

Entscheidertage

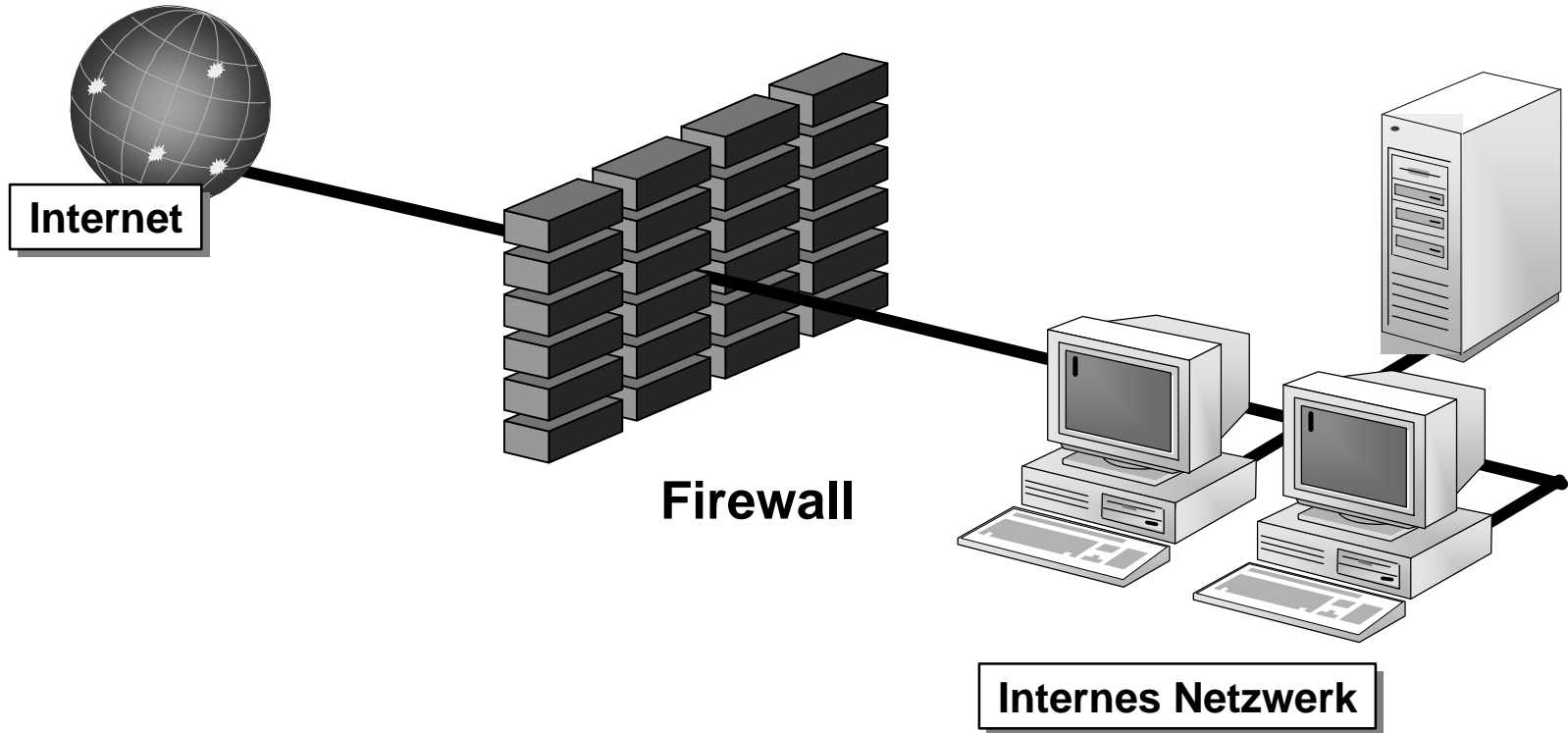
Layer \equiv Drei
EDV-Schulungen

**Microsoft Internet Security &
Acceleration Server 2004**

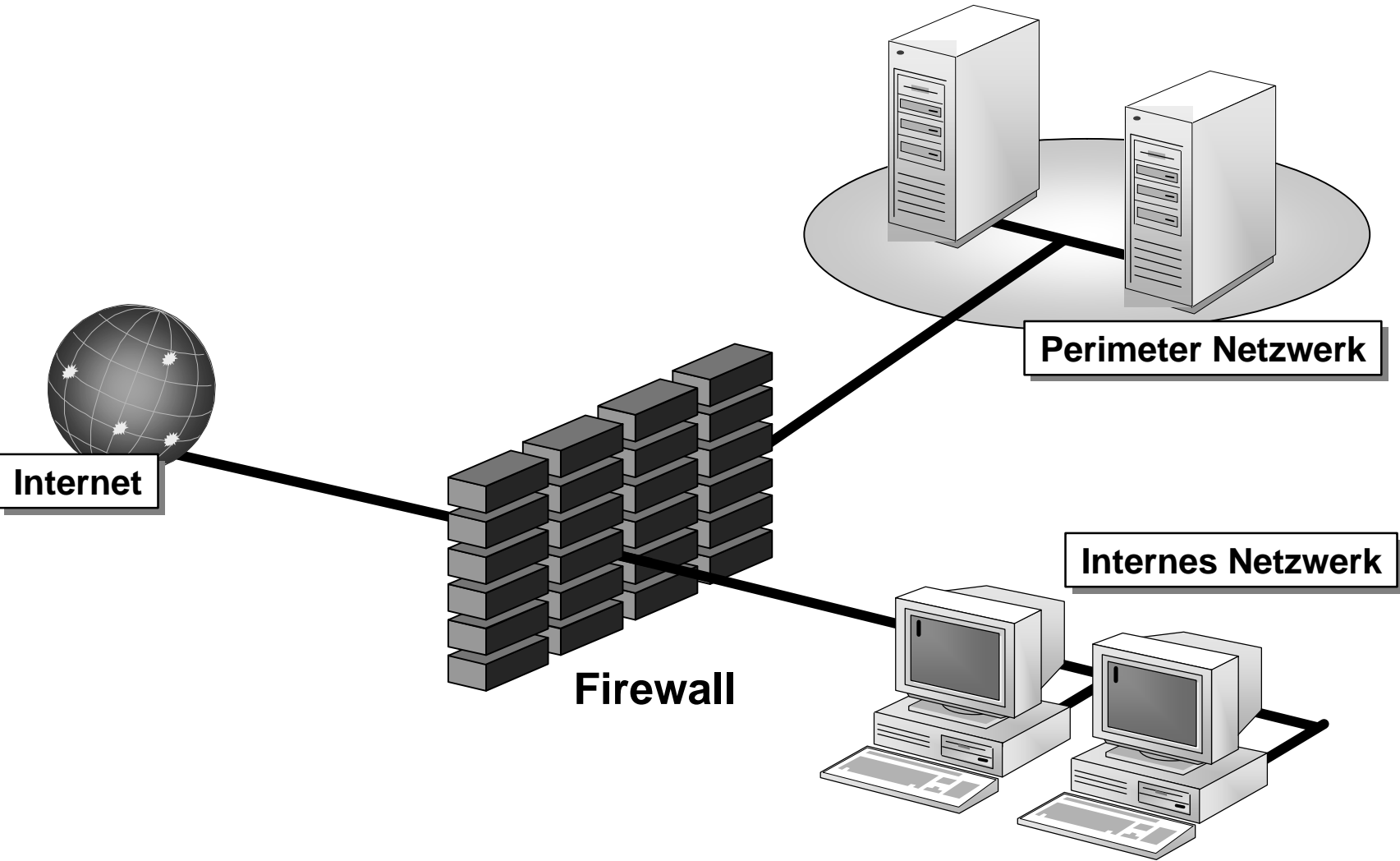
Agenda

- ◆ **Firewallgrundlagen**
- ◆ **ISA Server 2004 Versionen**
- ◆ **ISA Server 2004 Leistungsmerkmale**
- ◆ **ISA Server 2004 Mehrfachnetzwerke**
- ◆ **ISA Server 2004 Übersicht**
- ◆ **ISA Server 2004 Basis-Einrichtung**
- ◆ **ISA Server 2004 Monitoring**
- ◆ **ISA Server 2004 VPN**
- ◆ **ISA Server 2004 Enterprise**
- ◆ **GFI Webmonitor**
- ◆ **Zukunft – ISA Server 2004 SP2**
- ◆ **Lust auf Links?**

