ISA Server 2004 – System Hardening - Von Marc Grote

Die Informationen in diesem Artikel beziehen sich auf:
Microsoft ISA Server 2004

Dieser Artikel beschreibt die notwendigen Schritte um einen installierten ISA Server 2004 so abzusichern, damit ein maximaler Schutz des ISA Servers und auch des darunter liegenden Betriebssystems gewährleistet ist. Es werden dabei nicht nur die Schritte erläutert, um einen ISA Server 2004 abzusichern, sondern auch Empfehlungen und Hinweise gegeben um für eine Gesamtsicherheit des Systems zu sorgen (sofern so etwas überhaupt möglich ist).

Dieser Artikel unterteilt sich in folgende Kapitel:

Erstellen einer Security Policy

Die Erstellung und laufende Pflege einer Security Policy ist in vielen Unternehmen ein unliebsames Übel und wird gerne ignoriert, weil es, zugegebenermaßen, mit
sehr viel Arbeit verbunden ist. Der Autor hält die Erstellung einer Security Policy in mittelständischen- und Großunternehmen jedoch für sehr sinnvoll.
Was ist eine Security Policy? - Eine SP definiert alle organisatorischen und technischen Maßnahmen eines Unternehmens welche zur Einrichtung, Betrieb und Wartung von Firewallsystemen notwendig sind. Die SP definiert nicht nur die technische Lösung und Dokumentation der Perimeter Sicherheit, sondern auch organisatorische Fragen wie Verpflichtungserklärungen der Mitarbeiter zum Datenschutz, Verhalten im Internet, aber auch Notfallpläne bei Kompromittierung des ISA Servers - Um nur ein Beispiel zu nennen: Sie sind Administrator eines mittelständischen Unternehmens mit 350 Beschäftigten, welches in hohem Maße von einer Internet Anbindung abhängig ist. jetzt stellen Sie fest, dass Sie einen 'Eindringling" im System haben oder das System von Viren befallen ist. Können Sie jetzt einfach die Systeme vom Internet trennen? Wer entscheidet über die weitere Vorgehensweise? Diese und viele andere Fragen und Antworten werden in einer SP festgehalten.
Ein weiterer Vorteil einer SP ist natürlich auch, dass Sie damit eine ständig aktualisierte Dokumentation der Firewall-Infrastruktur besitzen.

Schulung des Personals + verantwortungsvoller Umgang mit den Firewallsystemen

Es kann nicht oft genug betont werden, wie wichtig es ist, für die Verwaltung des ISA Server und der umgebenden Infrastruktur qualifiziertes und geschultes Personal einzusetzen, welches sich nicht nur mit der Verwaltung des ISA Servers auskennt, sondern auch Verständnis für Netzwerkprotokolle, Systemsicherheit und allgemeine Sicherheitskenntnisse nachweisen kann.
Des weiteren ist ein verantwortungsvoller Umgang mit den Firewallsystemen notwendig. Eine unbewusste Fehlbedienung der Firewall kann zu unerwünschten Ergebnissen führen. Mehr zu diesem Thema erfahren Sie in dem Kapitel "*Restriktives ISA Server Regelwerk*".

Sollten Sie selbst nicht in der Lage sein, ein Firewallsystem wie den ISA Server 2004 zu verwalten, suchen Sie sich bitte entsprechende Unterstützung durch externes Consulting oder mit Hilfe der ISA Server Newsgroup und Webseiten wie dieser.

Jeder Anfang ist schwer, aber es ist auch noch kein Meister vom Himmel gefallen.

Physikalische Sicherheit

Für einen sicheren ISA Server Betrieb müssen Sie sich auch um die physikalische Sicherheit der Systeme kümmern. Unter den Begriff "Physikalische Sicherheit" fallen:

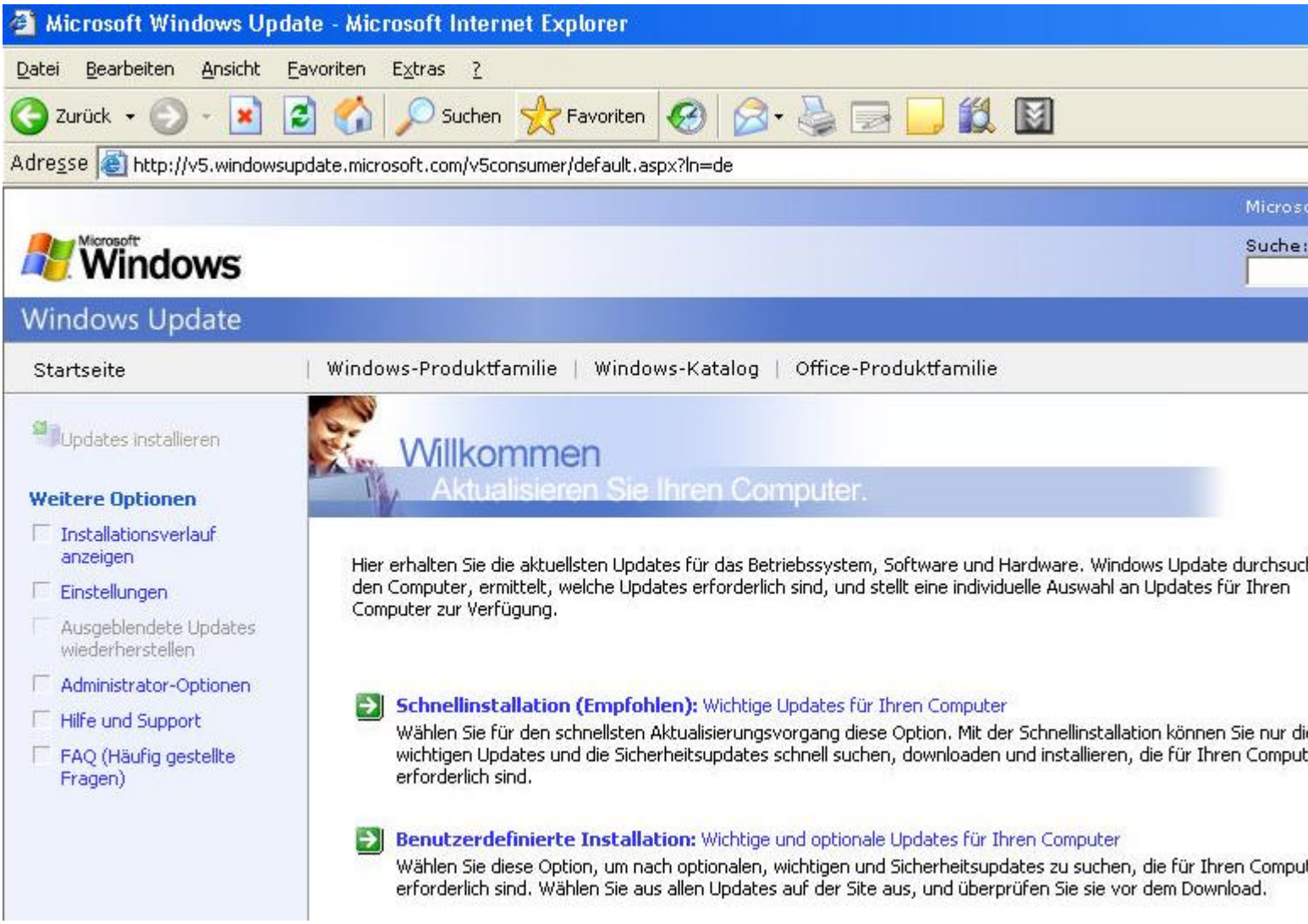
- Zugangsschutz zum Serverraum / IT-Infrastruktur (verstärkte Türen, Sicherheitsglas, Bewegungsmelder uvm.)
- Zutrittsschutz zum Serverraum / EDV-Raum (z. B. Zahlenschloss).
- Diebstahlschutz für die Server (zum Beispiel Montage in Racks mit abschließbaren Türen, spezieller Diebstahlschutz für Server)

