

**Haufe Mediengruppe**

# Praxisbericht

## Aufbau einer DMZ- Infrastruktur mit VMware Server

Stefan Mössner, Rudolf Haufe Verlag GmbH & Co. KG  
Vortrag 1C03 , DECUS-Symposium 2008  
04. / 05. Juni 2008  
Sheraton Congress Hotel, Frankfurt a. M.


**Haufe** **LEXWARE** **redmark** 

**Haufe Mediengruppe**

## Agenda

- Darstellung der alten DMZ-Infrastruktur
- Welche Probleme sind damit verbunden?
- Welche Anforderungen gibt es?
- Wie werden die Anforderungen erfüllt?
- Technische Umsetzung
- Darstellung der neuen DMZ-Infrastruktur
- Erfahrungen

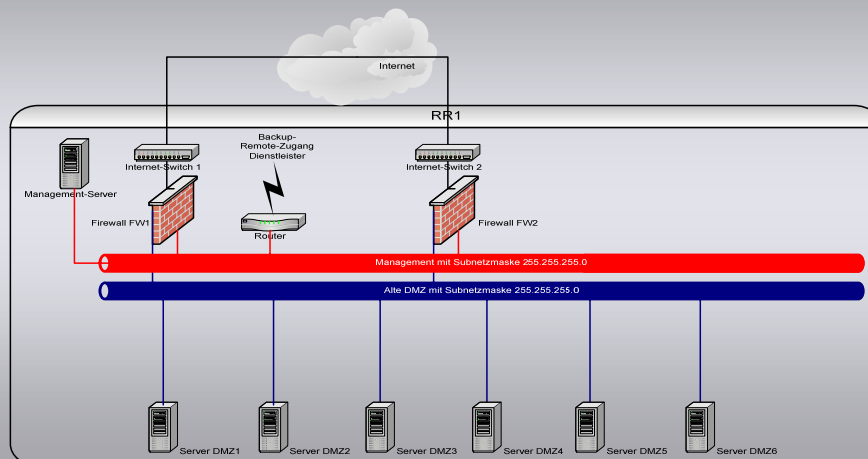
Seite: 2 Gestaltung: 2008 Haufe Mediengruppe DMZ-Infrastruktur mit VMware Server Erstellt von: Stefan Mössner

**Haufe** **LEXWARE** **redmark** 

## Darstellung der alten DMZ-Infrastruktur

- In der durch die IT betreuten DMZ werden nur wenige Webseiten gehostet.
- Es befinden sich 10 einzelne physikalische DMZ-Server in Betrieb.
- Die DMZ-Systeme sind eher infrastruktureller Natur:
  - Microsoft ISA für Outlook Web Access
  - Netviewer One2One
  - Mehrere verteilte FTP-Server
  - VPN-Konzentrator
  - Microsoft Terminal-Server
  - SAP-Router

## Schematische Darstellung der alten DMZ-Infrastruktur



## Haufe Mediengruppe

### Welche Probleme sind damit verbunden?

- Alle Systeme befinden sich in einem Rechnerraum → höheres Ausfallrisiko
- Keine redundanten Systeme → höheres Ausfallrisiko
- Serverhardware und -software ist teilweise veraltet → kein Support, z. B. für Windows NT
- Serverhardware nicht optimal ausgelastet, da nur wenige Transaktionen
- Viele einzelne Serversysteme → hoher Administrationsaufwand
- Teilweise nicht-managebare Switches im Einsatz → kein Netzwerk-Monitoring
- Alle Server befinden sich in einer DMZ → größeres Sicherheitsrisiko
- IP-Bereich der DMZ überschneidet sich häufig mit Netzen von per VPN angebundenen Partnern und Mitarbeitern → Routingprobleme