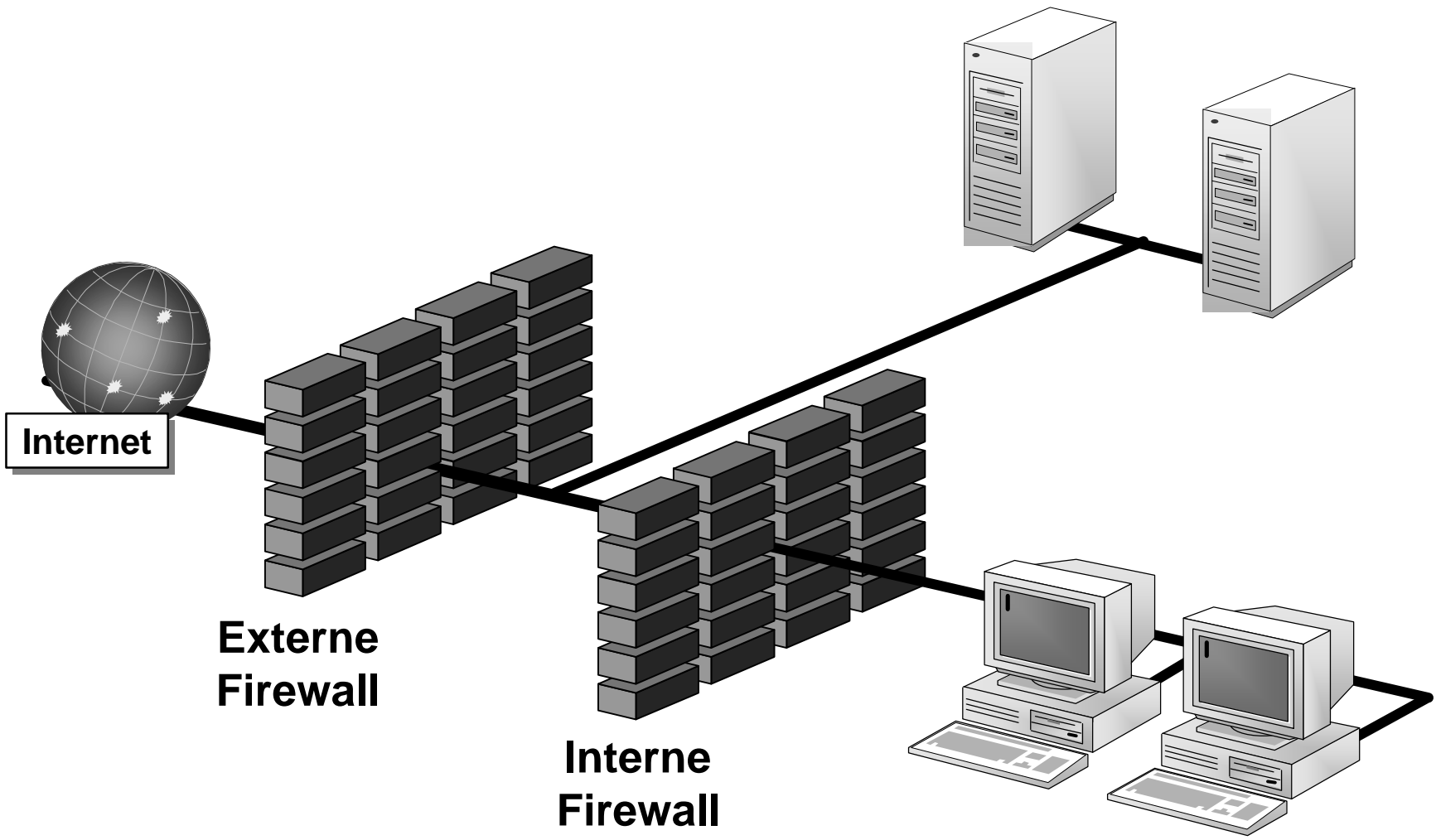
Firewallgrundlagen - Bastion Host



Perimeter Netzwerk mit Trihomed Firewall



Perimeter Netzwerk mit Back-to-Back Firewalls

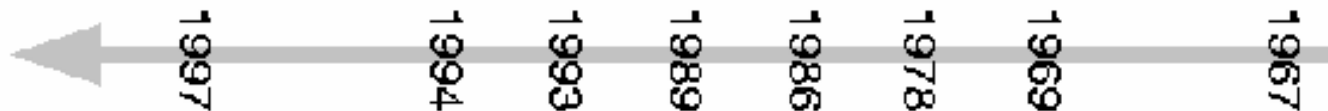


ISA Server Versionen

- ◆ 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

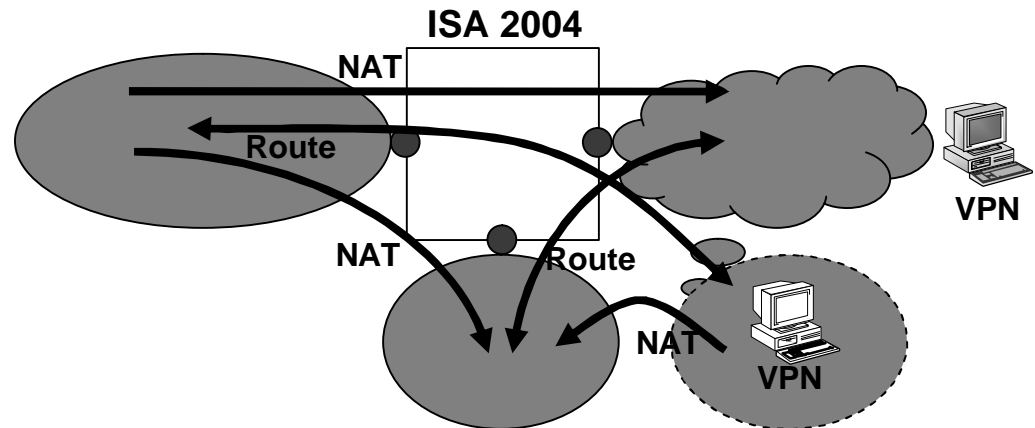
- ◆ **Umfassender Schutz bis auf die Anwendungsebene**
- ◆ **Die ideale Firewall für sichere Microsoft Exchange Server-Veröffentlichung**
- ◆ **Die ideale Firewall für sichere Microsoft Exchange Server-Veröffentlichung**
- ◆ **Einfache und sichere Veröffentlichung von Webservern**
- ◆ **Common Criteria EAL4+-Zertifizierung**
- ◆ **Netzwerkvorlagen und XML Import**
- ◆ **Firewall (ALF, Stateful) + Proxy Server + VPN Server**
- ◆ **Verfügbar als Appliance**
- ◆ **Server- und Web-Veröffentlichung**
- ◆ **Monitoring & Reporting**