Denken Sie auch daran, die restliche Infrastruktur entsprechend zu schützen. Es handelt sich hierbei natürlich nur um einige simple Beispiele. Das Thema "physikalische Sicherheit" kann Bände füllen.

Es gilt der Grundsatz: Kein System ist vor Angreifern sicher, wenn für den Angreifer ein physikalischer Zugriff auf die Systeme besteht.

Systemupdates für ISA und Windows

Der erste Schritt einer erfolgreichen Verteidigungslinie gegen potentielle Angriffe auf Ihre Infrastruktur ist die Überprüfung sowohl des ISA Servers als auch der Windows Plattform auf laufende Updates und neu entdeckte Sicherheitslücken. Stellen Sie ein sicher, dass Windows- und ISA Updates regelmäßig nach Prüfung eingespielt und dokumentiert werden.



Damit Sie bei potentiellen Sicherheitslücken auf dem laufenden sind, empfiehlt sich der regelmäßige Besuch der Microsoft Security Seiten und der Webseiten von Windows und ISA. Sie finden eine Übersicht über empfohlene Webseiten am Ende des Artikels.
Es besteht auch die Möglichkeit zum Abonnement von Newslettern, mit deren Hilfe Sie per E-Mail über neue Gefährdungen informiert werden.

Es lohnt sich auch ein regelmäßiger Blick auf die Webseite von www.msisafaq.de. Dieter Rauscher stellt auf dieser Seite eine Sammlung von Skripten zur Erstellung von HTTP Filter Signaturen zur Verfügung. Es handelt sich hier um Filter Signaturen diverses ISA Gurus.

Härten des Betriebsystems

Eine wichtige Aufgabe eines ISA Administrators ist es, das zugrunde liegende Betriebssystem (Windows 2000 oder Windows 2003) entsprechend abzusichern und auf die aktuellen Anforderungen abzustimmen. Ziel ist auch hier die Minimierung der Angriffsoberfläche.
Maßnahmen zur Minimierung der Angriffsoberfläche:

- Deaktivierung nicht benötigter Dienste
- Installation nur der notwendigsten Windows Komponenten
- Einschränkung der administrativen Zugriffe
- Einsatz von Sicherheitsvorlagen

Deaktivierung nicht benötigter Dienste

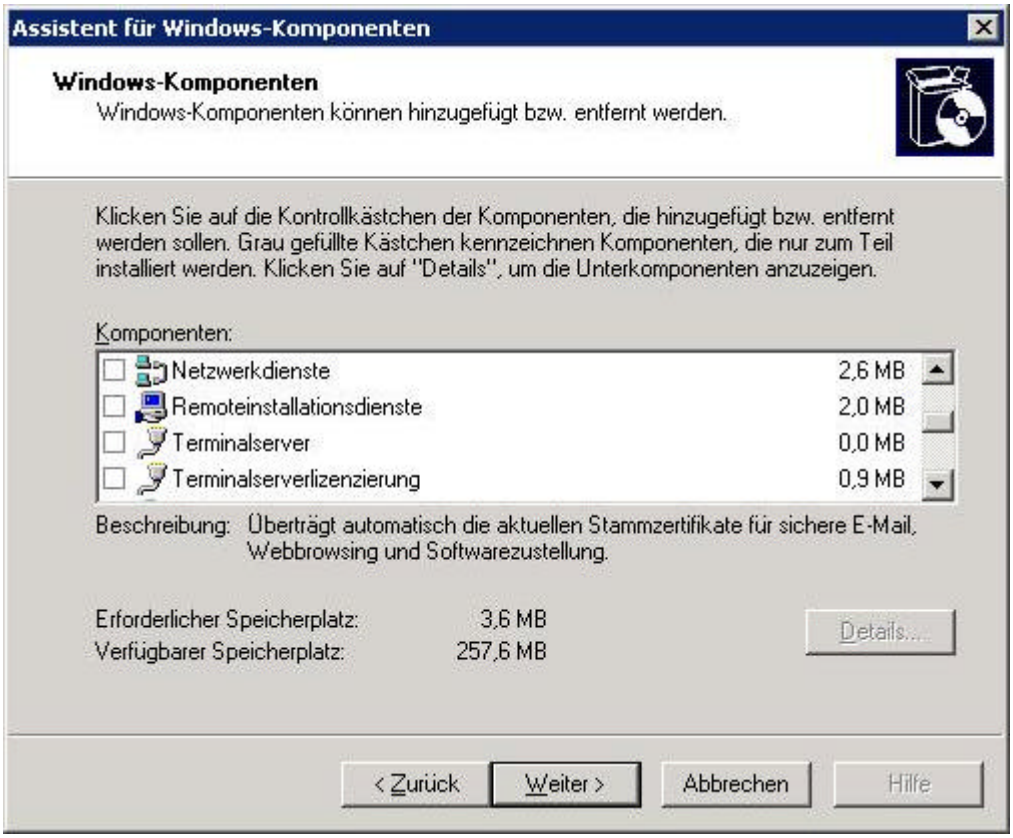
Erforderliche Dienste um die Funktionalität des ISA Servers sicher zu stellen:

