ISA Server 2004 – Firewall Client - Von Marc Grote

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

Einleitung

Dieser Artikel beschreibt die Funktionsweise des Microsoft ISA Server 2004 Firewall Client und dessen Konfiguration.

Ein Firewallclient im Microsoft Jargon ist ein Computer, auf dem die Firewallclientsoftware installiert und aktiviert ist. Auf dem Firewallclientcomputer wird eine Winsock-Anwendung ausgeführt, die den Microsoft-Firewalldienst von ISA Server 2004 verwendet. Für eine Übersicht über die unterstützten ISA Server 2004 Clienttypen, lesen Sie folgenden Artikel.

Wie funktioniert der Firewall Client

Beim Installieren eines Firewallclients auf dem Clientcomputer werden nicht die einzelnen Winsock-Anwendungen konfiguriert. Stattdessen wird ein gemeinsames Winsock genutzt, der auch von den anderen Anwendungen verwendet wird. Der Firewallclient fängt anschließend die Aufrufe der Anwendungen ab und ermittelt, ob die Anforderung an den ISA Server-Computer weitergeleitet wird.

Sie können festlegen, ob für das jeweilige Netzwerk (welches Sie am ISA Server konfiguriert haben) die Firewallclientunterstützung aktiviert werden soll. Bei aktivierter Firewallclientunterstützung nimmt der ISA Server 2004 eingehende Anforderungen an Port 1745 entgegen. Wenn ein Firewallclient über eine Winsock-Anwendung ein Objekt von einem Computer anfordert, überprüft der Client, ob der betreffende Computer als lokaler Computer eingestuft ist. Eine Adresse gilt als lokal, wenn sie im Adressbereich des jeweiligen Netzwerks enthalten ist.

Ist der anzurufende Server/Computer nicht lokal, wird die Anforderung an den Firewalldienst gesendet. Der Firewalldienst verarbeitet die Anforderung und leitet diese (basierend auf den Firewallrichtlinien) an das entsprechende Ziel weiter. Die Firewallclientsoftware kann, ebenfalls wie der Webproxy Client (allerdings nur für HTTP/HTTPS/FTP), Windows-Benutzerinformationen, die für Authentifizierungszwecke benötigt werden, an den ISA Server-Computer senden. Der FW-Client ist der einzige Client, welcher eine Benutzerauthentifizierung für jedes Protokoll unterstützt und ohne einen Anwendungsfilter komplexe Protokolle und sekundäre Verbindungen unterstützt.

Für eine wesentlich technischere Übersicht über den ISA Server Firewall Client, lesen Sie folgenden Artikel.

Was ist Winsock

Winsock ist die Kurzform für Windows Socket. Dabei handelt es sich um eine API (Application Programming Interface), die Windows-Programmen über das TCP/IP-Netzwerkprotokoll die Kommunikation mit anderen Computern ermöglicht.

