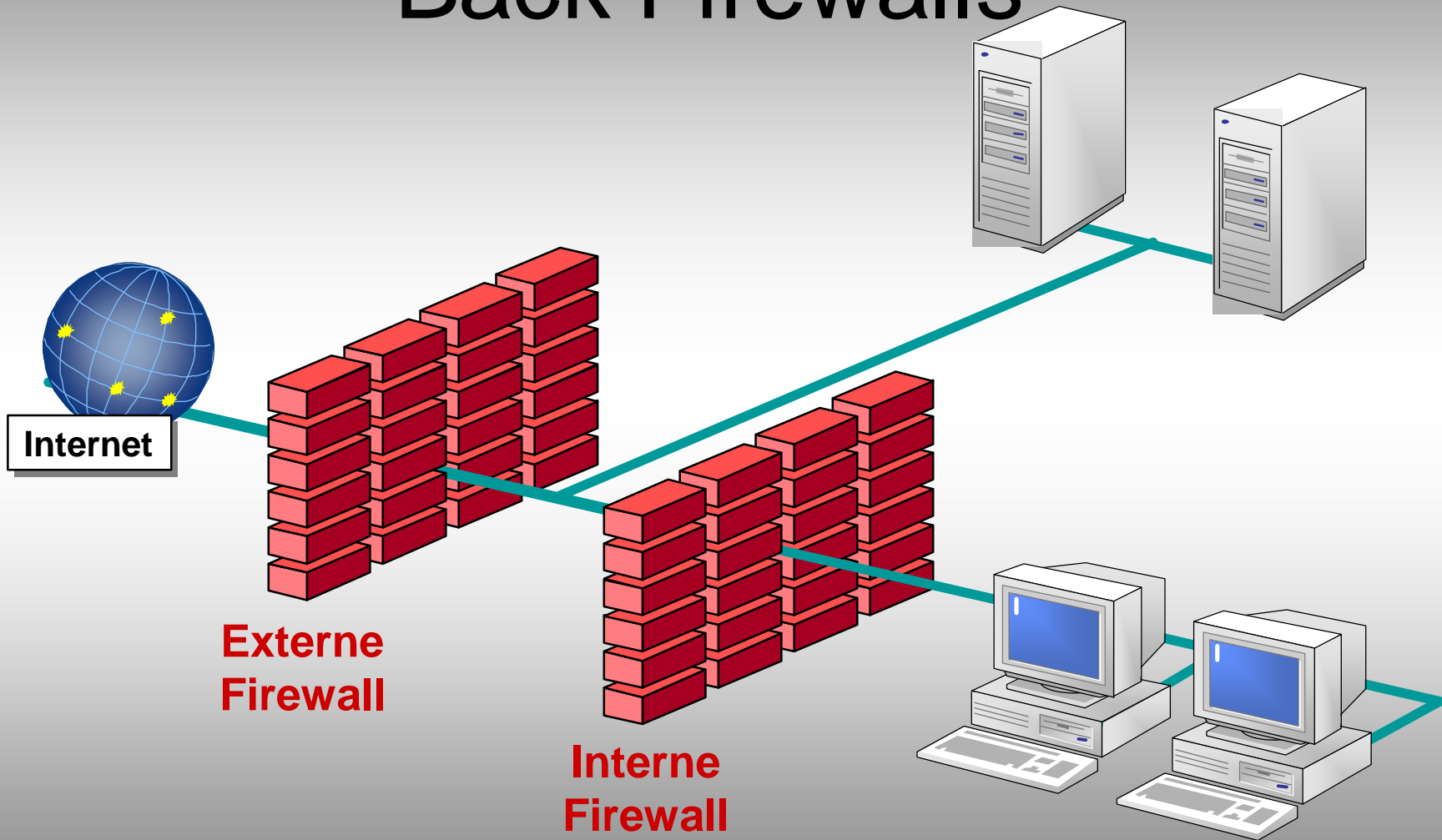
Firewallgrundlagen - Bastion Host



Perimeter Netzwerk mit Trihomed Firewall



Perimeter Netzwerk mit Back-to-Back Firewalls



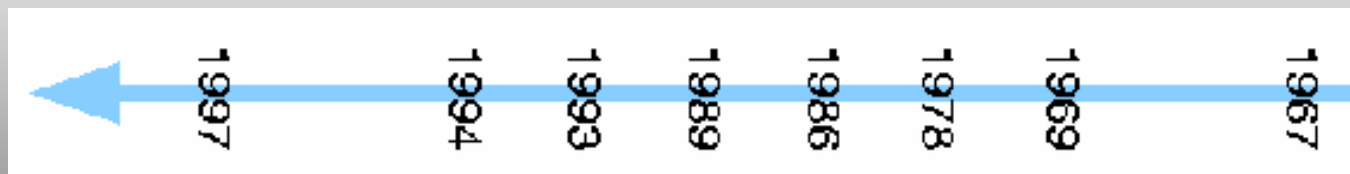
ISA Server Versionen

ISA Server 2004 ist in zwei Versionen verfügbar . . .

- ISA Server 2004 Standard
 - Multilayer Firewall + Proxy Server
 - Alle Funktionen einer richtigen Firewall
- ISA Server 2004 Enterprise
 - Alle Funktionen von ISA Server 2004 Standard +
 - NLB (Network Load Balancing)
 - Enterprise und Array-Policies
 - CARP (Cache Array Routing Protocol)
 - Zentrales Logging und Reporting

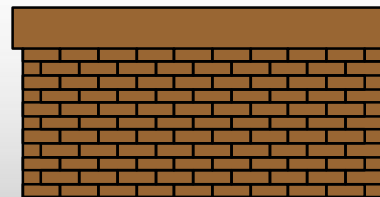
Proxy / ISA Server Historie

- Microsoft Proxy Server 1.0 (14.01.1997)
- Microsoft Proxy Server 2.0 (25.12.1997)
- Microsoft ISA Server 2000 (18.03.2001)
- Microsoft ISA Server 2004 (08.09.2004) –
Launch in Germany am 16.07.2004 – durch Dieter Rauscher



ISA - Einführung

- **Umfassender Schutz bis auf die Anwendungsebene**
- **Die ideale Firewall für sichere Microsoft Exchange Server-Veröffentlichung**
- **Die ideale Firewall für sichere Microsoft Exchange Server-Veröffentlichung**
- **Einfache und sichere Veröffentlichung von Webservern**
- **Common Criteria EAL4+-Zertifizierung: In Kürze**
- **Netzwerkvorlagen und XML Import**
- **Firewall (ALF, Stateful) + Proxy Server + VPN Server**
- **Verfügbar als Standard und Enterprise Version**
- **Verfügbar als Appliance**
- **VPNs (Client VPN, Site to Site VPN)**
- **Server- und Web-Veröffentlichung**
- **Monitoring & Reporting**
- **Erweiterbare Inhaltsfilterung und ein großes Netz von Partnern**
- **Integrierter Webcache und hierarchisches Caching**
- **Benutzerspezifische Authentifizierung an der Firewall**
- **Microsoft Windows-VPN und integrierte Quarantänefunktion**