Dienstname	Funktionszweck	Startart
COM+ Event System	Betriebssystem	Manuell
Cryptographic Services	Betriebssystem (Sicherheit)	Automatisch
Event Log	Betriebssystem	Automatisch
IPSec Services	Betriebssystem (Sicherheit)	Automatisch
Logical Disk Manager	Betriebssystem (Festplattenmanagement)	Automatisch
Logical Disk Manager Administrative Service	Betriebssystem (Festplattenmanagement)	Manuell
Microsoft Firewall	Erforderlich für den ISA Server	Automatisch
Microsoft ISA Server Control	Erforderlich für den ISA Server	Automatisch
Microsoft ISA Server Job Scheduler	Erforderlich für den ISA Server	Automatisch
Microsoft ISA Server Storage	Erforderlich für den ISA Server	Automatisch
MSSQL$MSFW	Erforderlich für MSDE Logging am ISA Server	Automatisch
Network Connections	Betriebssystem (Netzwerkinfrastruktur)	Manuell
NTLM Security Support Provider	Betriebssystem (Sicherheit)	Manuell
Plug and Play	Betriebssystem	Automatisch
Protected Storage	Betriebssystem (Sicherheit)	Automatisch
Remote Access Connection Manager	Erforderlich für den ISA Server	Manuell
Remote Procedure Call (RPC)	Betriebssystem	Automatisch
Secondary Logon	Betriebssystem (Sicherheit)	Automatisch
Security Accounts Manager	Betriebssystem	Automatisch
Server	Erforderlich für ISA Server Firewall Client Share	Automatisch
Smart Card	Betriebssystem (Sicherheit)	Manuell
SQLAgent$MSFW	Erforderlich für MSDE Logging am ISA Server	Manuell
System Event Notification	Betriebssystem	Automatisch
Telephony	Erforderlich für den ISA Server	Manuell
Virtual Disk Service (VDS)	Betriebssystem (Festplattenmanagement)	Manuell
Windows Management Instrumentation (WMI)	Betriebssystem (WMI)	Automatisch
WMI Performance Adapter	Betriebssystem (WMI)	Manuell

Installation nur der notwendigsten Windows Komponenten

Installieren Sie auf der Windows Maschine nur benötigte Komponenten und verzichten Sie auf zusätzliche Programme wie DHCP, WINS, RIS, Terminalserver usw. wenn diese nicht absolut notwendig

sind.

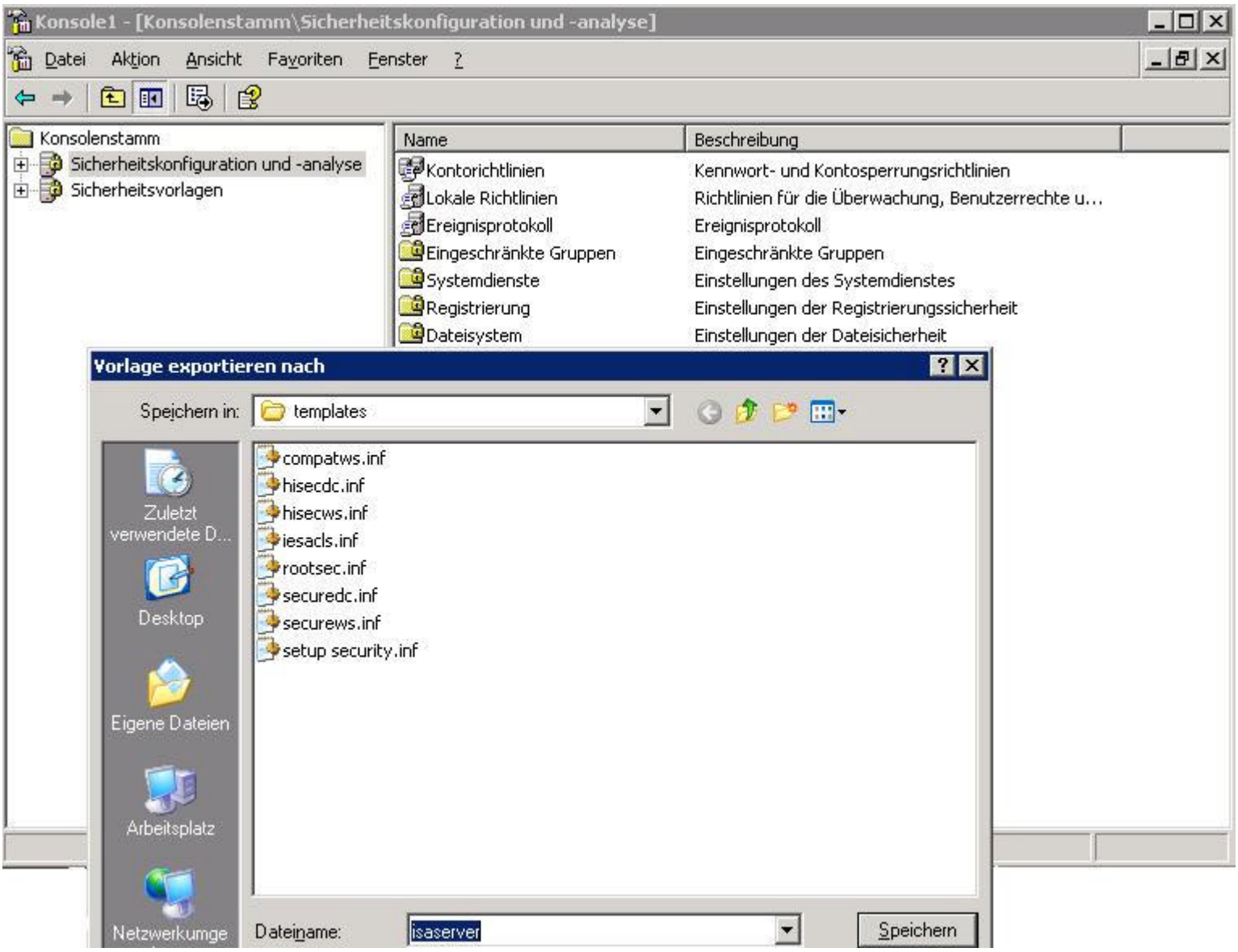


Einschränkung der administrativen Zugriffe

- Benennen Sie den Administrator Account nach erfolgter Windows Installation um und deaktivieren Sie den Account. Es kann sinnvoll sein, diesen Account dauerhaft zu monitoren, um zu ermitteln, wer versucht, sich mit dem Administrator Account anzumelden bzw. zu "hacken".
- Erstellen Sie einen zusätzlichen Account mit administrativen Berechtigungen, welchem Sie ein sehr langes und sicheres Kennwort vergeben.
- Reduzieren Sie ihre tägliche Arbeit am ISA Server mit administrativen Berechtigungen auf Minimum und verwenden Sie Administrator Privilegien nur, wenn das absolut notwendig ist.
- Beschränken Sie die Zahl der auf der Maschine eingerichteten Windows Administratoren auf ein Minimum.