Seite: 5 Gestaltung: 2008 Haufe Mediengruppe DMZ-Infrastruktur mit VMware Server

Erstellt von: Stefan Mössner



## Haufe Mediengruppe

### Welche Anforderungen gibt es?

- Bessere Absicherung gegen Ausfälle (Strom, Hardware usw.)
- Schaffung von Systemredundanzen
- Höhere Sicherheit der Systeme
- Aktuelle Hard- und Software
- Neuer DMZ-IP-Bereich & Abschaltung alter DMZ
- Verbesserte Überwachungsmöglichkeiten
- weitestgehende Hardware-Konsolidierung
- Verringerung des Administrationsaufwands
- Bedarf an zusätzlichen Systemen in der DMZ, z. B. zentraler (S)FTP-Server

Seite: 6 Gestaltung: 2008 Haufe Mediengruppe DMZ-Infrastruktur mit VMware Server

Erstellt von: Stefan Mössner



## Wie werden die Anforderungen erfüllt?

- Einführung von Virtualisierung
  - Konsolidierung von Hardware verbunden mit optimaler Ressourcen-Auslastung
- Anschaffung neuer leistungsfähiger Serverhardware für Virtualisierung
- Aufteilung der physikalischen DMZ-Systeme auf mehrere Rechnerräume
  - Absicherung gegen Stromausfall eines Rechnerraumes
- Isolation der einzelnen DMZ-Systeme (physikalisch und virtuell) in einzelne VLANs
  - Vermeidung von Übergriffsmöglichkeiten bei erfolgreichem Angriff auf ein DMZ-System
- Installation redundanter Maschinen mit automatischem Failover, aufgeteilt auf mehrere Rechnerräume
- Redundante Netzwerkanbindung der physikalischen und virtuellen Systeme
  - Absicherung gegen Netzwerkausfälle innerhalb eines Rechnerraumes
- Neuinstallation der Server mit aktuellem Betriebssystem
  - optimierte Ressourcen-Verwendung für mehr Performance
  - höheres Sicherheitslevel
  - gewährleistetester Software-Support

## Technische Umsetzung – Hard- und Software 1

- Server: HP ProLiant DL380, 2x Intel CPU (3,2 GHz), 10 GB RAM, lokale HDDs, 14 NICs
    - Standardhardware mit hoher Leistung für den Betrieb von bis zu 6 virtuellen Servern
    - Preiswerte Anschaffung über HP Renew
    - 14 Netzwerkkarten, jeweils 2 zu einem Fault-Tolerant-Team verbunden: 6 Teams werden direkt den VMs, 1 Team dem Servermanagement zugeordnet → höhere Netzwerkperformance und Absicherung gegen Netzwerkausfälle für die einzelnen VMs verfügbar
  - Virtualisierung: VMware Server 1.0.x
    - Stabile Plattform
    - VMware ist Vorreiter beim Thema Virtualisierung
    - Umfangreiches VMware-Know-How im Unternehmen vorhanden durch Betrieb von VMware Server bzw. GSX (8x Windows und 2x Debian-Linux) und VMware ESX (5 Server)
    - Kostenfreie Software
    - Sehr einfaches Handling
- ...

## Technische Umsetzung – Hard- und Software 2

- OS: Windows 2003 Server Enterprise Edition R2, 32 Bit
  - Windows ist Unternehmensstandard
  - Unterstützung von Systemen mit größerem RAM (bis 64 GB, Standard Edition nur bis 4 GB)
  - Microsoft erlaubt kostenfreie Installation von bis zu vier VMs mit Windows 2003 Server bis einschl. Enterprise Edition
    - geringere Lizenzkosten gegenüber Einzelsystemen
  - Betrieb unter Linux ist problematisch: Linux kann VLAN-Tagging, aber es gibt dafür kein offizielles How-To und keinen Support seitens VMware
- Switches: Cisco Catalyst 2950 FX mit 24 Ports
  - Cisco ist Unternehmensstandard
  - Managebar
  - gute Fehleranalysemöglichkeiten