- ◆ **Integrierter Webcache und hierarchisches Caching**
- ◆ **Benutzerspezifische Authentifizierung an der Firewall**
- ◆ **Microsoft Windows-VPN und integrierte Quarantänefunktion**

Neue Funktionen

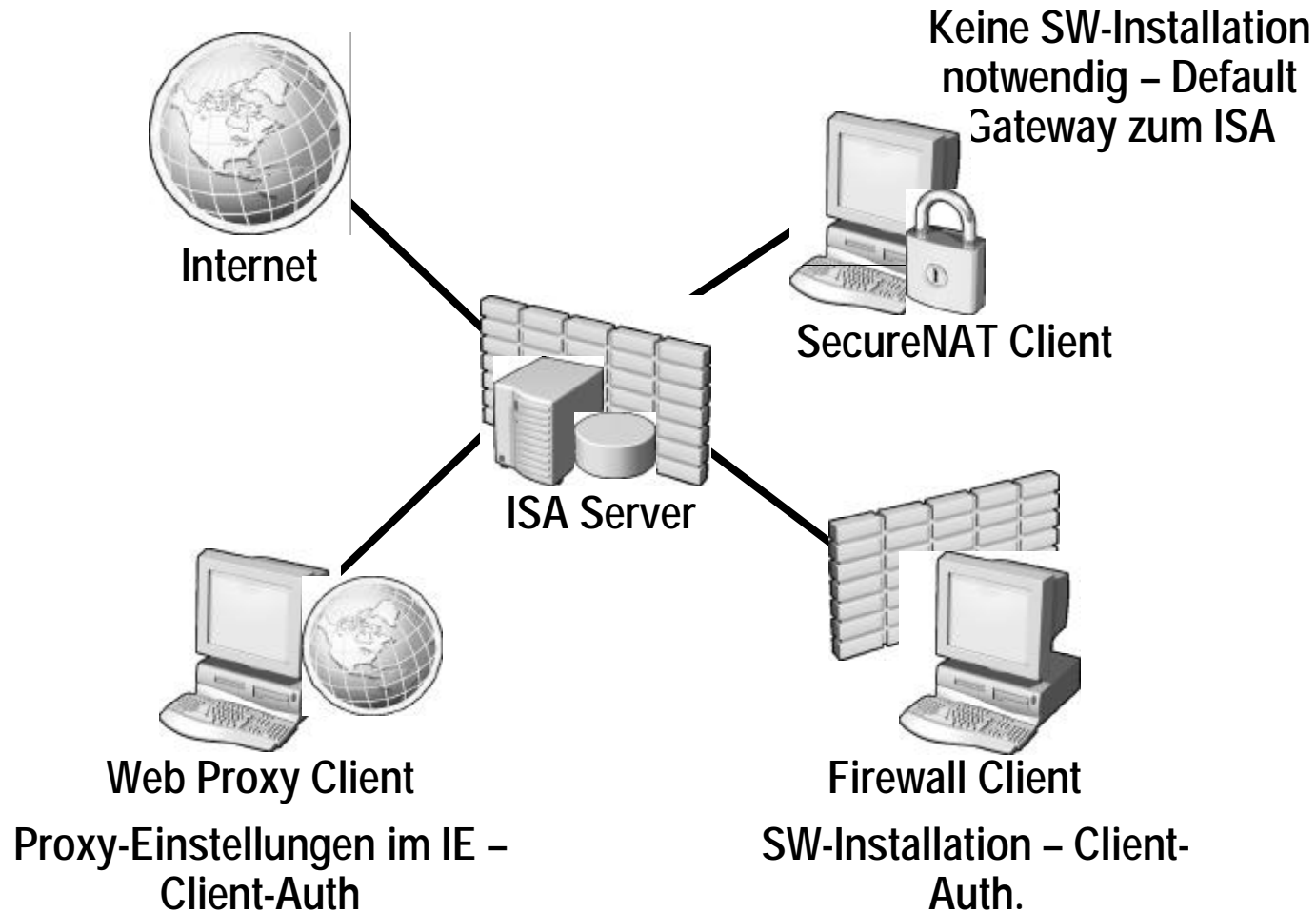
- **Neue, vereinfachte Benutzeroberfläche**
- **Flexible Unterstützung für unterschiedliche Netzwerk-Designs**
- **Verbesserte VPN-Unterstützung**
- **VPN-Quarantänefunktionen**
- **Erweiterte Protokollunterstützung / Individuelle Protokolldefinitionen**
- **OWA-Veröffentlichungs-Assistent**
- **Verbesserte Webveröffentlichung**
- **Portumleitung für Serververöffentlichungsregeln**
- **RADIUS-Unterstützung für Webproxycient-Authentifizierung**
- **Delegierung der Standardauthentifizierung**
- **Verbesserte SMTP-Nachrichtenüberwachung**
- **Verbesserte HTTP-Filterung**
- **Linkübersetzung**
- **Verbesserte Überwachung und Berichterstellung**