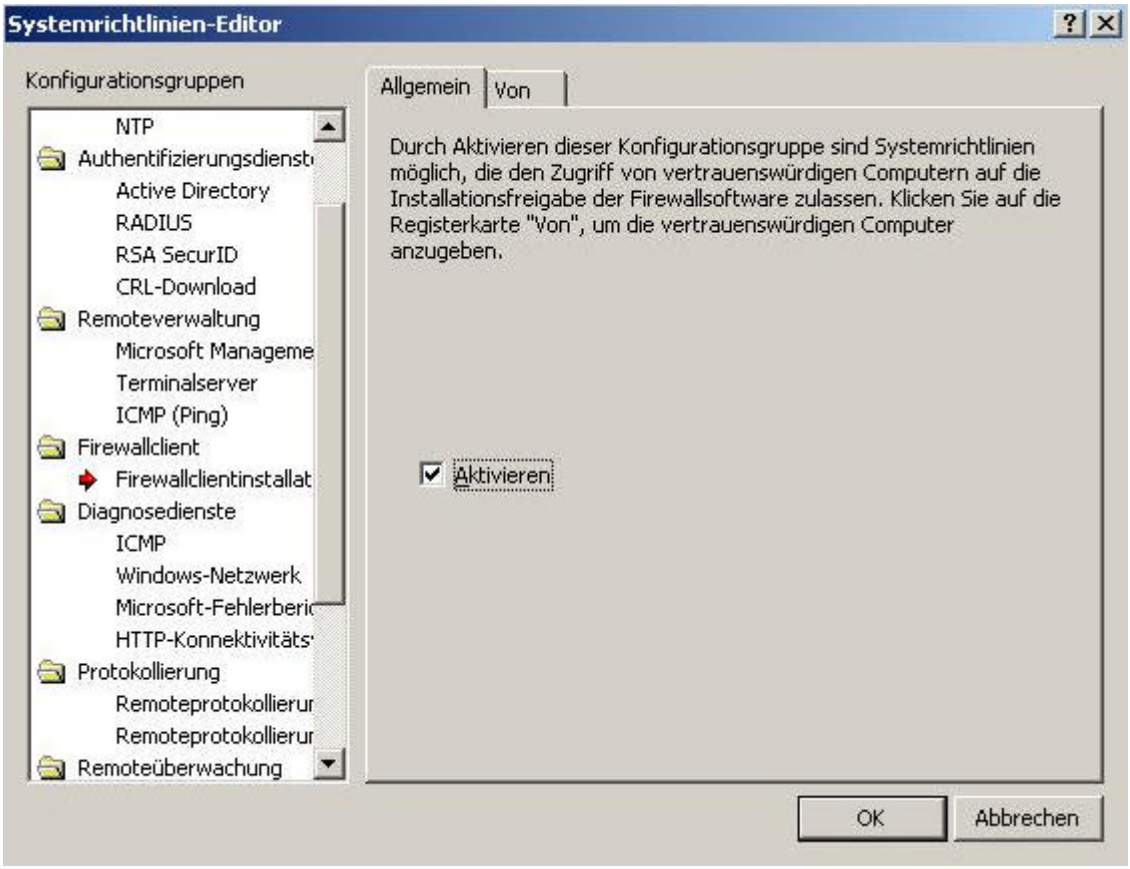
Allgemeines

Die ISA Server-Clientinstallationsdateien befinden sich normalerweise in einem Ordner auf dem ISA Server-Computer mit dem Freigabenamen **ISA_Servername/MSPClnt**. Das muss

seit ISA Server 2004 aber nicht mehr sein. Sie können die FW-Client Installationsfreigabe auch auf einem anderen Server zur Verfügung stellen.
Die Firewallclientsoftware darf **nicht** auf dem ISA Server-Computer installiert werden.
Bei der Installation wird die Firewallclientanwendung aktiviert.
Die Firewallclientsoftware kann auf Clientcomputern unter folgenden Betriebssystemen installiert werden:

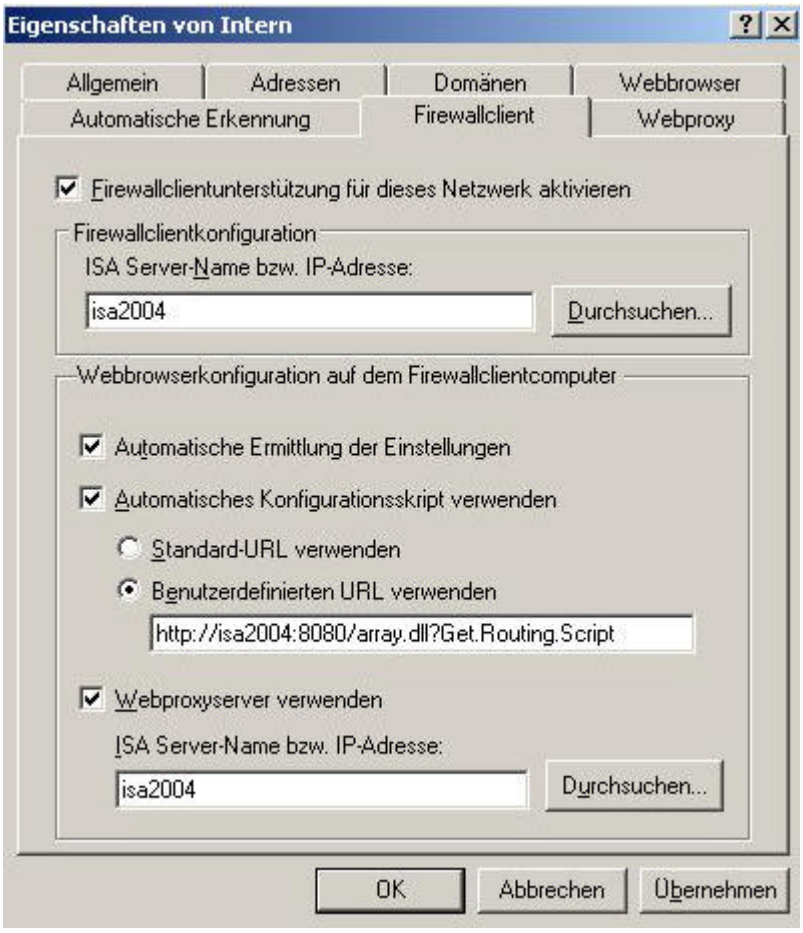
- Microsoft Windows Server 2003
- Windows 2000 Server
- Windows XP
- Windows Millennium Edition
- Windows NT 4.0.
- Windows 98 SE (wenn IE ab Version 5 installiert ist)

Clientcomputer können auf die Firewallclientfreigabe zugreifen, wenn die Systemrichtlinien-Konfiguration **Firewallclient** - **Firewallclientinstallation** für Firewallclient aktiviert ist.
Diese Konfiguration wird standardmäßig bei der Installation der Firewallclientfreigabe aktiviert.