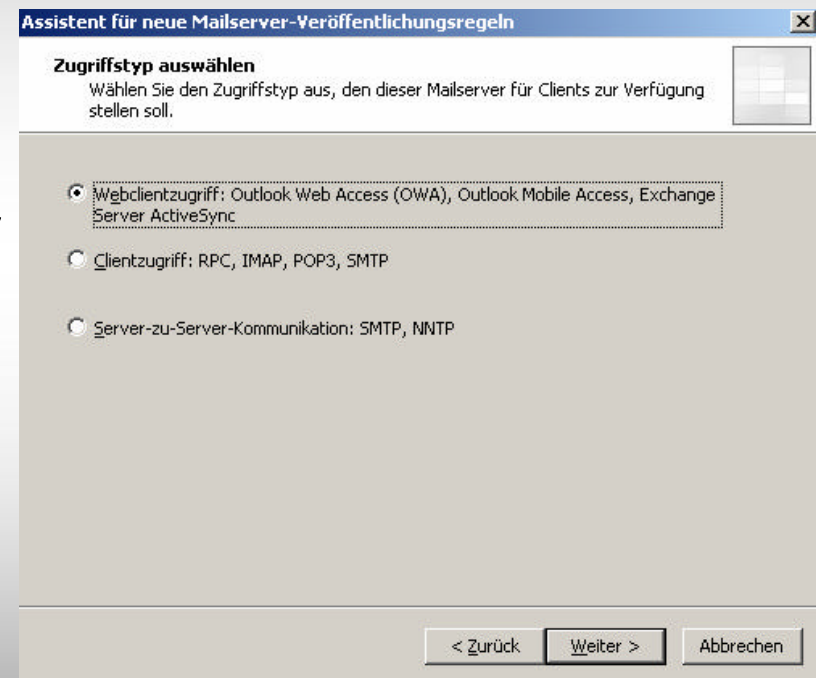


Neue Funktionen

- **Neue, vereinfachte Benutzeroberfläche**
- **Flexible Unterstützung für unterschiedliche Netzwerk-Designs**
- **Verbesserte VPN-Unterstützung**
- **VPN-Quarantänefunktionen**
- **Möglichkeit zur Erstellung benutzerdefinierter Firewallbenutzergruppen**
- **Erweiterte Protokollunterstützung / Individuelle Protokolldefinitionen**
- **OWA-Veröffentlichungs-Assistent**
- **Verbesserte Unterstützung für FTP-Upload-/Downloadrichtlinien**
- **Verbesserte Webveröffentlichung**
- **Portumleitung für Serververöffentlichungsregeln**
- **Verbesserte Cacheregeln für eine zentrale Objektspeicherung**
- **RADIUS-Unterstützung für Webproxycient-Authentifizierung**
- **Delegierung der Standardauthentifizierung**
- **SecureID-Authentifizierung**
- **Durch die Firewall generierte Formulare (formularbasierte Authentifizierung)**
- **Verbesserte SMTP-Nachrichtenüberwachung**
- **Verbesserte HTTP-Filterung**
- **Linkübersetzung**
- **Verbesserte Überwachung und Berichterstellung**

ISA Server Funktionen

- Server Veröffentlichung
 - Web Server
 - Exchange Server
 - Weitere Server
- Anwendungsfiler, Webfilter
 - SMTP
 - DNS
 - HTTP
 - Streaming Media
- VPN Wizard
- Intrusion Detection



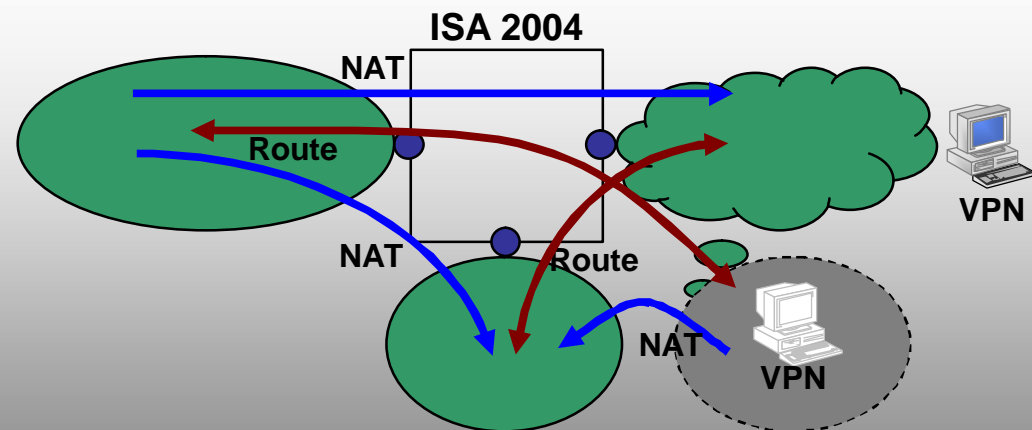
ISA Server Szenarien

- Edge Firewall
 - Caching
 - Webverkettung
- Veröffentlichung
 - Exchange
 - Web Server
- Remote Access (VPN)
Standorte
 - Remote Standort
Sicherheit
 - S2S VPN (IPSec)
- Integrierte Lösung
 - Single Server
Sicherheitslösung
 - Einfaches, einheitliches
Management
- Flexible Topologie
 - 3-Leg, Front/Back, ...
 - Multi Netzwerk
Unterstützung