Netzwerke	Netzwerksätze	Netzwerkregeln	Webverknüpfung
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 zugeordnet		
VPN-Clients	Diesem Netzwerk sind zurzeit keine IP-Adressen zugeordnet		

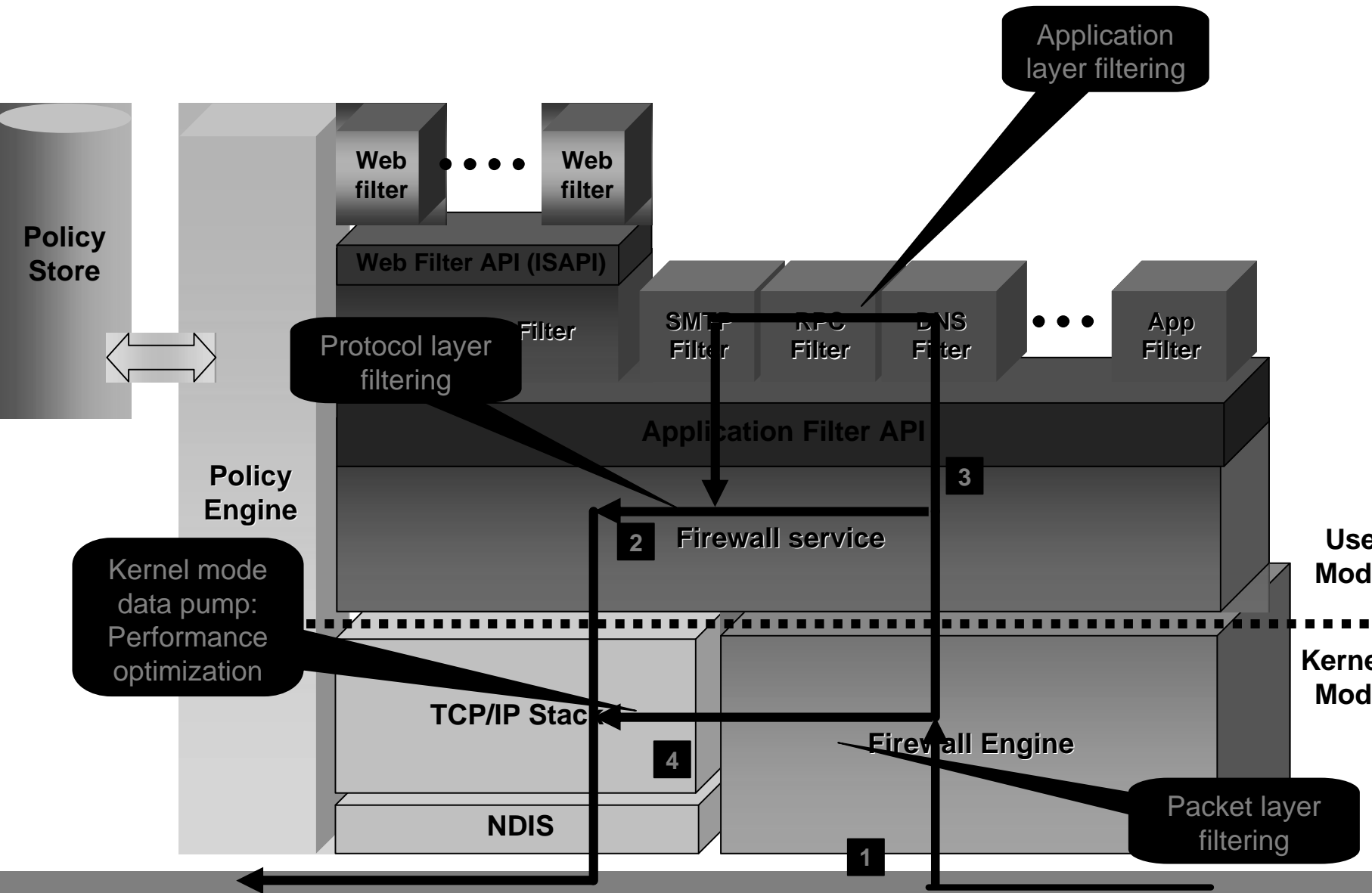
Netzwerkregeln



ISA Server - Clients



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
- ◆ Anwendungsfilter Framework
 - Filter für allgemeine Protokolle
HTTP, SMTP, RPC, FTP, H.323, DNS, POP3, Streaming Media
 - Einfach erweiterbare Architektur (SDK)