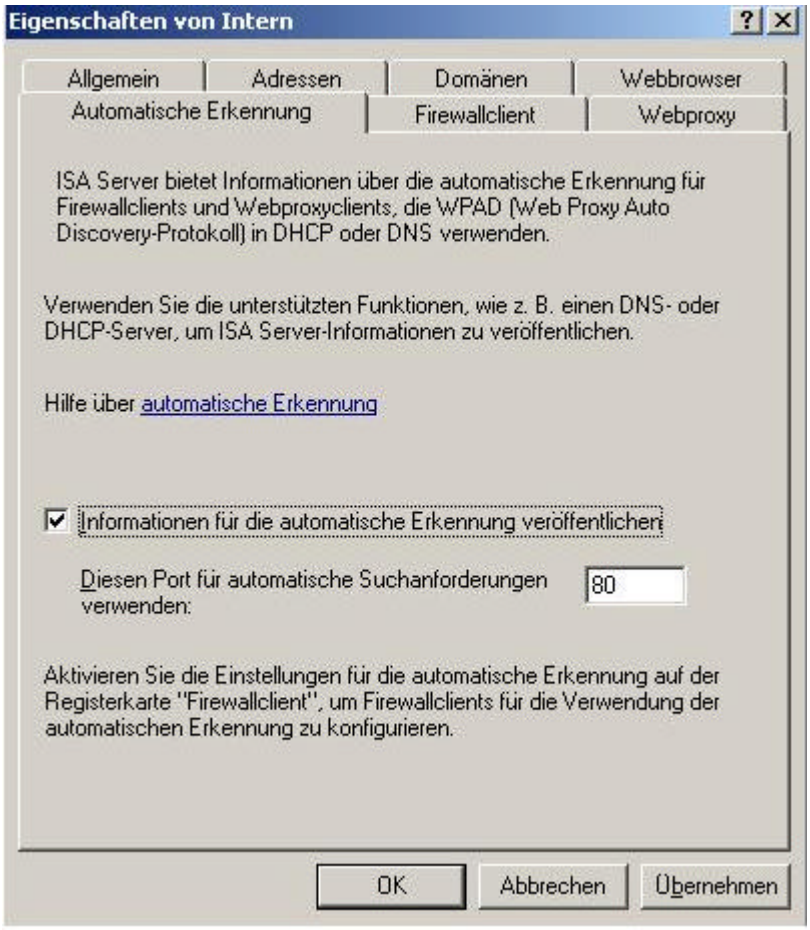
Aktivierung des Servers für die Firewall Client Verwendung

Starten Sie die ISA Server Verwaltungskonsole, navigieren Sie zu **Konfiguration** - **Netzwerke** - und dann in die Eigenschaften des Netzwerkobjektes **Intern** im Reiter **Netzwerke.** Klicken Sie dort den Reiter **Firewallclient** an und nehmen Sie die notwendigen Einstellungen vor.



Im Bereich **Webbrowserkonfiguration auf dem Firewallclientcomputer** können Sie ein **automatisches Konfigurationsskript** angeben. Hier ist die Angabe einer .INS Datei des IEAK (Internet Explorer Administration Kit) möglich, mit welchem weitere Einstellungen konfiguriert werden. Lesen Sie hier mehr zum IEAK.

Der ISA Server kann für die automatische Erkennung des ISA Servers für den Firewall- und Webproxy Client konfiguriert werden.



Für weitere Informationen rund um das Thema **Automatische Erkennung**, lesen Sie folgenden Artikel.