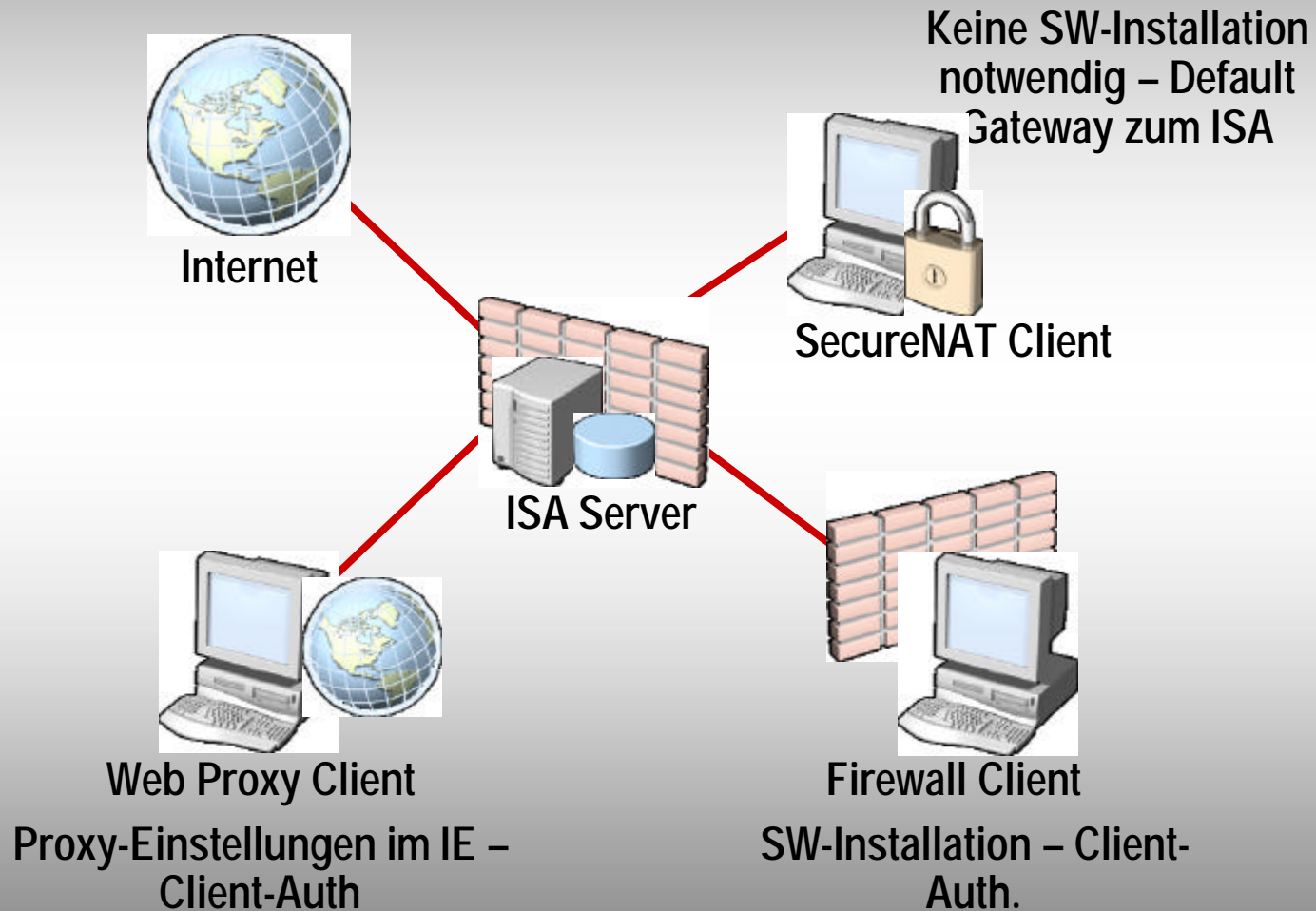
Mehrfachnetzwerke

Name	Adressbereiche
Entwicklung	172.15.1.0 - 172.15.1.255
Extern	Für die ISA Server-Netzwerke externe IP-Adressen
Hamburg	10.14.0.0 - 10.14.255.255
Intern	192.168.1.0 - 192.168.1.255
Lokaler Host	Mit diesem Netzwerk sind keine IP-Adressen assoziiert.
Muenchen	192.8.200.0 - 192.8.200.255
Quarantäne-VPN-Clients	Diesem Netzwerk sind zurzeit keine IP-Adressen zugeordn
VPN-Clients	Diesem Netzwerk sind zurzeit keine IP-Adressen zugeordn

Netzwerkregeln



ISA Server - Clients



Praxis – GUI klicken

Microsoft Internet Security & Acceleration Server 2004 Enterprise Edition

Konfigurationsspeicherserver: isa2004.isadom.intern Unternehmensnetzwerke

Name	Adressbereiche	Beschreibung
Extern		Repräsentiert alle Computer, die in keinem anderen Netzwerk er
Lokaler Host		Repräsentiert die Computer, auf denen ISA Server-Dienste aus
Quarantäne-VPN-Clients		Repräsentiert die Clientcomputer, die mit dem ISA Server-VPN v
VPN-Clients		Repräsentiert die Clientcomputer, die mit dem ISA Server-VPN v

Praxis

ISA Server 2004 Neue Funktionen

Erweiterter Schutz

Application Layer Sicherheit zum Schutz von Microsoft Applikationen

Inhaltsüberprüfung

- Erweiterter HTTP-Filter und weitere Anwendungsfiler
- Stateful Routing

Erweiterte Exchange Server Integration

- Unterstützung für Outlook RPC over HTTP
- Erweiterter Outlook Web Access Sicherheit
- Konfigurationsassistenten (Wizards)

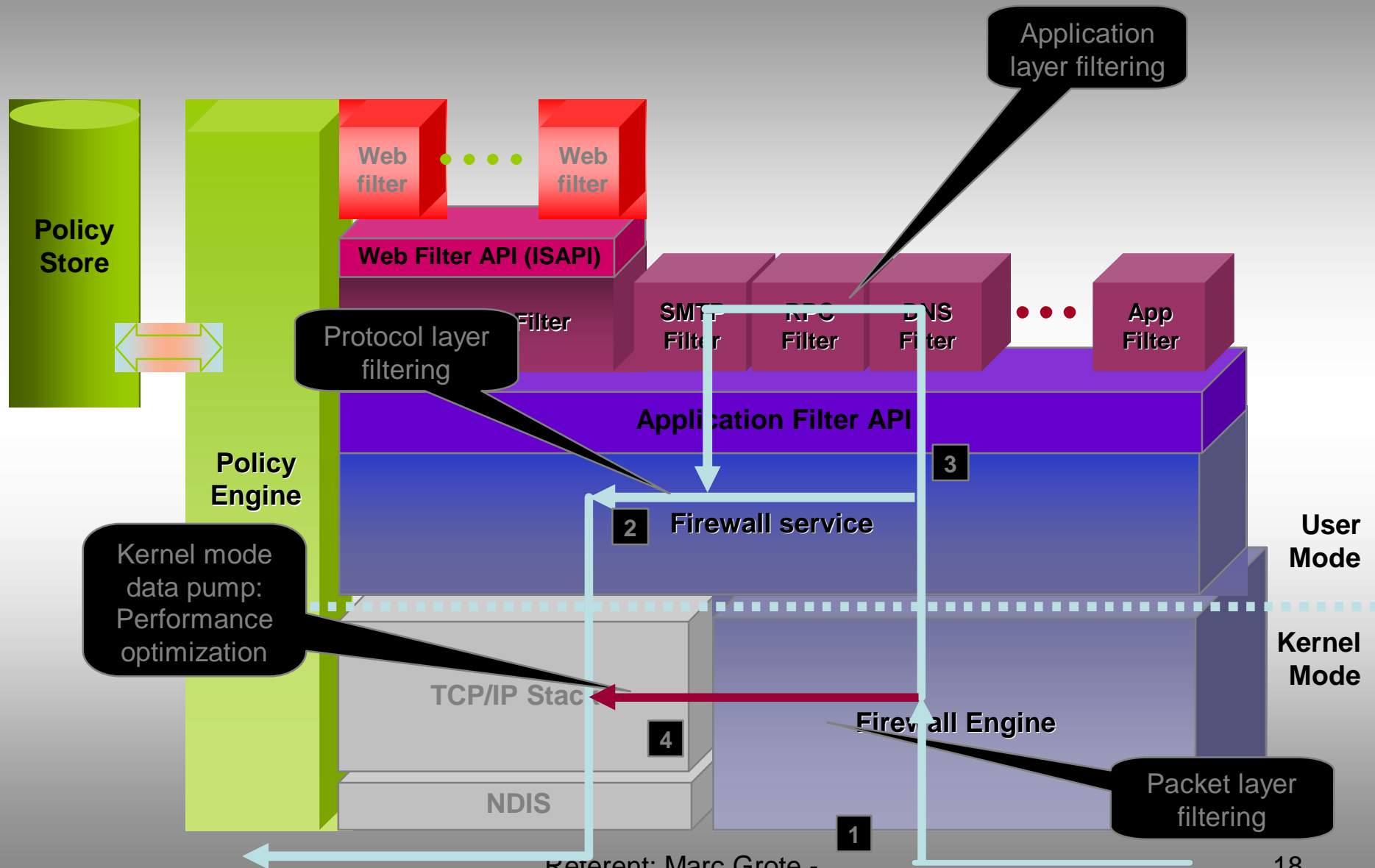
Voll integriertes VPN

- Firewall-VPN Filterung
- Site to Site IPSEC
- VPN Quarantäne

Vielfache Authentifizierungsmeth.