- 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

Problem:

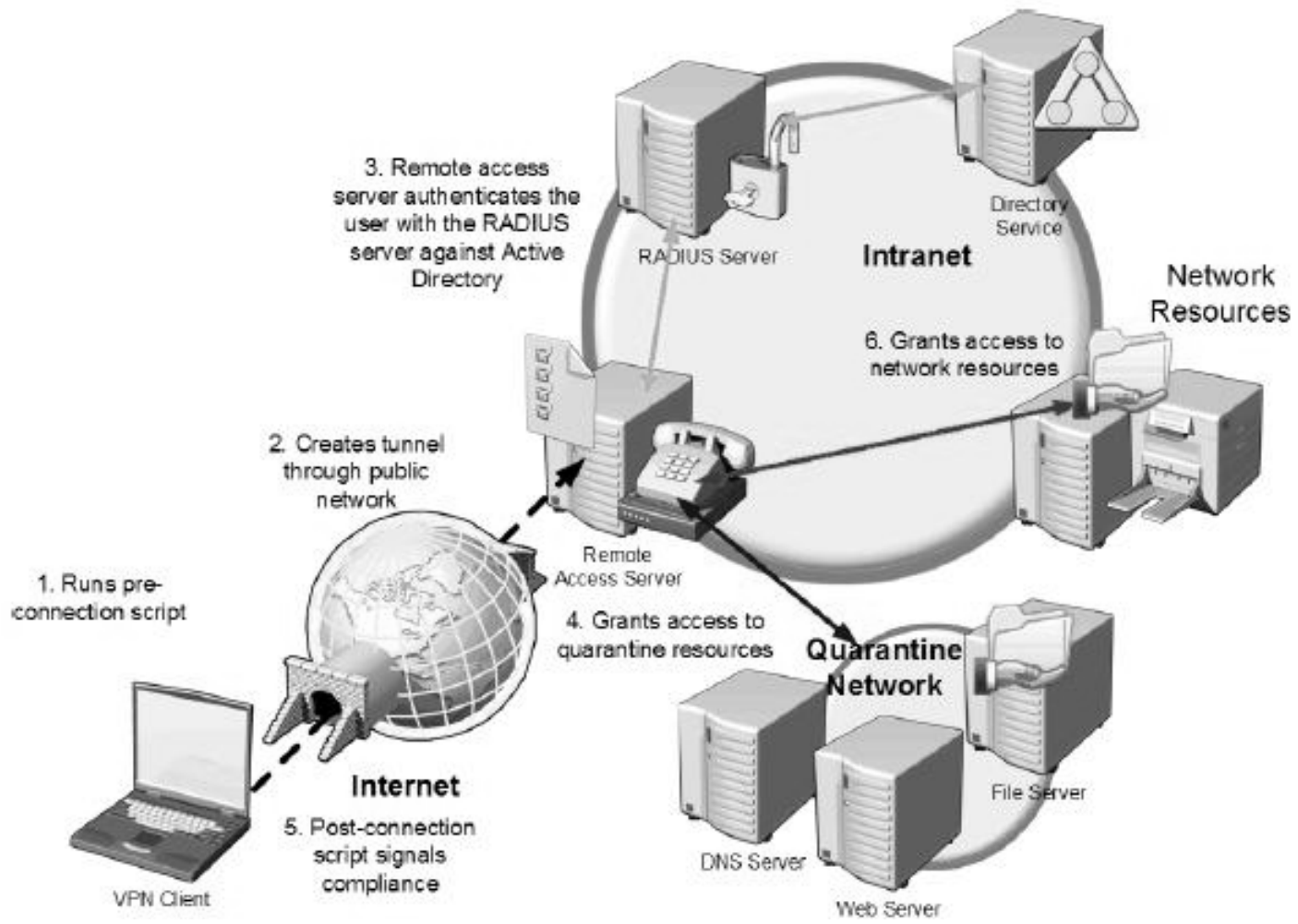
Keine Kontrolle über eingehaltene Security Policy von VPN Clients bei der Einwahl

Lösung:

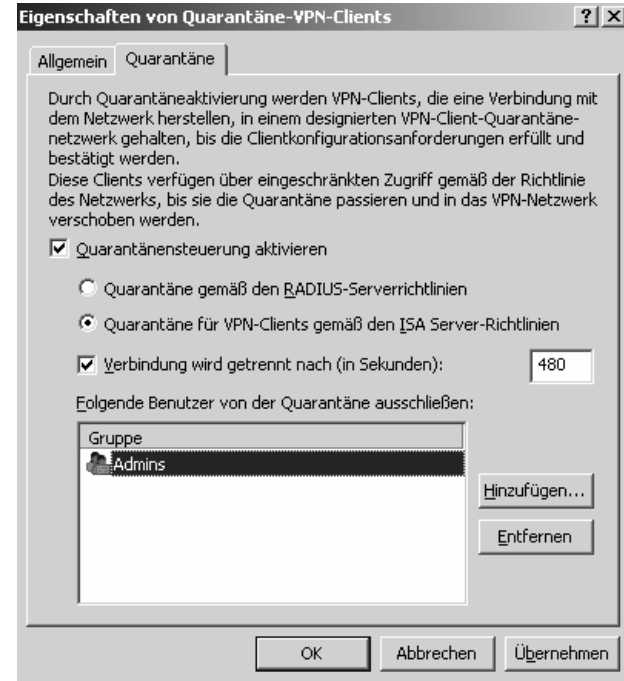
VPN-Quarantäne. VPN Clients erhalten erst Zugriff auf interne Netzwerkkressourcen, wenn durch den Administrator erstellte Richtlinien eingehalten worden sind.