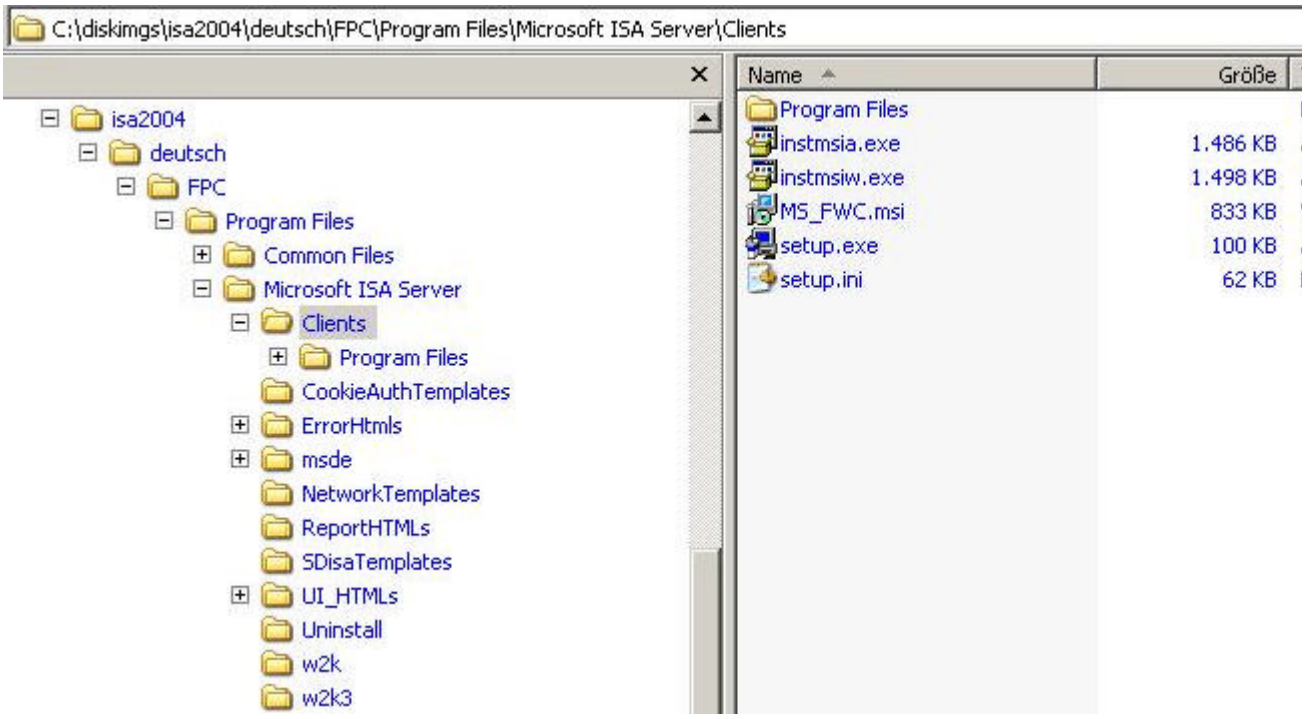
Firewall Client Installation

Der Firewall Client kann auf verschiedenen Arten installiert werden:

- Händische Installation
- Installation über die Softwareverteilungsfunktion der Gruppenrichtlinien von Windows 2000 / 2003
- Unbeaufsichtigte Installation über ein Skript

Händische Installation

Die händische Installation erfolgt durch manuelles Ausführen der FWC (Firewall Client) Setup-Routine (SETUP.EXE).



Folgen Sie den Anweisungen des Setup Wizards.

Der Firewall Client ist schnell installiert.

Angabe, ob der ISA Computer händisch eingetragen werden soll oder ob der ISA ´Server Computer automatisch ermittelt werden soll. Für die automatische Ermittlung sind zusätzliche Schritte erforderlich.

Installation über die Softwareverteilungsfunktion der Gruppenrichtlinien von Windows 2000 / 2003

Sie können den Firewall Client problemlos über die Softwareverteilungsfunktion der Gruppenrichtlinien von Windows 2000/2003 verteilen. Microsoft liefert für die Installation ein passendes MSI File mit. Kopieren Sie das Verzeichnis Clients von der ISA CD in die

Softwareverteilungsfreigabe. Für eine detaillierte Beschreibung der Softwareverteilung, lesen Sie den Artikel **Softwarezuweisung** unter **HowTo** auf der folgenden Webseite.

Unbeaufsichtigte Installation über ein Skript

So führen Sie eine unbeaufsichtigte Firewallclientinstallation durch:
Geben Sie an der Eingabeaufforderung auf dem Firewallclientcomputer folgendes ein:

Pfad\Setup /v"[SERVER_NAME_OR_IP=ISA_Servername] [ENABLE_AUTO_DETECT={1|0}] [REFRESH_WEB_PROXY={1|0}] /qn"

Erklärung:

Pfad steht für den Pfad zu den freigegebenen ISA Server-Clientinstallationsdateien. Diese Dateien befinden sich normalerweise auf dem ISA Server-Computer in einem Ordner mit dem Freigabenamen ISA\MSPclnt.
ISA_Servername steht für den Namen des ISA Server-Computers, zu dem der Firewallclient eine Verbindung herstellen soll.
Der Parameter **ENABLE_AUTO_DETECT=1** gibt an, dass der Firewallclient automatisch den ISA Server-Computer erkennt, über den Verbindungen hergestellt werden ist.
Der Parameter **REFRESH_WEB_PROXY=1** gibt an, dass die Firewallclientkonfiguration mit der Webproxykonfiguration aktualisiert werden soll, die auf dem ISA Server-Computer definiert wurde.

Unbeaufsichtigte Deinstallation

Um eine unbeaufsichtigte Deinstallation durchzuführen, geben Sie an einer Eingabeaufforderung folgendes ein:

MsiExec.exe /X {199B7F78-69B7-47C5-8D4B-A3ED1391FB6B} /qn

Um dieses Verfahren durchführen zu können, müssen Sie auf dem Clientcomputer Mitglied der Gruppe Administratoren sein.

Erweiterte Firewallclienteinstellungen

Nach der Installation übernimmt die Firewallclientsoftware die Einstellungen, die durch den ISA Server 2004-Computer konfiguriert wurden, von dem aus die Firewallclientanwendung installiert wurde. Durch diese Servereinstellungen werden unter anderem die **automatische Webproxykonfiguration**, der **ISA Server-Name**, die **automatische Erkennung von ISA Server** sowie andere Funktionen bestimmt.

Nachdem die Firewallclientsoftware installiert ist, aktualisiert der ISA Server 2004 diese Clienteinstellungen bei jedem Neustart eines Clientcomputers und alle sechs Stunden nach der ersten Aktualisierung.