- Unterstützung für RADIUS und RSA SecurID
- Benutzer- und Gruppenbasierte Regeln
- Erweiterung durch ThirdParty

ISA 2004 Architektur



Application Layer Filtering (ALF)



- Moderne Bedrohungen erfordern neue Lösungen (HTTP/S = Universal Firewall Bypass Protocol)
 - Schutz gegen Nimda, Slammer... und Co.
 - Erweiterter HTTP-Filter, Signaturen, URL-Schutz
 - Beste Unterstützung für Microsoft Anwendungen
- Anwendungsfiler Framework
 - Filter für allgemeine Protokolle
 - HTTP, SMTP, RPC, FTP, H.323, DNS, POP3, Streaming Media
 - Einfach erweiterbare Architektur (SDK)


Praxis – GUI klicken

HTTP-Richtlinie für diese Regel konfigurieren

Allgemein Methoden Erweiterungen Header Signaturen

Anforderungsheader

Maximale Headerlänge (Bytes): 32768

 Diese Einstellung betrifft alle Regeln. Hinweis: die aktuelle Unternehmensrichtlinie begrenzt die maximale Headerlänge auf 32768 Byte.

Anforderungsnutzlast

Jede Nutzlastlänge zulassen

Maximale Nutzlastlänge (Bytes):

URL-Schutz

Maximale URL-Länge (Bytes): 10240

Maximale Abfragelänge (Bytes): 10240

Normalisierung verifizieren

High Bit-Zeichen sperren

Ausführbare Dateien

Antworten sperren, die von Windows ausführbaren Inhalt enthalten

OK Abbrechen Übernehmen

Konfiguriert die FTP-Protokollrichtlinie.

Protokoll

Definieren Sie die FTP-Protokollrichtlinie für verwandte Regeln.

Nur lesen

Wenn "Nur lesen" aktiviert ist, werden FTP-Uploads gesperrt.

OK Abbrechen Übernehmen

Praxis

VPN Protection

- Stateful VPN Filterung
 - VPN Datenverkehr kann mit Firewallregeln gefiltert werden
- VPN Traffic kann geregelt werden
 - VPN Netzwerke, Netzwerkbeziehungen
 - Statische oder dynamische IP
- IPSec Tunnel Mode Unterstützung
 - Unterstützung für Drittanbieter
 - Vereinfachte Administration
- VPN Quarantäne Unterstützung
 - Clients in Quarantäne-Netzwerk wenn diese nicht der Policy entsprechen
 - Regelwerk anpassbar durch den Admin

Praxis – GUI klicken

VPN-Clients Remotestandorte

 **VPN-Clientzugriff konfigurieren**
Legen Sie fest, wie Clients über eine VPN-Verbindung auf das Firmennetzwerk zugreifen können.

 **Verifizieren, dass der VPN-Clientzugriff aktiviert ist**
Ermöglicht Remoteclients, eine Verbindung mit dem Netzwerk über eine VPN-Verbindung herzustellen.

 **Windows-Benutzer angeben oder einen RADIUS-Server auswählen**
Geben Sie die Windows-Benutzer (Domänengruppen) an, die VPN-Zugriff verwenden dürfen, oder (falls RADIUS-Authentifizierung verwendet wird) wählen Sie einen RADIUS-Authentifizierungsserver aus.

 **VPN-Eigenschaften und Remotezugriffskonfiguration verifizieren**
Vergewissern Sie sich, dass die VPN-Eigenschaften, wie z. B. Protokolle und Zugriffspunkte entsprechend der Netzwerkanforderungen konfiguriert sind.

 **Firewallrichtlinie für das VPN-Clientnetzwerk anzeigen**
Vergewissern Sie sich, dass die Firewallrichtlinienregeln für das **VPN-Clientnetzwerk** konfiguriert sind, oder Netzwerk- und Firmensicherheitsanforderungen konfiguriert wurden.

 **Netzwerkregeln anzeigen**

Praxis

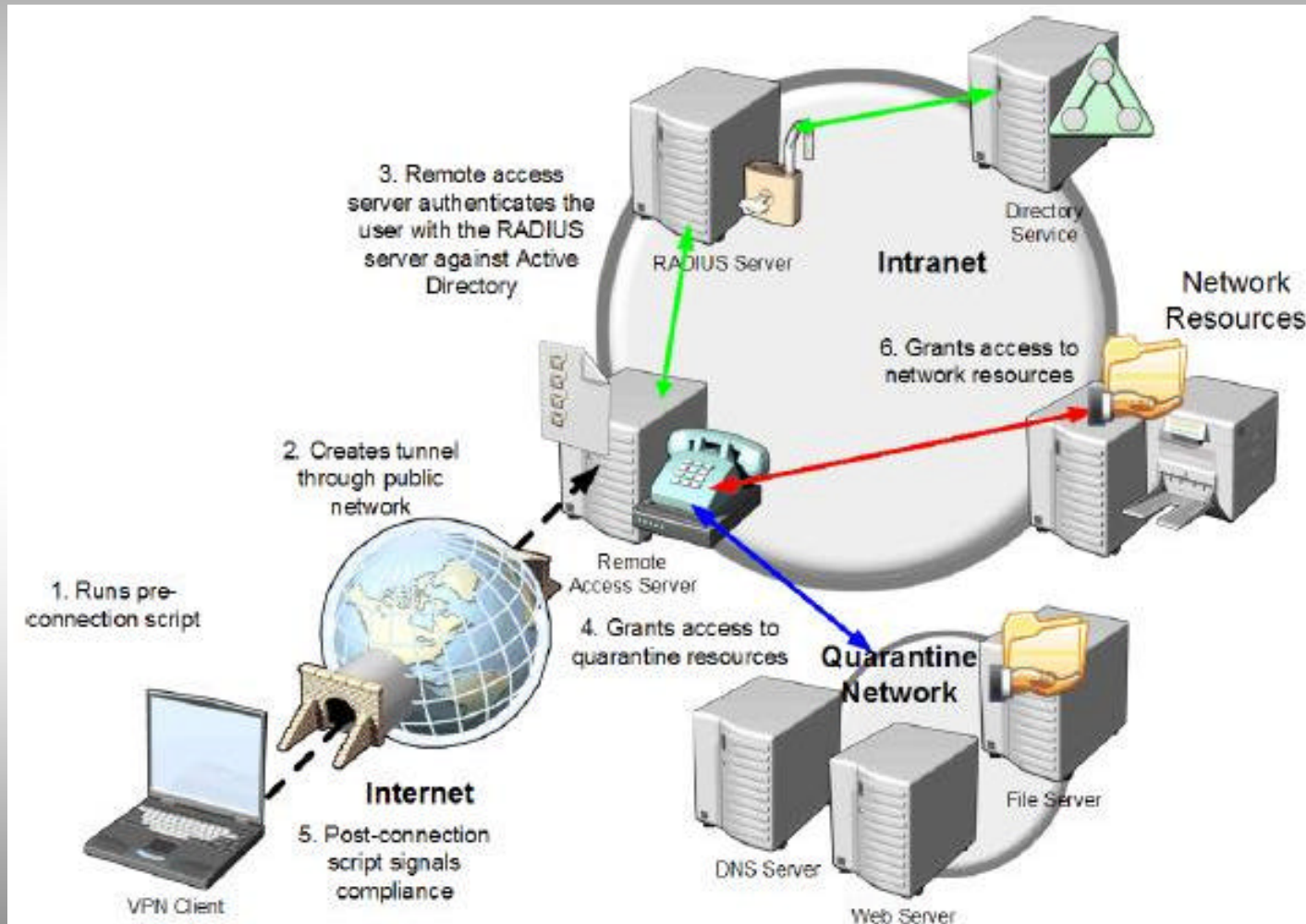
VPN Quarantäne – Teil I

Problem: Keine Kontrolle über eingehaltene Security Policy von VPN Clients bei der Einwahl

Lösung: VPN-Quarantäne. VPN Clients erhalten erst Zugriff auf interne Netzwerkressourcen, wenn durch den Administrator erstellte Richtlinien eingehalten worden sind.