Einsatz von Sicherheitsvorlagen

Ein bewährtes Prinzip zur Sicherung einer Windows 2000 / 2003 Maschine nach einem festen Schema sind so genannte Sicherheitsvorlagen. Sicherheitsvorlagen sind strukturierte Textdateien (.INF Dateien) die als Basis für eine Sicherheitskonfiguration mit dem Security Configuration Editor (SCE) verwendet werden können.
In den Sicherheitsvorlagen werden Einstellungen wie Kontenrichtlinien, Überwachungsrichtlinien, Registrierungseinstellungen, Konfiguration für Systemdienste uvm. definiert. Nach erfolgter Definition können Sie das aktuelle System anhand der Sicherheitsvorlage konfigurieren. Mit Hilfe der Sicherheitsvorlage ist sichergestellt, dass Sie immer ein und dieselbe Sicherheitskonfiguration auf Ihre Systeme anwenden.



ISA Server 2004 Firewalltypen

ISA Server 2004 bietet die Konfiguration von verschiedenen Firewalltypen. Die Konfiguration basiert auf so genannten Netzwerkvorlagen. ISA Server 2004 bietet folgende Netzwerkvorlagen an:

Edgefirewall
Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der sich ISA Server an der äußeren Schnittstelle des Netzwerks befindet. Ein Netzwerkadapter ist hierbei mit dem internen Netzwerk verbunden. Der andere Netzwerkadapter verfügt hingegen über eine Verbindung mit einem externen Netzwerk (Internet). Bei Auswahl dieser Vorlage können Sie den gesamten ausgehenden Datenverkehr zulassen oder den ausgehenden Datenverkehr einschränken, so dass nur der Webzugriff gestattet wird.

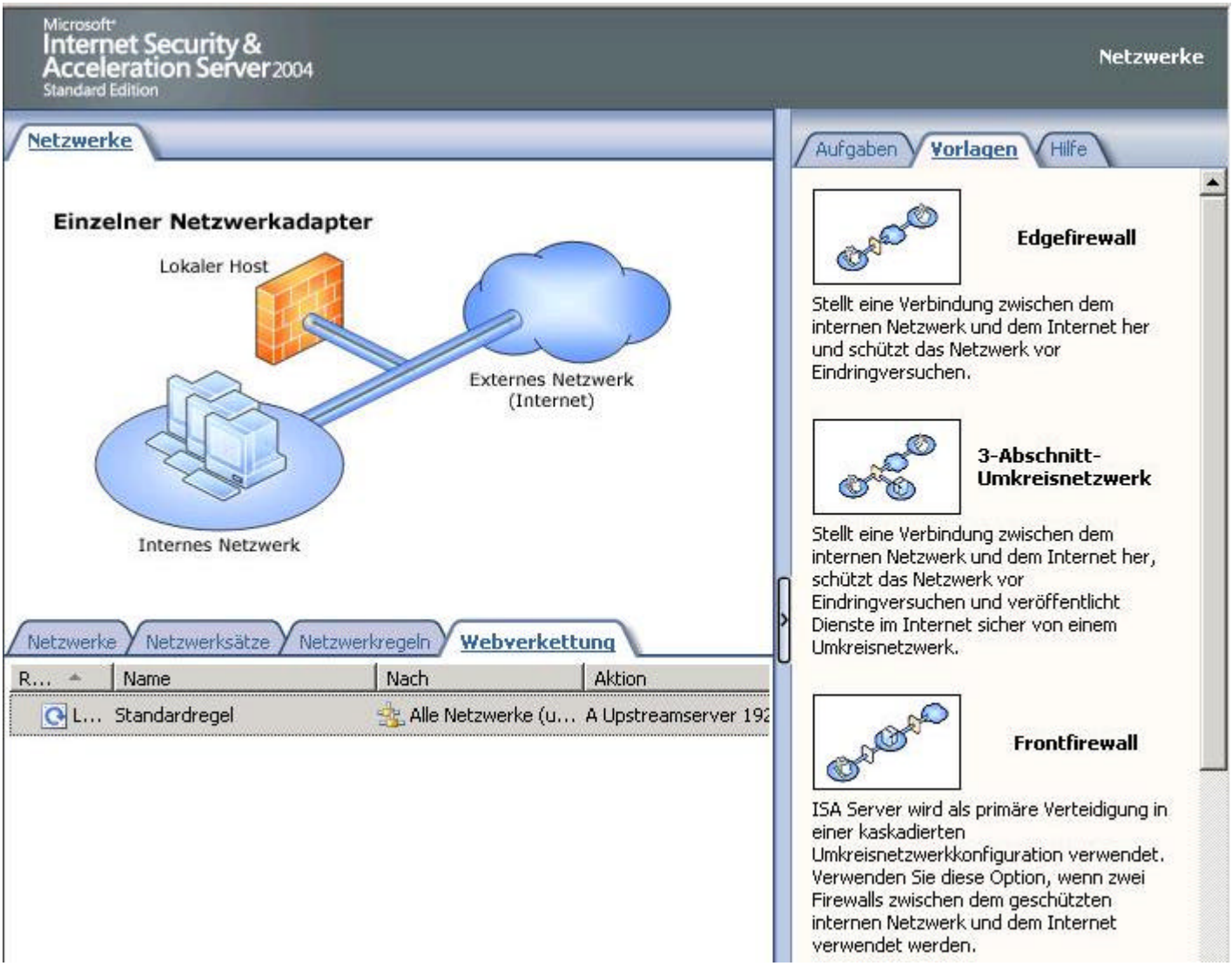
3-Abschnitt-Umkreisnetzwerk
Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der ISA Server mit dem internen Netzwerk, dem externen Netzwerk und einem Umkreisnetzwerk (auch als DMZ, demilitarisierte Zone oder abgeschirmtes Subnetz bezeichnet) verbunden ist.