Zusätzlich zu diesen Einstellungen aktualisiert ISA Server den FW-Client regelmäßig mit Informationen zu IP-Adressen, die der Client als lokale Adressen erkennen soll.

Für die meisten Winsock-Anwendungen funktioniert die Standardfirewall-Clientkonfiguration ohne jegliche zusätzliche Änderungen. In einigen Fällen müssen Sie jedoch Clientkonfigurationsinformationen hinzufügen (ein Beispiel hierfür ist Outlook). Der Firewallclient kann für jeden Benutzer und für jeden Computer lokal auf dem Firewallclientcomputer konfiguriert werden. Die Konfiguration erfolgt, indem Änderungen an

den INI-Dateien vorgenommen werden, die auf dem Firewallclientcomputer installiert sind.

Sie können die Standardeinstellungen für alle Komponenten nach der Installation ändern. Die neuen Konfigurationseinstellungen werden erst beim Aktualisieren der Clientkonfiguration wirksam.

INI-Dateien

Die Konfigurationsdaten werden in mehreren Dateien gespeichert, die auf dem Firewallclientcomputer installiert sind. Bei der Installation des Firewallclients auf dem Computer werden im einzelnen folgende Dateien auf dem Firewallclientcomputer installiert:

- Common.ini
- Management.ini
- Application.ini

Common.ini

In der Datei COMMON.INI werden allgemeine Konfigurationen für alle Anwendungen festgelegt.

Beispiel für den Inhalt dieser Datei

[Common]
ServerName=ISA2004 (gibt den ISA Server 2004 Computernamen an)
Disable=0 (gibt an, ob der ISA FW Client deaktiviert ist)
Autodetection=0 (gibt an, ob eine automatische Firewallerkennung aktiv ist)

Management.ini

Die Datei Management.ini werden die Konfigurationseinstellungen für die Firewallclientverwaltung festgelegt.

Beispiel für den Inhalt dieser Datei

[TrayIcon]
TrayIconVisualState=1 (gibt an, ob das ISA FW Client Symbol in der Taskleiste auftauchen soll)

Application.ini

Die Datei Application.ini enthält Konfigurationseinstellungen für bestimmte Anwendungen.

Beispiel für den Inhalt dieser Datei

[FW_Client_Proggi]
Disable=0
NameResolution=R
LocalBindTcpPorts=4711
LocalBindUdpPorts=4711-4723, 7400-7460
RemoteBindTcpPorts=32
RemoteBindUdpPorts=3200-3250
ServerBindTcpPorts=200-400
ProxyBindIp=80:192.168.1.23

Persistent=1
ForceCredentials=1
NameResolutionForLocalHost=L

Diese Dateien werden auf Betriebssystemebene für alle am Computer angemeldeten Benutzer erstellt und können für jeden einzelnen Benutzer auf dem Computer erstellt werden. Die Einstellungen für einzelne Benutzer haben Vorrang gegenüber den allgemeinen Konfigurationseinstellungen. Diese Dateien werden abhängig vom Betriebssystem an verschiedenen Speicherorten erstellt. Bei Windows XP werden die Dateien in zwei Ordner kopiert:

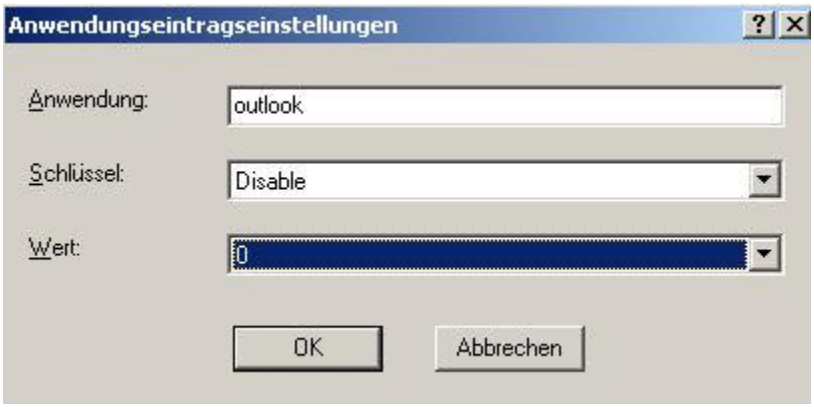
\Dokumente und Einstellungen\All Users\\Lokale Einstellungen\Anwendungsdaten\Microsoft\Firewall Client 2004
\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Anwendungsdaten\Microsoft\Firewall Client 2004

Einstellungen in der Datei Application.ini können auch zentral am ISA Server vorgenommen werden und gelten dann für alle FW-Clients.