## Technische Umsetzung – Migration 1

1. Installation der physikalischen VMware Server
  - Basisinstallation der physikalischen Host-Server
2. Migration einzelner physikalischer Systeme als virtuelle Server mit VMware Converter
  - kostenfreie Software (nur Enterprise Edition ist kostenpflichtig und bietet mehr Features)
  - Übernahme der physikalischen Systeme kann im laufenden Betrieb nahezu ohne Ausfallzeiten erfolgen (in der Regel ist nur ein Systemreboot notwendig)
3. Parallele Neuinstallation einiger DMZ-Systeme als virtuelle Server
  - Installation neuer virtueller Maschinen
  - Installation der Anwendungen innerhalb der VMs
4. Umstellung der bestehenden DMZ in ein VLAN
  - Umstellung ist mit einer Downtime bzgl. Netzwerkanbindung verbunden (ca. 30 Minuten)

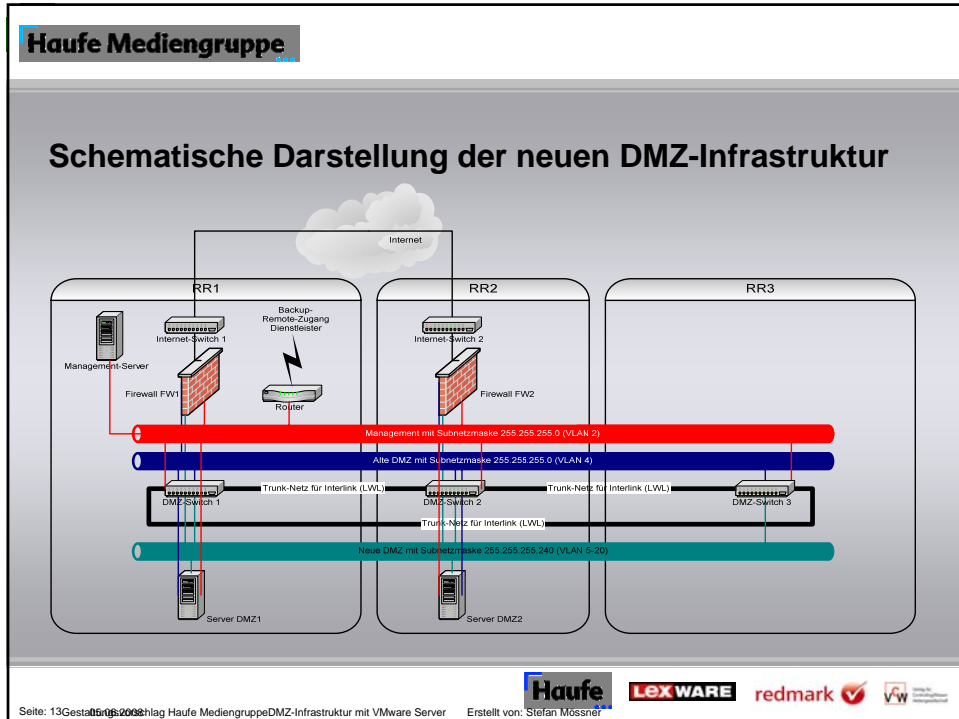
→ ...

## Technische Umsetzung – Migration 2

5. Einrichtung neuer DMZs als weitere VLANs  
→ parallel zur bestehenden DMZ
6. Einbindung der VMware-Hosts und der jeweiligen VMs in die neuen DMZs
7. Produktivnahme neuer DMZs an einem Abend  
→ Übernahme physikalischer Systeme (Switchports in VLAN migrieren)  
→ Migration der aktuellen Anwendungsdaten auf die neuen Systeme  
→ Umstellung NAT auf Firewall  
→ Test