Frontfirewall-Netzwerkvorlage
Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der sich ISA Server an der äußeren Schnittstelle eines Netzwerks befindet und zum Schutz des internen Netzwerks ein weiterer Firewall am

Back-End konfiguriert ist.

Backfirewall-Netzwerkvorlage
Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der ISA Server an der Schnittstelle zwischen einem Umkreisnetzwerk und dem internen Netzwerk eingesetzt wird und zum Schutz des internen Netzwerks am Back-End ein weiterer Firewall konfiguriert ist.

Einzelner Netzwerkadapter
Bei dieser Vorlage wird eine Netzwerkkonfiguration mit einem einzelnen Netzwerkadapter angenommen, der sich innerhalb eines Umkreis- oder Firmennetzwerks befindet. In dieser Konfiguration dient ISA Server als Webproxy- und Cacheserver.



Für weitere Informationen zum Thema Netzwerkdefinition lesen Sie folgenden Artikel.

ISA Installationsmöglichkeiten

ISA Server 2004 lässt sich auf Windows 2000 und Windows 2003 installieren. Aufgrund der erweiterten Sicherheitsfunktionen und des etwas eingeschränkten Funktionsumfangs des ISA Servers unter Windows 2000 empfiehlt der Autor die Installation des ISA Servers auf einer Windows 2003 Maschine.
Bei der Installation des ISA Servers stellt sich des öfteren die Frage, wie die Windows 2000 / 2003 Maschine an das interne Netzwerk angebunden wird.

Es gibt hier zwei ultimative Aussagen:

- Installieren Sie den ISA Server 2004 **niemals** auf einem Windows 2000 / 2003 Domänencontroller
- Installieren Sie den ISA Server 2004 nicht auf einem Windows 2000 / 2003 Mitgliedsserver wenn sich der ISA Server als so genannte Frontfirewall oder auch Egde Firewall direkt mit dem "Internet" verbunden ist.

Microsoft empfiehlt auch in einigen Whitepapern die Installation der ISA Server 2004 in einem separaten Forest. Diese Konstellation macht aus Sicht des Autors erst Sinn, wenn man eine Vielzahl von ISA Servern betrieben will und zum Beispiel von Gruppenrichtlinien und der Speicherung der Array Informationen im Active Directory (nur ISA 2004 Enterprise) profitieren will.

Keine Regel ohne Ausnahme:

Betreiben Sie den ISA Server im Rahmen einer Front- und Backend Firewallkonfiguration als Backend-Server, bestehen keine Sicherheitsbedenken, den ISA Server 2004 auf einem Windows 2000 / 2003 Mitgliedsserver zu installieren.
Lässt Ihr IT Budget keine Investition in zusätzliche Hardware und Software-Lizenzen zu, können Sie den ISA Server natürlich auf einem Domänencontroller installieren (Microsoft geht mit dem Small Business Server 2003 ja diesen Weg).

Installieren Sie den ISA Server 2004 erst, nachdem Sie das zugrunde liegende Windows System entsprechend "gehärtet" haben. Installieren Sie den ISA Server von einer vertrauenswürdigen Installationsquelle, welche garantiert virenfrei ist und von deren Herkunft Sie sicher sind, dass es sich um die Original ISA Installationsdateien handelt.
Schließen Sie die Windows Maschine, auf der ISA Server 2004 installiert werden soll, nicht an das "Internet" an, bis Sie den ISA Server 2004 vollständig installiert, konfiguriert und die notwendigen Updates installiert haben. Nach erfolgter ISA Installation existiert eine Default Policy, die so genannte Cleanup Rule, welche sämtlichen Datenverkehr zum Internet verweigert.

Restriktives ISA Server Regelwerk

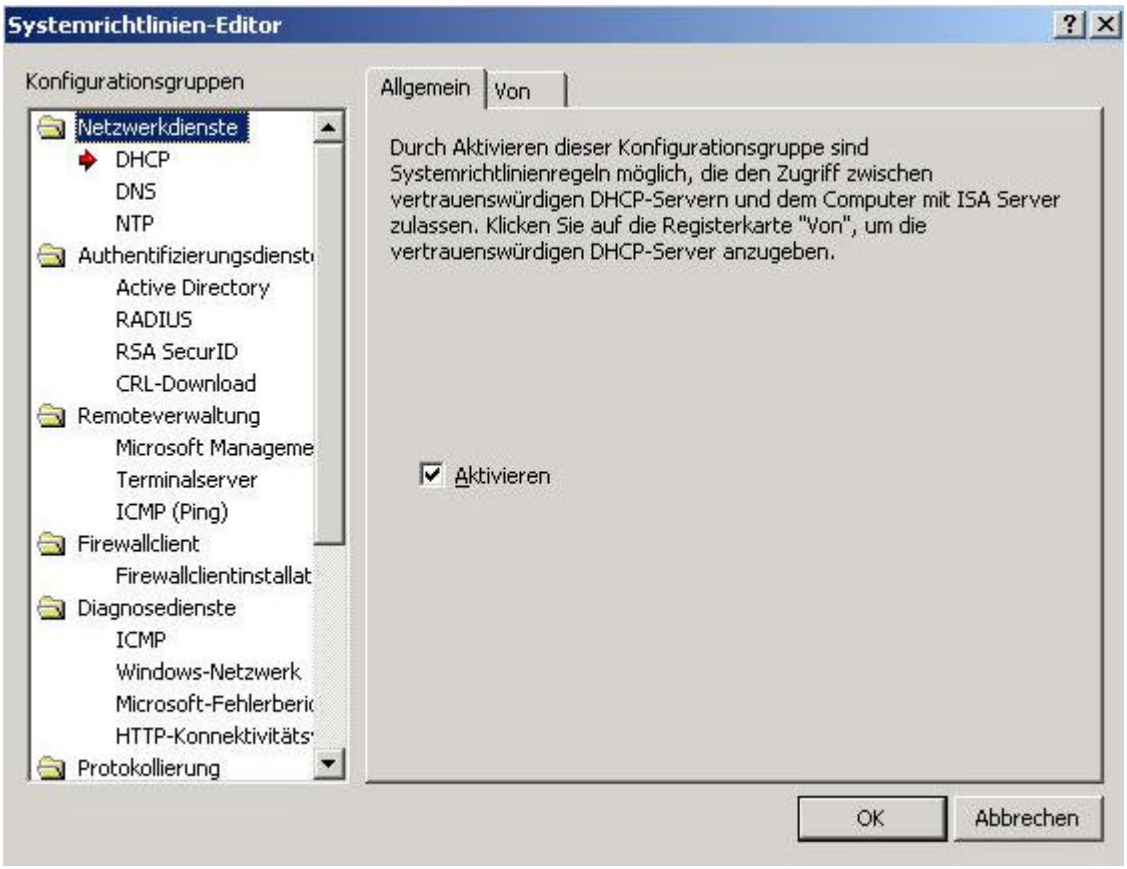
Stellen Sie als ISA Server Administrator sicher, dass Sie mit einem minimalen ISA Server Regelwerk arbeiten, welches nur das absolute Mindestmaß an Firewallrichtlinien zulässt.