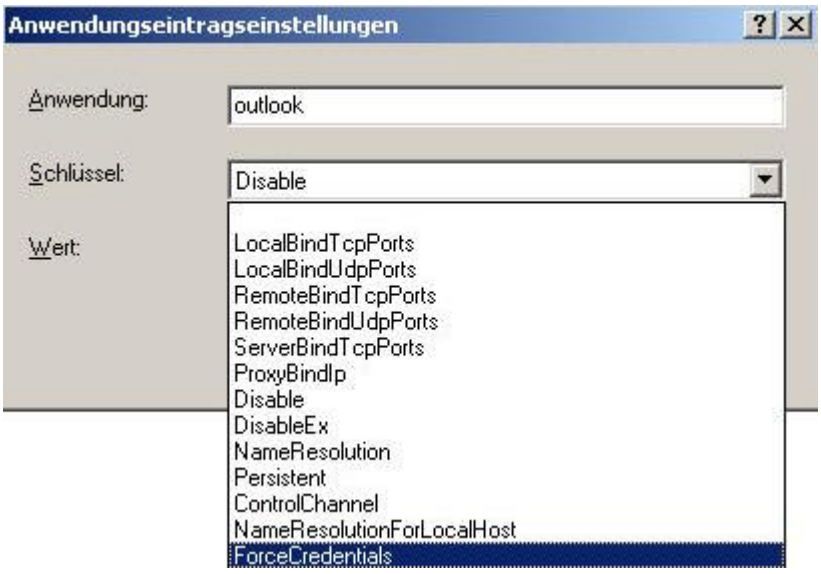
Starten Sie dazu die ISA Server Verwaltungskonsole und navigieren Sie zu **Konfiguration** - **Allgemein** - **Firewallclienteinstellungen definieren** und dann in den Reiter **Anwendungseinstellungen.**

Beispiel Outlook

In der deutschen ISA Newsgroup gibt es häufiger Aússagen, dass Outlook bei aktiviertem Firewall Client nicht richtig funktioniert. Schuld ist hier die Standard Einstellung des ISA Servers für den FW Client, Outlook für die Verwendung über die Firewall zu deaktivieren. Die Anwendung **outlook** hat per Default einen Schlüssel **Disable** dessen Wert auf **1** gesetzt ist. Damit Outlook über den ISA Server funktioniert, setzen Sie den Wert auf **0**.



Weitere Anwendungseintragseinstellungen sind:



Beschreibung der Einstellungen (aufbereitet aus der ISA Server Onlinehilfe)

Eintrag	Beschreibung
ServerName	Gibt den Namen des ISA Server-Computers an, zu dem der Firewallclient eine Verbindung herstellen soll
Disable	Mögliche Werte: 0 oder 1. Ist der Wert auf 1 eingestellt, wird die Firewallclientanwendung für die betreffende Clientanwendung deaktiviert
DisableEx	Werte: 0 oder 1. Ist der Wert auf 1 eingestellt, wird die Firewallclientanwendung für die betreffende Clientanwendung deaktiviert. Dies betrifft ausschließlich den Firewallclient für ISA Server 2004. Wenn diese Option aktiviert ist, wird die Einstellung Disable außer Kraft gesetzt
NameResolution	Mögliche Werte: "L" oder "R". Standardmäßig werden Domänennamen in dezimaler, durch Punkte getrennter Schreibweise bzw. Internetdomänennamen zur Namensauflösung an den ISA Server-Computer umgeleitet. Alle anderen Namen werden auf dem lokalen Computer aufgelöst. Ist dieser Wert auf "R" eingestellt, werden alle Namen zur Auflösung an den ISA Server-Computer umgeleitet ("Redirection"). Ist dieser Wert auf L eingestellt, werden alle Namen auf dem lokalen Computer aufgelöst ("Local")
LocalBindTcpPorts	Gibt einen TCP-Port (Transmission Control Protocol), eine TCP-