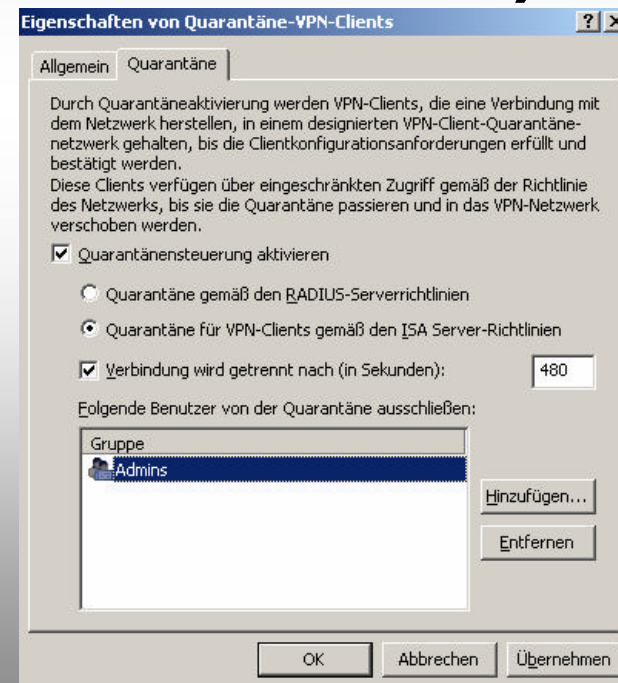
Beispiel: Firewall, Virens Scanner mit aktueller Signatur

VPN Quarantäne – Teil II



VPN Quarantäne Teil III

- ISA 2004 – mit VPNQ
ConfigureRQSforISA.VBS
RQS Tools (in W2K3 SP1 enthalten)
– sonst Download
CMAK
Firewall Policies
Quarantäne-Skript



Erweiterte Sicherheit


(Diese Folie habe ich auf Neudeutsch gelassen)

- Flood-DoS protection
 - SYN-flood protection
 - Client connection quota
 - Applicable to Worm/Virus floods
 - Spoofed UDP packet flooding mitigation
- Attack/Intrusion Detection
 - IP options, DNS Attacks, IP half-scan, Port scan
- IP options filtering
 - Filter out individual options
- Lockdown mode
 - Beendet die Firewalldienste wenn z. B. Logging nicht mehr möglich ist

Authentication Framework

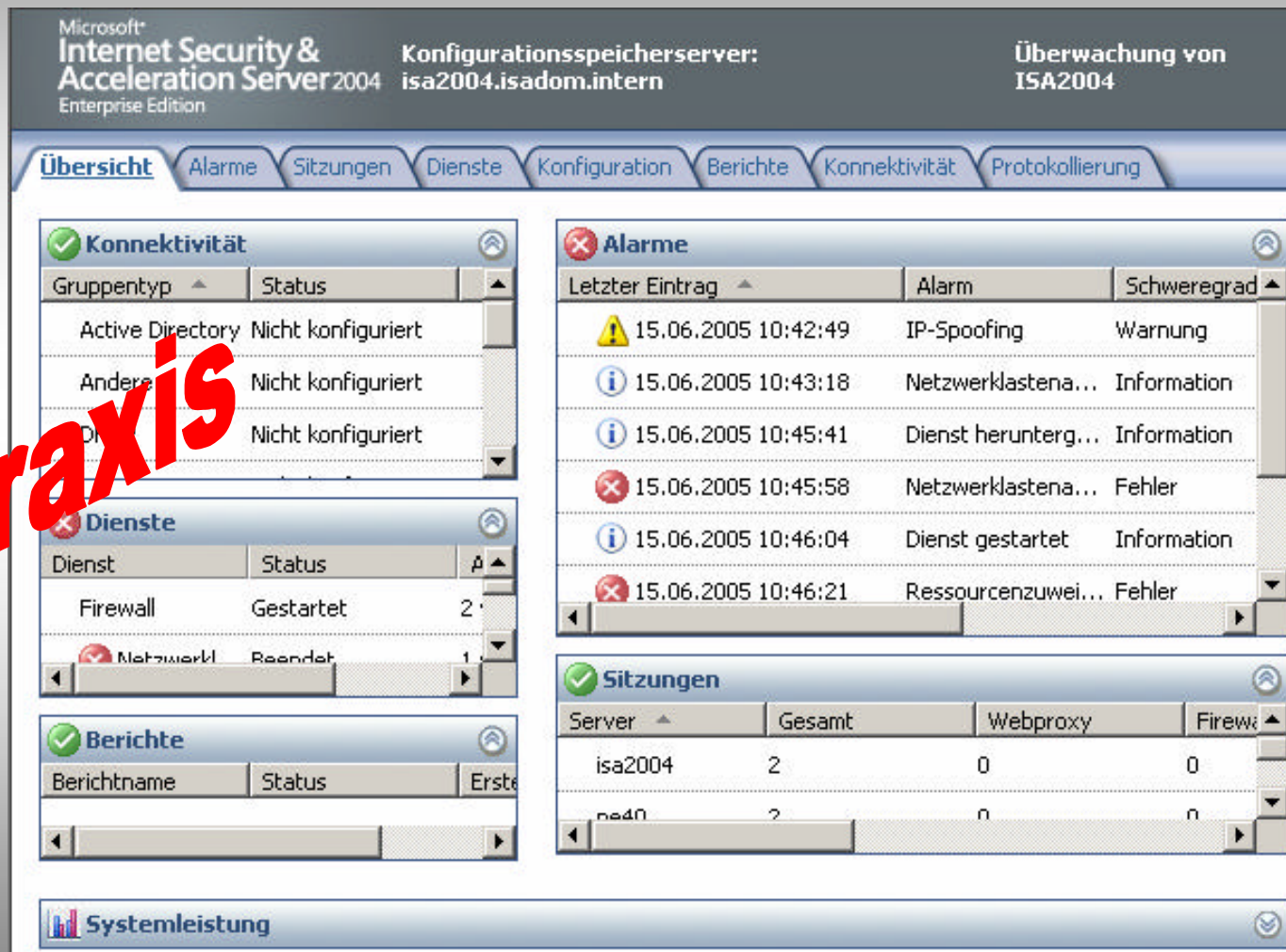
- Multi source authentication
 - Firewall client authentication
 - Transparent user authentication
 - Application transparent, Protocol independent
 - Kerberos/NTLM
 - Web proxy authentication
 - Proxy auth. Reverse proxy auth, Pass through auth, SSL bridging
 - Basic, digest, NTLM, Kerberos, Certificates
 - RADIUS authentication, SecurID authentication
 - CRL support
 - Erweiterbar!
 - VPN Clients
 - EAP (certificates, smartcards, others), MS-CHAPv2, CHAP, (S-PAP, PAP)
 - RADIUS / Windows
- Extensible authentication/authorization framework
 - Third Party – Anbindung eigener Authentifizierungen