Faustformel: Bei der Einrichtung eines Firewallregelwerkes wird nach dem Minimalprinzip gearbeitet.

Gehen Sie dazu wie folgt vor:

Verschaffen Sie sich einen Überblick über Ihre Infrastruktur und protokollieren Sie die notwendigen Kommunikationsbeziehungen von **INTERN** nach **EXTERN** und zum **ISA Server** selbst.
Legen Sie fest, welche Kommunikationsbeziehungen von **EXTERN** nach **INTERN** notwendig sind.
Basierend auf diesen Informationen gehen Sie dazu über, die notwendigen Protokolle zu definieren (wenn Sie der ISA Server noch nicht vorkonfiguriert hat), erstellen Sie die notwendigen Computersätze, Zielsätze usw.

Modifizieren Sie jetzt als erstes die Systemrichtlinie des ISA Servers, um diese auf Ihre Bedürfnisse anzupassen. Microsoft liefert mit dem ISA Server 2004 eine Standard Systemrichtlinie aus, welche den Zugriff auf das interne Interface des ISA Servers schützt und nur bestimmte Infrastrukturprotokolle wie DNS, DHCP usw. zulässt. Passen Sie diese Systemrichtlinie auf Ihre aktuelle Konfiguration an um eine geringstmögliche Angriffsfläche zu bieten.



Jetzt können Sie die entsprechenden Regelwerke erstellen und dokumentieren. Dokumentieren Sie jede erstellte Firewall Policy mit dem Erstellungsgrund und was diese Policy ermöglichen soll, damit Sie auch in naher Zukunft einen Überblick über Ihr Regelwerk behalten. Beachten Sie auch die Reihenfolge der Firewall Policies. ISA Server 2004 arbeitet die Firewall Policies anders als der ISA Server 2000 ab.

Kleiner Tipp:

Platzieren Sie die am häufigsten verwendeten Firewall Policies am Anfang des Regelwerkes um die Performance etwas zu erhöhen. Achten Sie aber trotzdem darauf, dass durch das Verschieben der Regeln keine unerwünschten Ergebnisse auftreten.

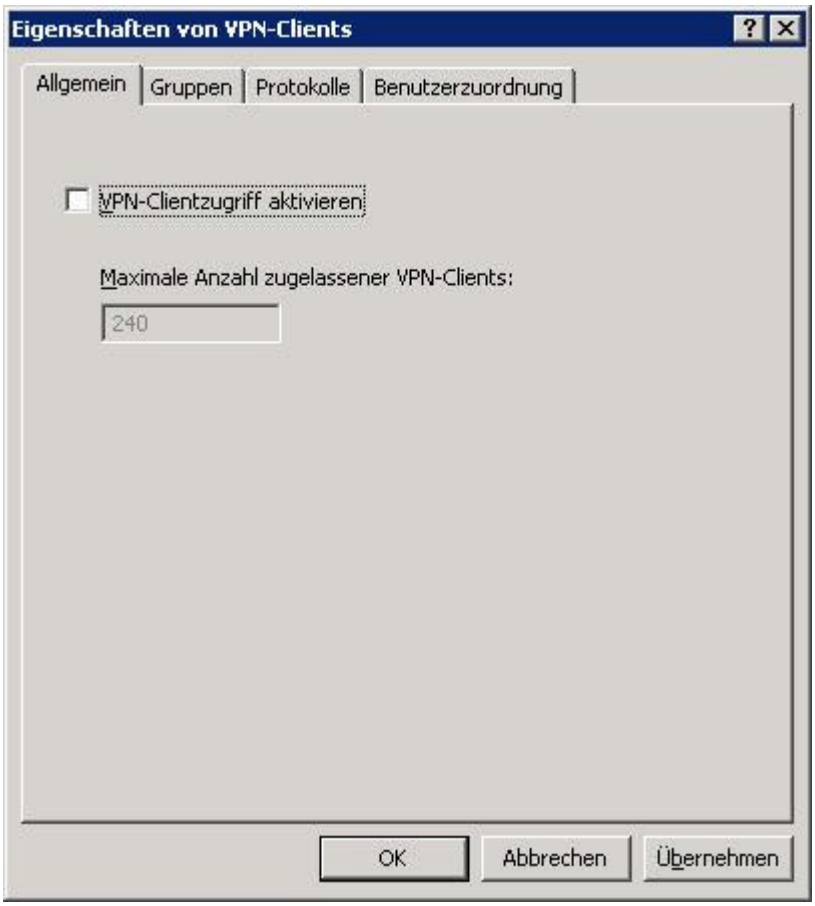
Arbeiten Sie nach dem Minimalprinzip, dass heißt, erstellen Sie das Regelwerk so restriktiv und minimal wie möglich.