Beispiel: Firewall, Virens Scanner mit aktueller Signatur

VPN Quarantäne – Teil II



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



- ◆ 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

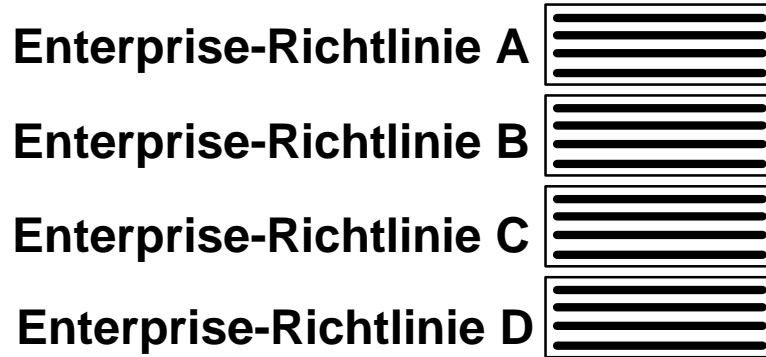
- ◆ Dashboard – Zentrale Sicht
- ◆ Alarme – Ein Platz für alle Probleme 😊
- ◆ Sitzungen – Aktive Sitzungen
- ◆ Dienste – Laufen die Dienste?
- ◆ Konnektivität – Verbindungsprüfung
- ◆ Protokollierung – Realtime Logging und Historie
- ◆ Berichte – Wer surft am meisten

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

ADAM

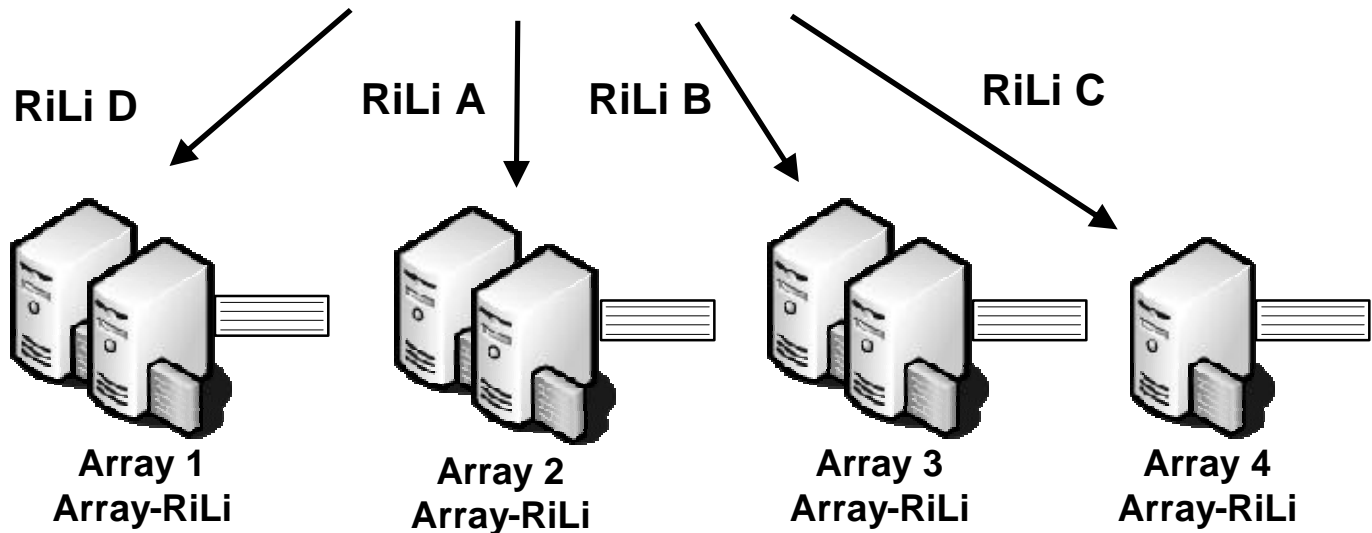
- ◆ „Mini“ Active Directory mit reduzierten Funktionen und Komplexität
- ◆ Zentraler Datenspeicher für ISA 2004 Enterprise
- ◆ Konfigurationsspeicherserver
- ◆ Kommunikation über LDAP(S)/RPC
- ◆ Redundanz möglich
- ◆ Ermöglicht ISA Server 2004 Enterprise Arrays in einer Arbeitsgruppe – nur ein CSS
-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