	Liste oder einen TCP-Bereich mit lokaler Bindung an
LocalBindUdpPorts	Gibt einen UDP-Port (User Datagram Protocol), eine UDP-Liste oder einen UDP-Bereich mit lokaler Bindung an
RemoteBindTcpPorts	Gibt einen TCP-Port, eine TCP-Liste oder einen TCP-Bereich mit Remotebindung an
RemoteBindUdpPorts	Gibt einen UDP-Port, eine UDP--Liste oder einen UDP-Bereich mit Remotebindung an
ServerBindTcpPorts	Gibt einen TCP-Port, eine TCP-Liste oder einen TCP-Bereich für alle Ports an, die mehr als eine Verbindung annehmen sollen
Persistent	Mögliche Werte: 0 oder 1. Ist dieser Wert auf 1 eingestellt, kann ein bestimmter Serverstatus auf dem ISA Server-Computer aufrecht erhalten werden, wenn ein Dienst beendet und neu gestartet wird und der Server nicht antwortet. Der Client sendet während einer aktiven Sitzung regelmäßig eine Keep-Alive-Meldung an den Server. Antwortet der Server nicht, versucht der Client beim Neustart des Servers, den Status der gebundenen und abhörenden Sockets wieder herzustellen
ForceCredentials	(Kann nur am Firewallclientcomputer eingestellt werden.) Wird verwendet, wenn ein Windows-Dienst oder eine Windows-Serveranwendung als Firewallclientanwendung ausgeführt wird. Ist dieser Wert auf 1 eingestellt, wird die Verwendung anderer Anmeldeinformationen für die Benutzerauthentifizierung erzwungen. Diese Informationen sind lokal auf dem Computer gespeichert, auf dem der Dienst ausgeführt wird. Die Benutzeranmeldeinformationen werden auf dem Clientcomputer mit der Anwendung Credtool.exe gespeichert, die zum Lieferumfang der Firewallclientsoftware gehört. Die Benutzeranmeldeinformationen müssen auf ein Benutzerkonto verweisen, das von ISA Server authentifiziert werden kann. Dieses Konto kann sich auf dem ISA Server-Computer oder einer für ISA Server vertrauenswürdigen Domäne befinden. Das Benutzerkonto ist normalerweise so eingestellt, dass es nicht abläuft. Andernfalls müssen die Benutzerinformationen jeweils vor Ablauf des Kontos erneuert werden
NameResolution ForLocalHost	Mögliche Werte sind "L" (Standardeinstellung), "P" oder "E". Gibt an, wie der lokale Computername (Client) beim Aufruf der API gethostbyname aufgelöst wird. Der Computername LocalHost wird durch Aufruf der Winsock-API-Funktion gethostbyname() unter Verwendung der Zeichenfolge LocalHost, einer leeren Zeichenfolge oder eines NULL-Zeichenfolgenzeigers aufgelöst. Winsock-Anwendungen rufen gethostbyname(LocalHost) auf, um ihre lokale IP-Adresse zu suchen und an einen Internetserver zu senden. Ist die Option auf "L" eingestellt, gibt gethostbyname() die IP-Adressen des lokalen Hostcomputers zurück. Ist die Option auf "P" eingestellt, gibt gethostbyname() die IP-Adressen des ISA Server-Computers zurück. Ist die Option auf "E" eingestellt, gibt gethostbyname() nur die externen IP-Adressen des ISA Server-Computers zurück – die IP-Adressen, die sich nicht in der lokalen Adresstabelle befinden
ControlChannel	Mögliche Werte: "Wsp.udp" oder "Wsp.tcp" (Standardeinstellung). Gibt den Wert des verwendeten Steuerkanals an
EnableRouteMode	Mögliche Werte sind 0 und 1 (Standardeinstellung). Wenn

	EnableRouteMode auf 1 eingestellt und ein Routeverhältnis zwischen dem Firewallclientcomputer und dem angeforderten Ziel eingerichtet ist, wird die IP-Adresse des Firewallclients als Quelladresse verwendet. Ist dieser Wert auf 0 eingestellt, wird die IP-Adresse des ISA Server-Computers verwendet. Dieses Flag wird von älteren Versionen des Firewallclients nicht unterstützt

Reihenfolge der Anwendung der Einstellungen

Die INI-Dateien im Ordner des Benutzers haben Vorrang.
Als Nächstes überprüft der Firewallclient den Inhalt des Ordners All Users. Alle weiteren Konfigurationseinstellungen werden ggf. übernommen. Falls eine festgelegte Konfigurationseinstellung zu den entsprechenden benutzerspezifischen Einstellungen im Widerspruch steht, wird sie ignoriert.
Die Firewallclientanwendung erkennt den ISA Server-Computer, mit dem eine Verbindung hergestellt werden soll, entsprechend den in der Firewallclientverwaltung festgelegten Einstellungen.
Schließlich untersucht der Firewallclient die Einstellungen auf Serverebene. Alle für ISA Server festgelegten Konfigurationseinstellungen werden übernommen. Falls eine festgelegte Konfigurationseinstellung zu den entsprechenden benutzer- oder computerspezifischen Einstellungen im Widerspruch steht, wird sie ignoriert.

Lokale Adressen des Firewallclients

Standardmäßig betrachtet der Firewallclient alle Adressen im Netzwerk, für die dieser Client konfiguriert ist, sowie die in der lokalen Routingtabelle auf dem Firewallclientcomputer angegebenen Adressen als lokale Adressen. Wenn beispielsweise der Firewallclient eine Verbindung zum Netzwerkadapter für das interne Netzwerk herstellt, werden alle im internen Netzwerk konfigurierten IP-Adressen als lokal angesehen. Bei jedem Versuch einer Winsock-Anwendung auf dem betreffenden Client, eine Verbindung zu einer IP-Adresse herzustellen, wird anhand der Datei **Locallat.txt** bestimmt, ob es sich bei der IP-Adresse um eine Adresse im internen Netzwerk handelt. Falls die Adresse als lokale Adresse angesehen wird, kommt es zu einer direkten Verbindungsherstellung. Wenn die Adresse nicht als lokale Adresse gilt, wird die Verbindung über den Microsoft-Firewalldienst auf ISA Server hergestellt.