Aktivierte ISA Server Komponenten

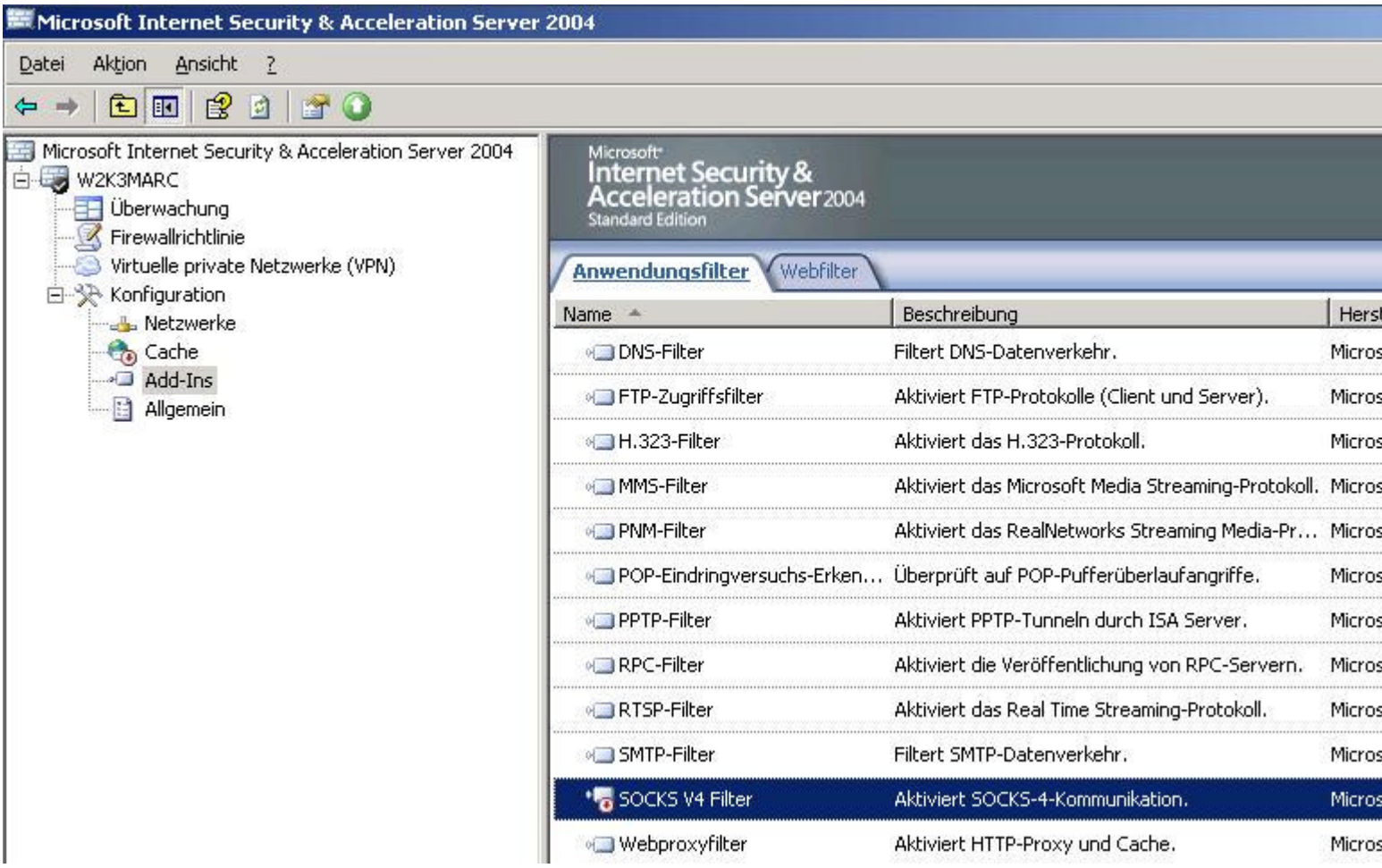
Je nach Einsatzzweck des ISA Server 2004, sollten Sie nur die absolut notwendigen ISA Komponenten

während der Installation auswählen und auch nach der Installation nur die benötigten Komponenten aktivieren.
Benötigen Sie zum Beispiel den ISA Server nicht als Webcache Lösung, lassen Sie den Cache deaktiviert (Default Einstellung des ISA Server 2004).

Verwenden Sie den ISA Server 2004 nicht als VPN Server, so können Sie die VPN Funktionalität am ISA Server 2004 auch deaktivieren.



Deaktivieren Sie auch nicht benötigte Anwendungs- und Webfilter.



ISA Server Verwaltungsdelegation

ISA Server 2004 bietet als erste Microsoft Firewall die Möglichkeit, an nicht administrative Benutzer ISA Berechtigungen zu delegieren. Es stehen drei verschiedene Verwaltungsdelegationen zur Verfügung:

- ISA Server-Standardüberwachung
- Erweiterte ISA Server-Überwachung
- ISA Server-Hauptadministrator

ISA Server-Standardüberwachung

Benutzer und Gruppen mit dieser Rolle können die Computer- und Netzwerkaktivität des ISA Server-Computers überwachen, ohne jedoch einzelne Überwachungsfunktionen konfigurieren zu können.

Erweiterte ISA Server-Überwachung

Benutzer und Gruppen mit dieser Rolle können sämtliche Überwachungsaufgaben (einschließlich der Konfiguration von Protokollen und Alarmdefinitionen) sowie alle für die Rolle ISA Server-Basisüberwachung verfügbaren Überwachungsfunktionen durchführen.