Enterprise und Array-Richtlinien

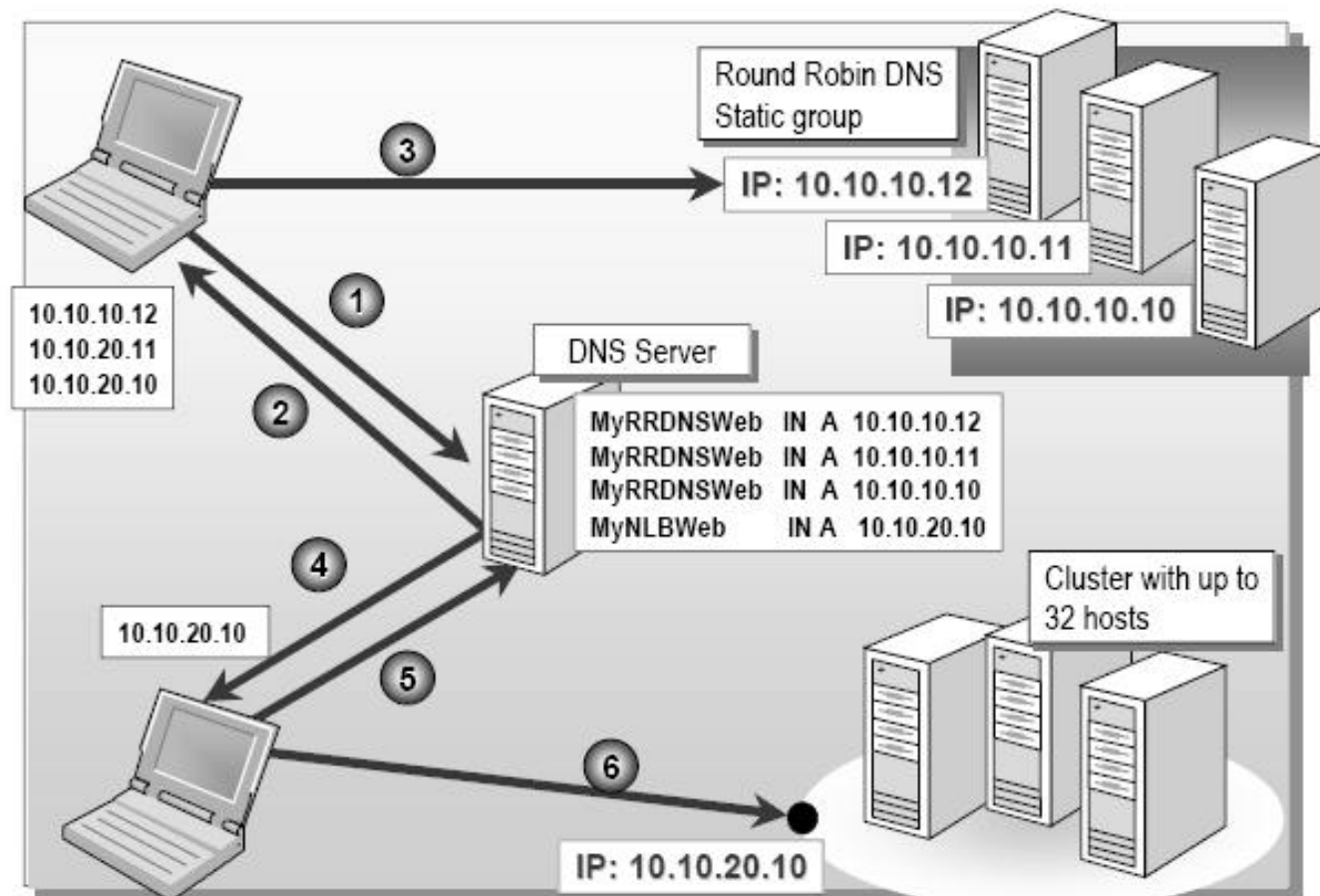


Enterprise-Ebene

Array-Ebene

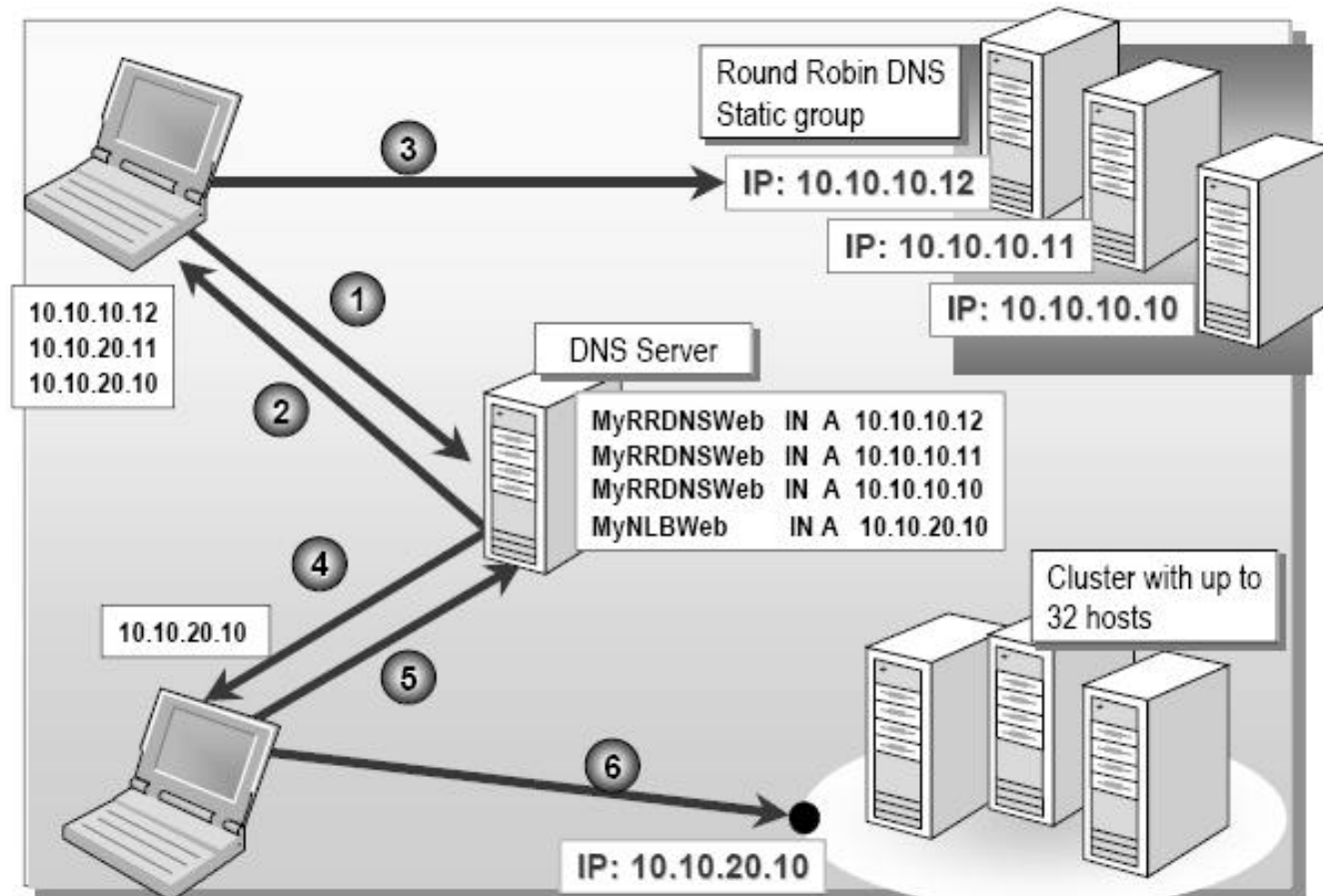


NLB Teil I



- ◆ 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

NLB Teil I



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

- Integriert als Webfilter in ISA Server 2004
- Ergänzungsmodule Malware, Trojaner, Adware und Spyware
- Inhaltsfilterung mit Zugriffsschutz vor Seiten mit anstößigen Inhalten
- Überprüfung sämtlicher Downloads auf Viren
- Blockieren von Web-Sites per URL-Gruppen aus ISA Server-Sperrregeln
- Blockierung von Dateitypen
- Übersichtlicher und präziser Überblick über Internet-Aktivitäten
- Kontrolle des Internet-Traffics per Web-basiertem Interface
- Statistiken zum Datentransfer für jeden Anwender
- Täglicher Bericht über alle Anwender, IPs und Web-Sites
- Live-Statistik zu heruntergeladenen Dateitypen pro Web-Site
- Abbruch von aktiven bandbreitenintensiven Verbindungen

GFI Webmonitor 3.0 GUI – Teil I

http://monitor.isa/ - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Wechseln zu Links

Adresse <http://monitor.isa/>

GFI WebMonitor

- Monitor
 - Active Connections
 - URL History
 - Users History
 - Last Web Access
- Configuration
 - Access Permissions
 - General Options
 - Site Rating
 - Web Traffic Scanning**
 - BitDefender
 - Kaspersky
- General
 - Version Information
 - Licensing
 - How to Purchase
 - Support Center
 - GFI WebMonitor
 - GFI LANguard N.S.S.
 - GFI LANguard S.E.L.M.

Web Traffic Scanning

Configure which downloaded content types will be blocked, allowed or scanned for viruses and malware through the BitDefender/Kaspersky virus engines.

Web Traffic Scanning General Options

GFI WebMonitor performs Web Traffic Scanning on the data objects passing to the ISA Server based on both its real file type as well as HTTP content type. Specify whether GFI WebMonitor is to perform access and content type control on the data passing through the ISA Server:

- Enable Web Traffic Scanning.
Select one or more antivirus engines to scan data objects with:
 - BitDefender Anti-Virus
 - Kaspersky Anti-Virus

Apply

File Type processing options