LAT - Da ist sie wieder (aber nur auf der Clientseite)

Eine lokale Version dieser Informationen kann ebenfalls erstellt werden. Sie können mit Notepad eine benutzerdefinierte Datei für die lokale Adresstabelle (LAT) eines Clients unter dem Namen **Locallat.txt** erstellen und im Ordner \Dokumente und Einstellungen\All Users\Lokale Einstellungen\Anwendungsdaten\Microsoft\Firewall Client 2004 auf dem Firewallclientcomputer speichern. Sie können weitere IP-Adressbereiche hinzufügen, die der Client als Bestandteil des lokalen Netzwerks erkennt. Der Client bestimmt anhand der eigenen **Routingtabelle**, der **serverspezifischen Einstellungen** und der Datei **Locallat.txt,** welche IP-Adressen zum lokalen Netzwerk gehören.

Beim Erstellen der Datei **Locallat.txt** geben Sie die IP-Adresspaare in die Datei ein. Jedes Adresspaar definiert entweder einen IP-Adressbereich oder eine einzelne IP-Adresse. Das folgende Beispiel zeigt eine Datei **Locallat.txt** mit zwei Einträgen. Der erste Eintrag ist ein IP-Adressbereich und der zweite eine einzelne IP-Adresse.

192.168.1.0 192.168.1.255 - gibt einen Netzwerkbereich an

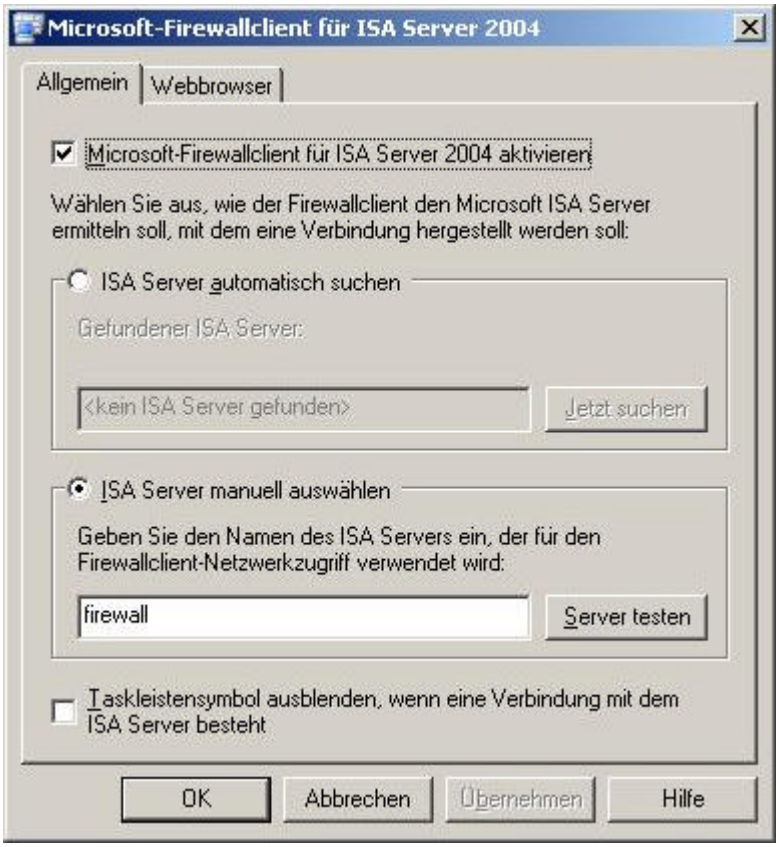
192.168.1.18 192.168.1.18 - gibt eine IP-Adresse an.

Firewall Clienteinstellungen

Nach erfolgter Firewallclient-Installation, können Sie die Einstellungen des Firewall Clients modifizieren.

Klicken Sie dazu doppelt auf das ISA Icon im Tray.

Eine Übersicht über sämtliche FW-Clientkonfigurationseinstellungen finden Sie in der Datei C:\Programme\Microsoft Firewall Client 2004\ISAClient.htm



Wenn Sie verhindern wollen, dass Benutzer den Firewall Client deaktivieren, entfernen Sie sämtliche Benutzerberechtigungen auf die Datei COMMON.INI und geben Sie dem Benutzer statt dessen nur Leseberechtigungen auf die Datei, damit der Benutzer die Konfiguration lesen kann (System und Administratoren sollten natürlich weiterhin Vollzugriff haben.

Im Reiter **Webbrowser** können Sie festlegen, dass der Webbrowser auf dem Clientcomputer automatisch so konfiguriert wird, dass er als Proxyserver den auf der Seite **Allgemein** angegebenen ISA Server-Computer verwendet.

Verschlüsselte Firewallclientverbindungen

Der ISA Server 2004 FW-Client bietet die Möglichkeit, den Datenverkehr zwischen dem Firewallclient und dem ISA Server zu verschlüsseln. Verwenden Sie frühere Versionen der Firewallclientsoftware, so können diese FW-Clients eine Verbindung zum ISA Server 2004 aufbauen wenn Sie in der ISA Verwaltungskonsole den Haken bei **Unverschlüsselte Firewallverbindungen zulassen** setzen. Nach Aktivierung dieser Funktion erfolgt die Kommunikation zwischen FW-Client und ISA Server unverschlüsselt.

Stand: 21.12.2004/MG. http://www.it-training-grote.de