ISA 2004 Monitoring Tools

- Dashboard – Zentrale Sicht
- Alarme – Ein Platz für alle Probleme 
- Sitzungen – Aktive Sitzungen
- Dienste – Laufen die Dienste?
- Konnektivität – Verbindungsprüfung
- Protokollierung – Realtime Logging und Historie
- Berichte – Wer surft am meisten

Praxis – GUI klicken

(das ist kein von mir installierter ISA )



Microsoft Internet Security & Acceleration Server 2004 Enterprise Edition

Konfigurationsspeicherserver: isa2004.isadom.intern

Überwachung von ISA2004

Übersicht | Alarme | Sitzungen | Dienste | Konfiguration | Berichte | Konnektivität | Protokollierung

Konnektivität

Gruppentyp	Status
Active Directory	Nicht konfiguriert
Andere	Nicht konfiguriert
...	Nicht konfiguriert

Dienste

Dienst	Status	...
Firewall	Gestartet	2
Netzwerk	Beendet	1

Berichte

Berichtname	Status	Erste
...

Alarmliste

Letzter Eintrag	Alarm	Schweregrad
15.06.2005 10:42:49	IP-Spoofing	Warnung
15.06.2005 10:43:18	Netzwerklastena...	Information
15.06.2005 10:45:41	Dienst herunterg...	Information
15.06.2005 10:45:58	Netzwerklastena...	Fehler
15.06.2005 10:46:04	Dienst gestartet	Information
15.06.2005 10:46:21	Ressourcenzuwei...	Fehler

Sitzungen

Server	Gesamt	Webproxy	Firew...
isa2004	2	0	0
isa40	2	0	0

Systemleistung

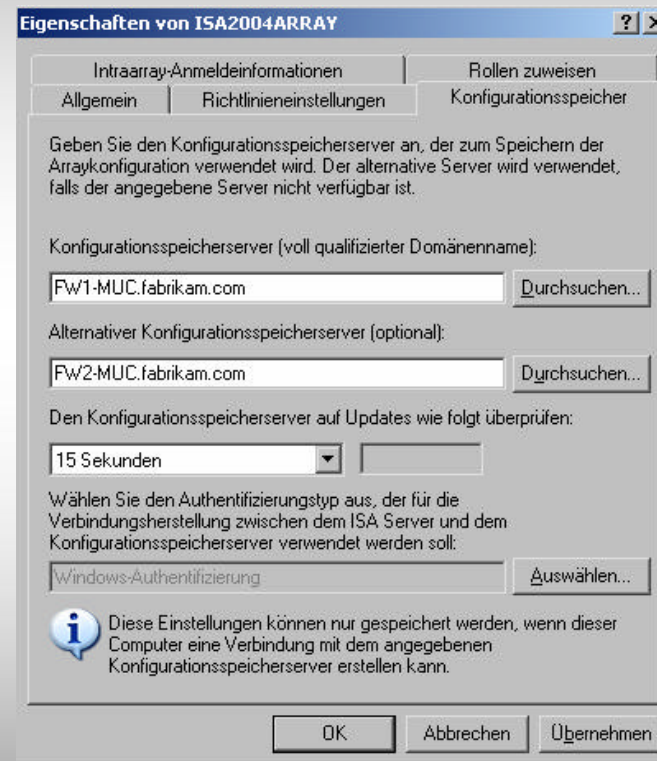
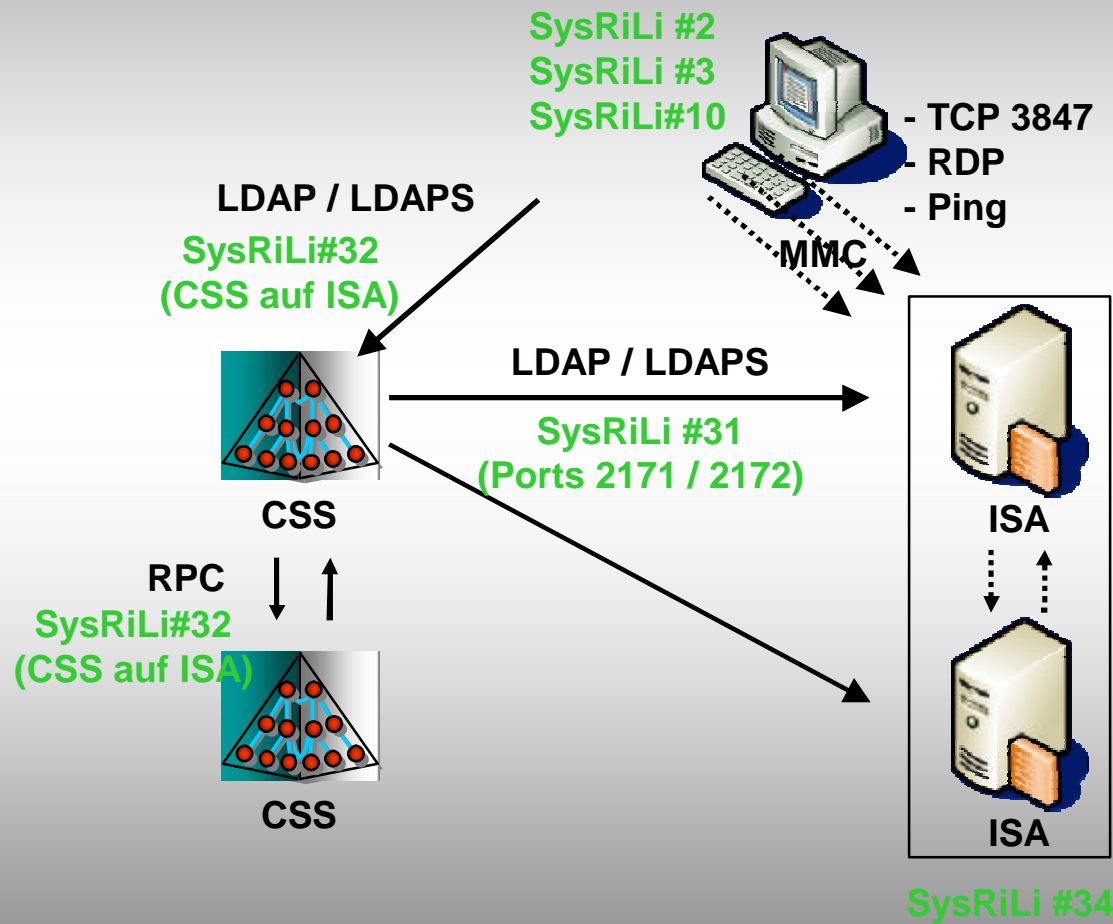
ISA Server 2004 Enterprise - Funktionen

- ADAM (Active Directory Application Mode)
- Enterprise und Array-Richtlinien
- NLB (Network Load Balancing)
- CARP (Cache Array Routing Protocol)
- Zentrales Logging und Reporting