ISA Server-Hauptadministrator

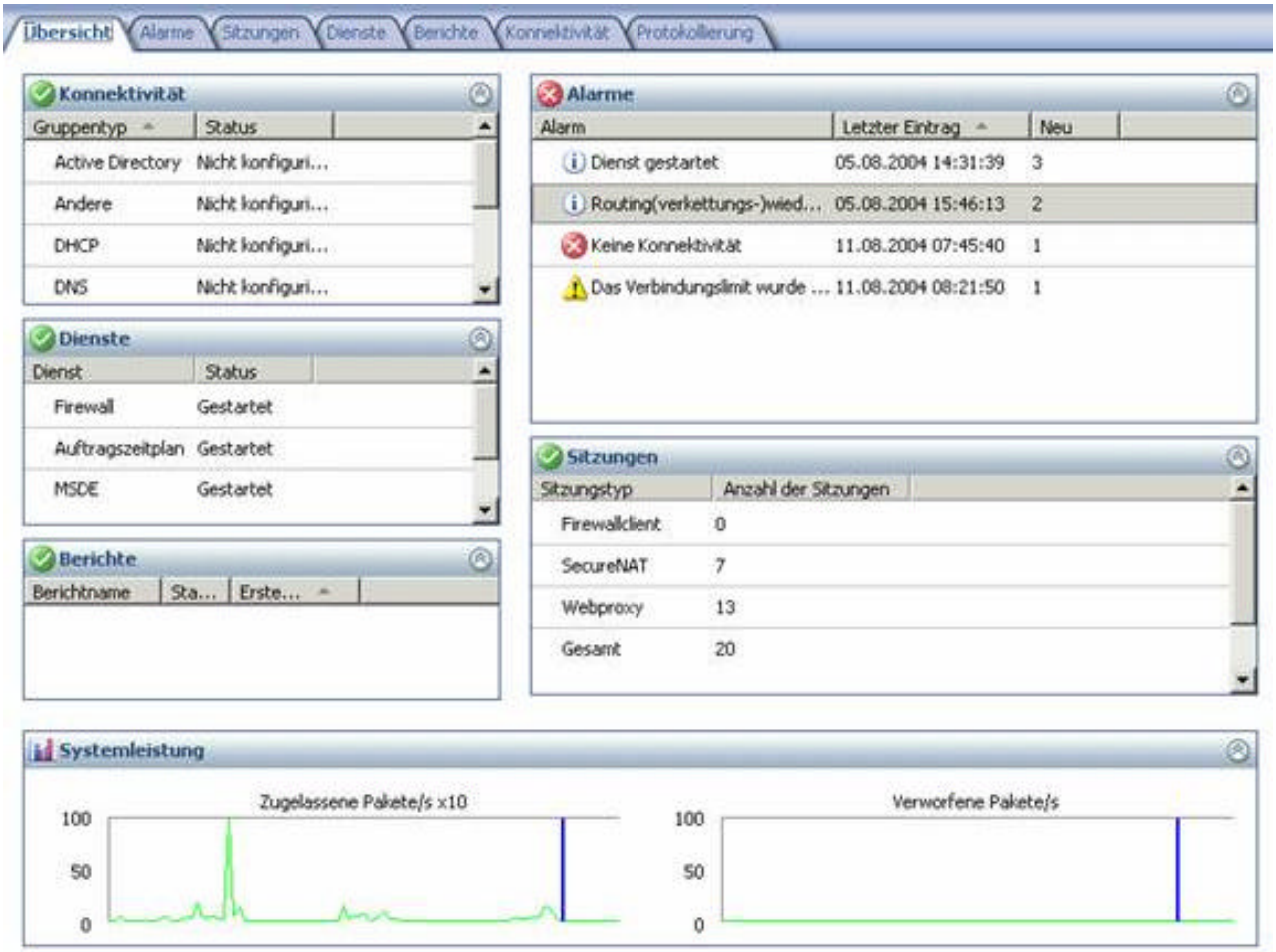
Benutzer und Gruppen mit dieser Rolle können sämtliche ISA Server-Aufgaben durchführen, einschließlich des Anwendens von Netzwerkvorlagen, der Netzwerk- und Regelkonfiguration und der Überwachung.

Laufende Überwachung der Firewall

Als ISA Server Administrator ist es Ihre ureigenste Aufgabe, das Firewallsystem ständig überwachen und für eine ausreichende Performance zu sorgen.

Zu den Überwachungs/Wartungstätigkeiten gehören:

- Tägliche Analyse der ISA Server Logdateien auf verdächtige Aktivitäten
- Tägliche Durchsicht der Meldungen der Ereignisanzeige
- Überprüfen der Festplattenkapazität um einen Systemüberlauf zu vermeiden
- Sichern der Logdateien und der Ereignisanzeige auf einen anderen Rechner als den ISA Server um im Falle eine Angriffs Logmanipulation vorzubeugen und eine gewisse Revisionssicherheit bei Protokolldaten zu erreichen.



Für weitere Informationen zum Thema Monitoring lesen Sie folgenden Artikel und diesen.

Lassen Sie sich auf alle Fälle bei dem Eintreten von wichtigen Ereignissen auf dem ISA Server informieren. Es stehen Ihnen dazu verschiedene Möglichkeiten zur Verfügung:

Sie können sich zum Beispiel per E-Mail informieren lassen, wenn ein bestimmter ISA Alarm auftritt. Für weitere Informationen zum Thema ISA Alarme lesen Sie folgenden Artikel.

Applikationen auf dem ISA Server

Sehr häufig wird die Frage gestellt, wie man denn bestimmte Applikationen auf dem ISA Server installiert und diese dann zur Nutzung von internen und auch externen Zugriffen konfiguriert.

Es gibt hier eine definitive Aussage: **Eine Firewall ist eine Firewall und kein Applikationsserver!**

Was heißt das konkret? Im Normalfall ist der ISA Server eine reine Firewall und es sind keine Applikationen auf dem ISA Server installiert, weil diese die Sicherheit der Firewall kompromittieren können und das System offener für so genannte Exploits machen.
Vermeiden Sie nach Möglichkeit die Installation von Anwendungen direkt auf dem ISA Server. Installieren Sie statt dessen Applikationen, welche im Internet zugänglich sein sollen, in der DMZ (DeMilitarisierten Zone). Sie können auch interne Server über ISA Server 2004 Serververöffentlichungs- und Webserververöffentlichungsregeln verfügbar machen.

Einsatz von Virenscanner- und anderer Gateway-Software

Fast schon obligatorisch zu erwähnen ist es, dass Sie auf dem ISA Server 2004 einen sich ständig aktualisierenden Virenscanner installieren, welcher das System laufend auf Virenbefall überprüft. Es existieren eine Vielzahl von Virenscannerlösungen für den ISA Server.
Da der ISA Server den Einstiegspunkt in Ihr Firmennetzwerk darstellt, gilt der Grundsatz: "Stoppen Sie Eindringlinge und Viren so früh wie möglich". Aus diesem Anlass installieren Sie auf dem ISA Server auch Content Management Systeme, Intrusion Detection Systeme (IDS) und Gateway basierte Virenscanner, welche sämtlichen Datenverkehr von **EXTERN** nach **INTERN** auf Virenbefall, schadhaften Code, ausführbaren Dateien uvm. durchsucht und basierend auf Ihrer festgelegten Policy verweigert, bzw. überprüft.
Es stehen eine Vielzahl von Third Party Produkten für den ISA Server 2004 zur Verfügung. Klicken Sie hier für eine Anbieter Übersicht.

Für weitergehende Informationen lesen Sie folgende Artikel:

Hardening the Windows Infrastructure on the ISA Server 2004 Computer
ISA Server 2004 Security Hardening Guide

Empfohlene Webseiten

www.microsoft.com/security - Microsoft Seiten rund um das Thema Sicherheit
www.microsoft.com/isaserver - Die ISA Server Webseiten
www.msisafaq.de - Selbstredend
www.isaserver.org - Die ISA Server Webseite von Dr. Tom Shinder
www.isatools.org - Eine Vielzahl von ISA Tools (auch zum Thema Sicherheit) von Jim Harrison

Stand: Donnerstag, 21. Oktober 2004/MG. http://www.it-training-grote.de