## Darstellung der neuen DMZ-Infrastruktur

- Ab Februar 2007:
  - 2 physikalische VMware-Hosts
  - 6 virtuelle Maschinen (3 pro Host): davon 2 Windows-NT-Server
  - 4 physikalische DMZ-Server (zuvor 10): 1x ISA-, 2x Terminal-Server und 1x Webserver
- Ab Mai 2007:
  - Ablösung der Windows NT Server durch Windows Server 2003, verbunden mit der Abschaltung der Windows-NT-Domäne in der DMZ im Februar 2008
  - Virtualisierung des physikalischen Webservers (Migration mit VMware Converter)
- Seit April 2008:
  - 2 physikalische VMware-Hosts
  - 7 virtuelle Maschinen (Aufteilung: 3+4)
  - 4 physikalische DMZ-Server: 1x ISA-, 2x Terminal-Server und ein VPN-Gateway-Server



**Haufe Mediengruppe**

## Erfahrungen 1

- Keine Ausfälle seit Inbetriebnahme im Februar 2007  
→ Sehr stabile Systemplattform
- Aus Zeitgründen und mit Ausblick auf bevorstehende Abschaltung wurden die Windows-NT-Systeme mit VMware Converter virtualisiert  
→ Einfache Migration, häufig verbunden mit Treiberproblemen bei SVGA-Grafikkarte von VMware
- Höherer Aufwand bei Verkabelung neuer DMZ-VMs  
→ massiver Netzwerkkabelbaum am Hostserver durch hohe Portdichte  
→ redundante Verkabelung in verschiedene Rechnerräume
- Geringer Installationsaufwand neuer DMZ-VMs  
→ in kurzer Zeit aus fertigen Vorlagen neue VMs erstellbar
- Geringer Administrationsaufwand im Betrieb  
→ zentrale „Anlaufstelle“ zur Verwaltung der einzelnen VMs  
→ kann durch Einsatz von Virtual Center für VMware Server noch weiter verbessert werden (kostenpflichtig)

→ ...

Seite: 14 Gestaltung: 06.2008 Haufe Mediengruppe DMZ-Infrastruktur mit VMware Server Erstellt von: Stefan Mössner

**Haufe** **LEXWARE** **redmark** **VW**

## Erfahrungen 2

- Geringer Administrationsaufwand bei Security-Updates
  - weniger Abstimmungsaufwand mit Fachbereichen
  - Einspielung und System-Reboot im laufenden Betrieb möglich durch redundante Umgebung
- Viele Überwachungsmöglichkeiten zur Fehleranalyse
  - Web-Oberfläche VMware Server mit groben Systemauslastungsangaben (mit Virtual Center noch weiterführende Analysen möglich)
  - CISCO IOS mit weitreichenden Analysefunktionen: Switchauslastung, Portüberwachung usw.
- Virtualisierung nicht immer sinnvoll oder technisch machbar
  - ISA-Server: Anzahl max. möglicher Netzwerkkarten
  - Terminal-Server: Virtualisierung besser unter ESX wegen besserer Systemperformance
  - Datenbank-Server: Virtualisierung besser unter ESX wegen besserer Systemperformance
  - Anwendungshersteller supportet virtuelle Umgebungen nicht
- Abschaltung der alten DMZ nicht möglich
  - Aufwand bei den dort verbliebenen Systemen sehr hoch, z. B. bei VPN-Konzentrator
- Migration erfolgte mit einem Minimum an Ausfallzeiten
  - insgesamt ca. 5 Stunden: einzelne Systeme waren nach ca. 30 Minuten online

# Fragen?

## Vielen Dank!

Stefan Mössner  
Systemadministration  
IT-Infrastruktur

Rudolf Haufe Verlag GmbH & Co. KG  
Ein Unternehmen der Haufe Mediengruppe  
Lörracher Str. 9, D-79115 Freiburg  
Tel: 0761/47 08-277, Fax: 0761/47 08-820-277  
E-Mail: stefan.moessner@haufe.de  
Internet: <http://www.haufe.de>