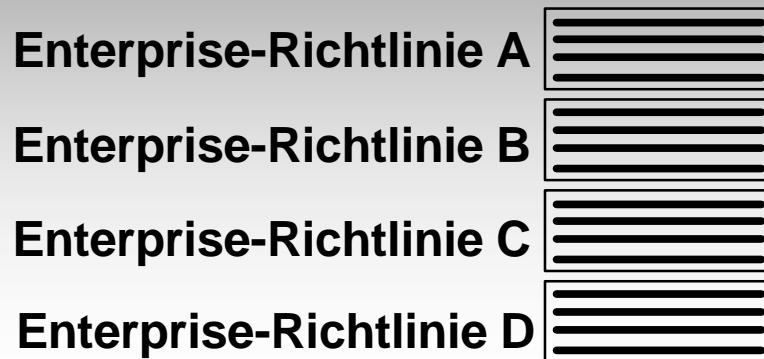
ADAM – Teil I

- „Mini“ Active Directory mit reduzierten Funktionen und Komplexität
- Zentraler Datenspeicher für ISA 2004 Enterprise
- Konfigurationsspeicherserver
- Kommunikation über LDAP(S)/RPC
- Redundanz möglich
- Ermöglicht ISA Server 2004 Enterprise Arrays in einer Arbeitsgruppe – nur ein CSS
- Windows Authentication oder Certificate Authentication
Achtung: <http://support.microsoft.com/?id=894609>
beachten

ADAM – Teil II

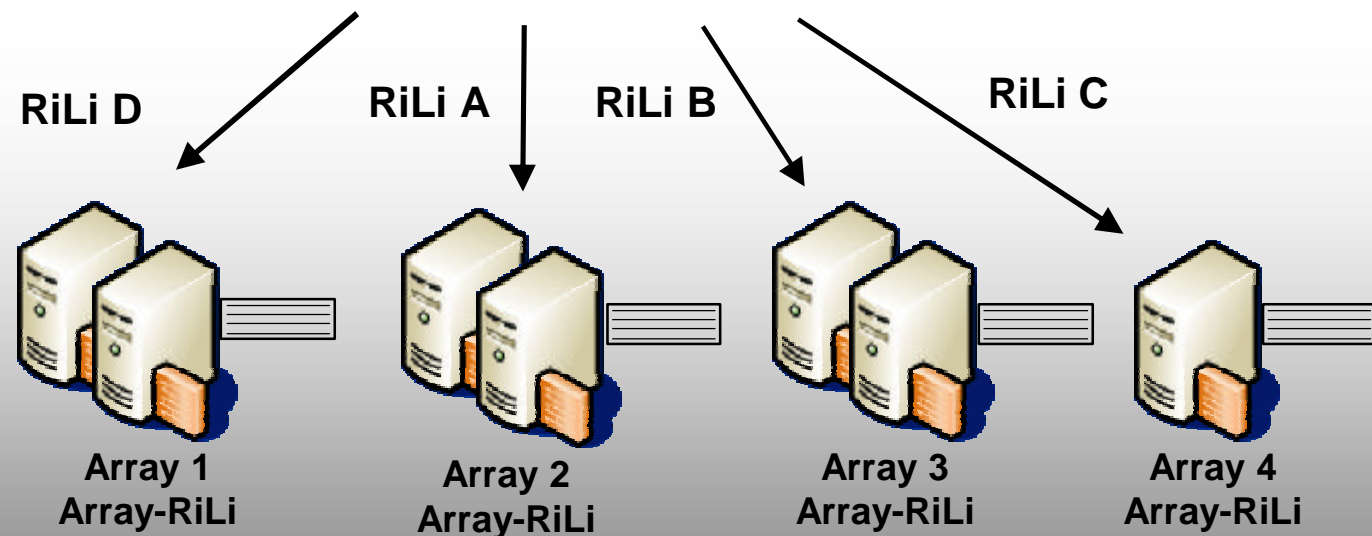


Enterprise und Array-Richtlinien

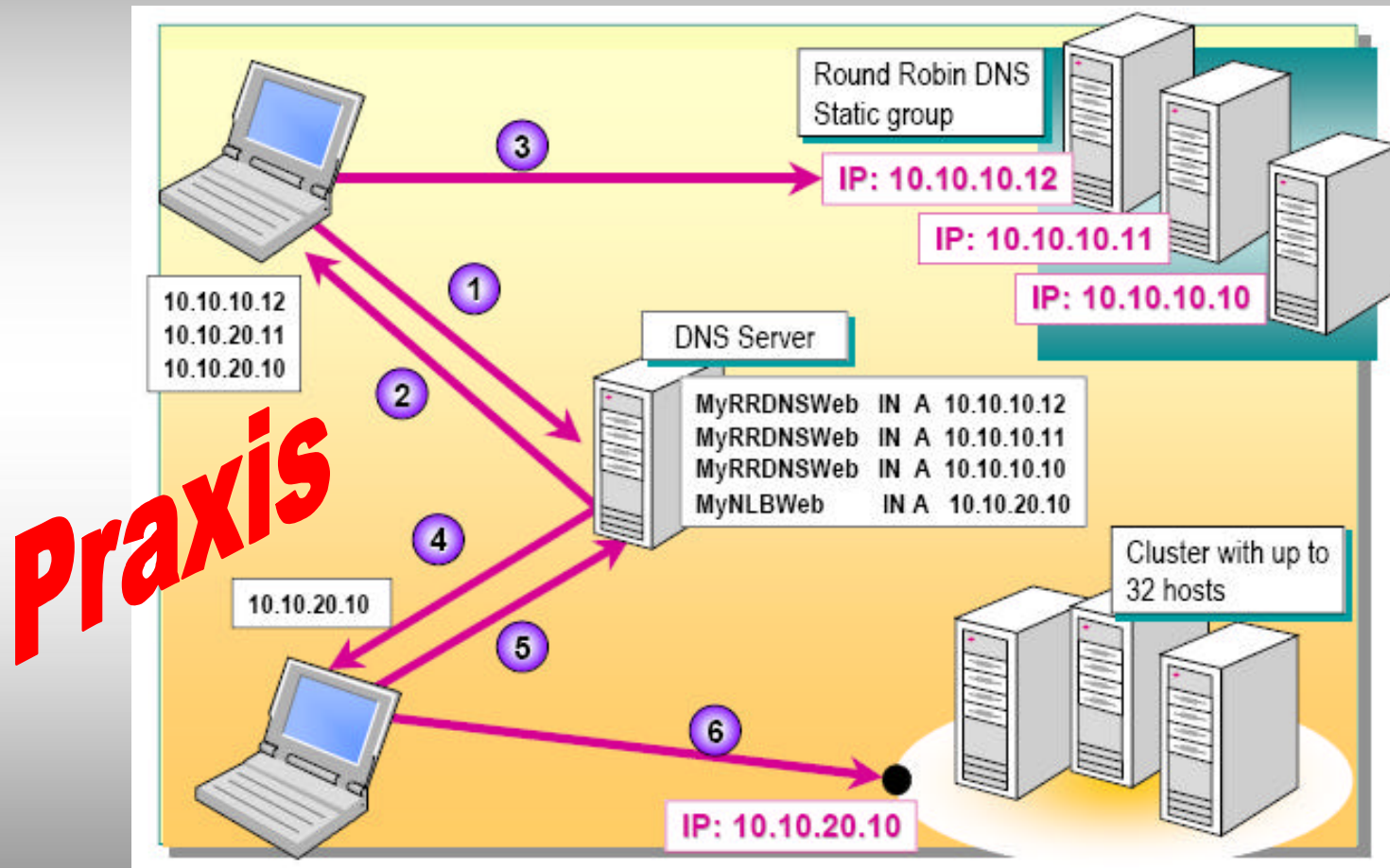


Enterprise-Ebene

Array-Ebene



NLB – Teil I



NLB – Teil II

Einsatzgebiete:

- NLB für einzelne Netzwerke
- NLB für multiple Netzwerke (BDA)
- NLB für Client VPN
- NLB für Standort-zu-Standort VPN

Vorteile:

- ISA kontrolliert die NLB-Konfiguration
- ISA kontrolliert, wann NLB-Heartbeats verwendet werden sollen
- ISA kontrolliert, wann bidirektionale Affinität genutzt werden soll
- ISA kontrolliert, wenn NLBhash verwendet werden soll

CARP

- CARP (Cache Array Routing Protocol)
- Intelligentes Cache-Management
- ISA Server Caches bilden einen logischen Cache
- Cacheinhalte werden nur einmal gespeichert
- Hashbasiertes Caching
- Server- und clientseitiges CARP

Praxis

Zukunft: Branch Office Updates für ISA Server 2004

- **Angekündigt auf der TechEd 2005**
- **Drei neue Funktionen**
 - **Microsoft Update (BITS Caching)**
 - **HTTP Komprimierung**
 - **Quality of Service für HTTP**
- **Verfügbar Ende des Jahres 2005**
- **Kostenlos für jeden ISA Kunden**
- **Verfügbar für ISA Enterprise und Standard**

Microsoft ISA Server 2004 - Appliance

- Microsoft ISA Server 2004 auf vorkonfigurierter Hardware
- Gehärtetes Betriebssystem
- Einfaches Setup
- Out-of-box Funktionalität
- Einfache Wiederherstellung

Anbieter:

Pyramid Computer
Wortmann AG
Celestix Networks
Corrent
Hewlett-Packard
Network Engine



Weitere Informationen:

<http://www.microsoft.com/isaserver/hardware/default.msp>

Werbung

Herzlich Willkommen!

Sie planen, ISA Server 2000 oder 2004 einzusetzen?
 Sie setzen ihn bereits ein?
 Sie suchen Hilfe bei der Konfiguration?

Dann sind Sie hier richtig, denn der Zweck dieser nicht-kommerziellen Website ist es, als Ergänzung zur [Newsgroup](#), HowTo's, Step-by-Step-Anleitungen und Ressourcen rund um *Microsoft Internet Security and Acceleration Server* zur Verfügung stellen.



Viele Grüße

Dieter Rauscher
 MVP ISA Server



News:

- [Buchankündigung](#)
[ISA Server 2004 - Das Handbuch](#)
 von den Autoren der msisafaq!

Veranstaltungen:

- [ISA Server 2004 Interaktives Training](#)
- [ISA Server 2004 Webcastreihe](#)

Neue Artikel auf msisafaq.de:

- [MCP-Prüfung](#) Marc Grote, 29.05.
- [Zertifikate](#) Marc Grote, 22.01.
- [DMZ](#) Marc Grote, 22.01.
- [Websites sperren](#) Armin Simon, 22.01.
- [Inplace Update](#) Marc Grote, 16.01.
- [RDP-Serververöffentlichung 2](#) Dieter Rauscher, 02.01.
- [RDP-Serververöffentlichung](#) Dieter Rauscher, 02.01.
- [Lokaler Remotedesktop](#) Dieter Rauscher, 02.01.
- [Firewallclient](#) Marc Grote, 02.01.

Aktuelle Microsoft Servicepacks:

- [SBS 2003 SP1](#) (19.05.2005)
- [SQL 2000 SP4](#) (06.05.2005)
- [Windows Server 2003 SP1](#) (30.03.2005)
- [ISA 2004 SP1](#) (01.03.2005)
- [Windows XP SP2](#) (09.08.2004)
- [Office 2003 SP1](#) (27.07.2004)
- [Exchange 2000 Post SP3 Rollup](#) (27.05.2004)
- [Exchange 2003 SP1](#) (25.05.2004)
- [ISA 2000 SP2](#) (20.05.2004)

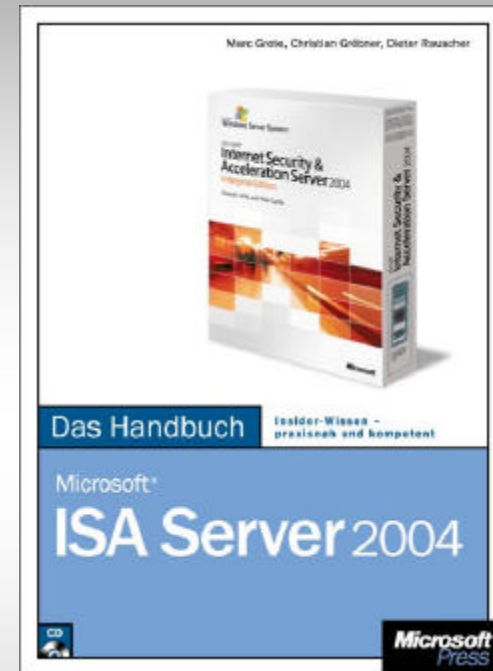
Aktuelle MS-KB Artikel zu ISA:

- [897716](#) - RPC data may be blocked, and Outlook may not start in Windows Server 2003 with SP1
- [887222](#) - The ISA Server RPC filter blocks RPC traffic after Windows Server 2003 Service Pack 1 is installed on a computer that is running ISA Server 2004 or ISA Server 2000

Referent: Marc Grote - <http://www.it-training-grote.de>

Microsoft ISA Server 2004 – Das Handbuch von Microsoft Press

- Ca. 600 Seiten Umfang
- Von drei ISA Server MVP
Marc Grote
Dieter Rauscher
Christian Gröbner
Veröffentlichung September 2005
- Basiert auf Microsoft ISA Server 2004 Standard und Microsoft ISA Server 2004 Enterprise
- Das Buch beschreibt die Implementierung von Microsoft ISA Server 2004 anhand einer fiktiven Firma



ISA Server 2004 Tech@Night

In der Zeit vom 12.09.2005 - 22.09.2005 halte ich Tech@Night Vorträge zum Thema ISA Server 2004 – Serververöffentlichung Best Practices. Die Veranstaltung wird an folgenden Orten stattfinden:

12.09.2005 - Hamburg

13.09.2005 - Berlin

14.09.2005 - Leipzig

20.09.2005 - Braunschweig

21.09.2005 - Bremen

22.09.2005 - Münster

Weitere Informationen hier:

<http://www.microsoft.com/germany/events/default.msp>

Lust auf Links?

- <http://www.msisafaq.de>
- <http://www.isaserver.org>
- <http://www.isatools.org>
- <http://www.microsoft.com/isaserver/default.mspx>
- <http://www.microsoft.com/isaserver/community/default.mspx>
- <http://support.microsoft.com/newsgroups/default.aspx?ln=de>

The End? Fragen?



Vielen Dank für Ihre
Aufmerksamkeit