Configure the GFI WebMonitor file type based access control policy. On downloading of a data object, GFI WebMonitor will extract its file type signature and HTTP content type (where applicable/available). This information is used by GFI WebMonitor to identify the type of processing action to perform on this object.

Fertig Internet

GFI Webmonitor 3.0 GUI – Teil II

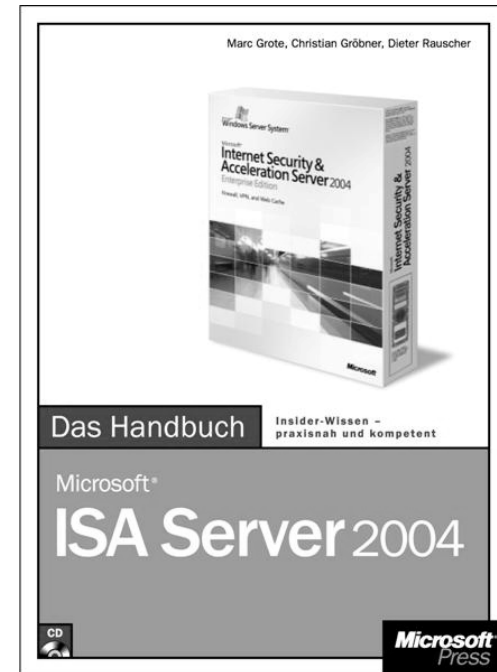
The screenshot shows the Microsoft Internet Security & Acceleration Server 2004 GUI. The window title is "Microsoft Internet Security & Acceleration Server 2004". The interface includes a menu bar (Datei, Aktion, Ansicht, ?), a toolbar with navigation icons, and a left-hand navigation tree. The tree is expanded to "Add-Ins", which contains "Überwachung", "Firewallrichtlinie", "Virtuelle private Netzwerke", "Konfiguration", "Netzwerke", "Cache", "Add-Ins", and "Allgemein". The main content area displays the "Webfilter" configuration page. At the top, it says "Microsoft Internet Security & Acceleration Server 2004 Standard Edition". Below this, there are tabs for "Anwendungsfiler" and "Webfilter". A table lists the installed filters:

Rei...	Name	Beschreibung	Richtung	Vers...	Herst...	Relati
1	Formularbasierter OWA-Au...	Aktiviert formularbasierte (Cookie-) Aut...	Eingehende Webanforde...	4.0	Microsof...	Cookie
2	SecurID-Filter	Aktiviert SecurID-Authentifizierung.	Eingehende Webanforde...	4.0	Microsof...	sdisa.c
3	Radius-Authentifizierungsfilter	Aktiviert die Radius-Authentifizierung.	Beide	4.0	Microsof...	radius:
4	GFI WebMonitor3 filter	GFI WebMonitor3 filter for ISA server	Ausgehende Webanford...	3.41	GFI Soft...	WebM
5	Linkübersetzungsfilter	Aktiviert die Linkübersetzung für veröff...	Eingehende Webanforde...	4.0	Microsof...	LinkTra
6	HTTP-Filter	Filtert HTTP-Datenverkehr und erzwingt...	Beide	4.0	Microsof...	HttpFil

- ◆ **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**

ISA Server 2004 – 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



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.mspx>

Lust auf Links?

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

Die letzte Folie!

- ◆ Vielen Dank für Ihre Aufmerksamkeit
- ◆ Haben Sie noch Fragen?

Layer = Drei
EDV-Schulungen