SA Server 2004 – IP-Einstellungen definieren - Von Marc Grote

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

Einleitung

SA Server 2004 bietet die Option zur Konfiguration von IP-Einstellungen, um die Sicherheit des Systems zu erhöhen und die Performance zu erhöhen. Befolgen Sie bei der Konfiguration den Hinweisen in diesem Artikel.

***N*ichtiger Hinweis:**

Ändern Sie diese Konfigurationsparameter nur, wenn Sie sich über die Auswirkungen im klaren sind. Das Filtern von IP-Optionen und die Änderung der Paketfragementierungsbehandlung kann bei unsachgemäßer Anwendung zu diversen Problemen führen.

Zur Konfiguration der IP-Einstellungen starten Sie die ISA Server 2004 Verwaltungskonsole, gehen zum Container ***Konfiguration*** und dort zum Container ***Allgemein***. Klicken Sie hier auf ***IP-Einstellungen definieren***.

Sie können drei verschiedene IP-Einstellungen vornehmen:

- IP-Optionen
- IP-Fragmente
- IP-Routing

P-Optionen

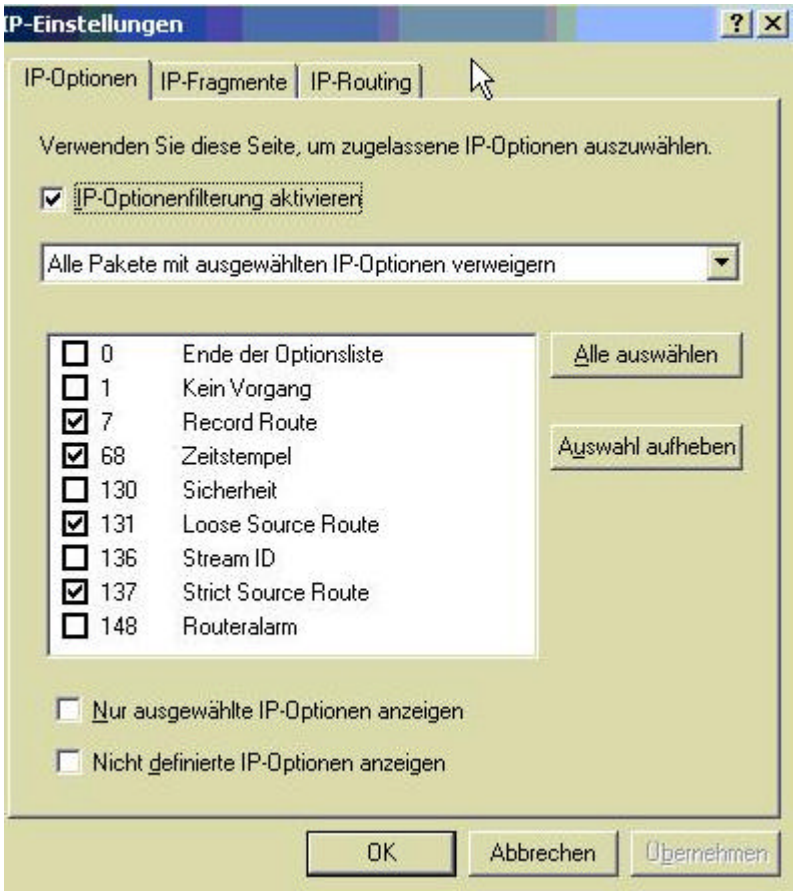
Bei den IP-Optionen handelt es sich um einen speziellen Bereich im IP-Header mit dem Namen IP-

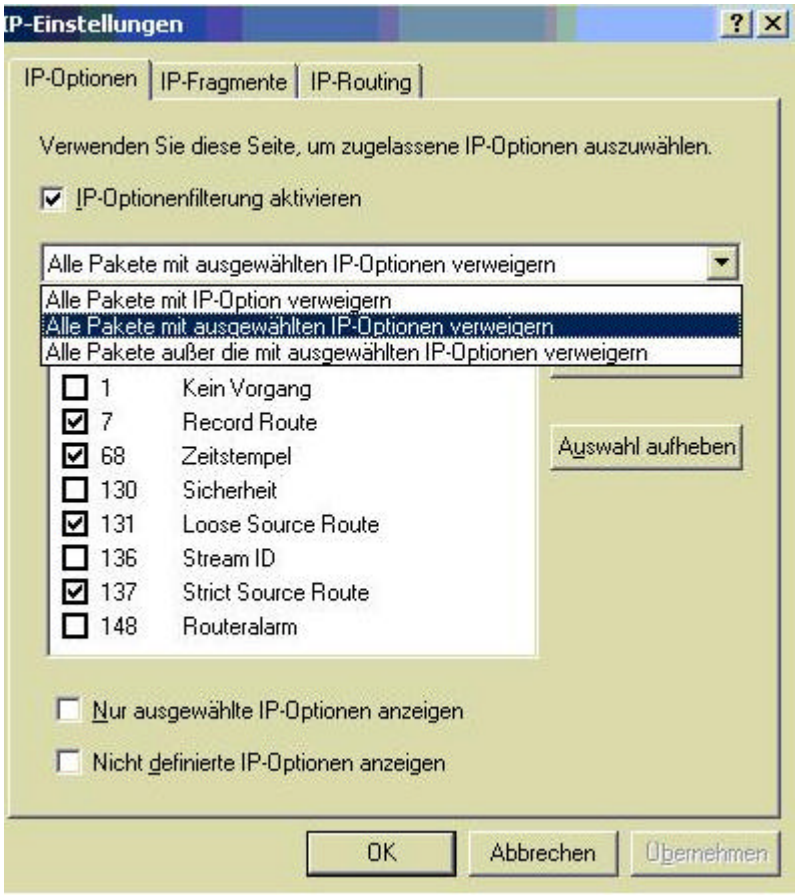
Options.
P-Optionen definieren zusätzliche Möglichkeiten des IP-Protokolls wie z. B. eine der bekanntesten: IP-Option 9 - Strict Source Route. Es gibt die Möglichkeit 256 IP-Optionen zu konfigurieren (0-255). IP-Optionen sind IPv4 spezifisch. Das IPv6 Protokoll wird keine IP-Optionen mehr im IP-Header enthalten.

SA Server 2004 blockiert einige IP-Optionen weil diese für Angriffe durch Hacker genutzt werden können. Nehmen wir als Beispiel noch mal die IP-Option 9: Die einfachste Routing – Attacke benutzt die nternet – Protokolloption 9 bzw. 3. In beiden Fällen kann die Route durch das Netzwerk vom Sender des P-Paketes bestimmt werden. Bei Verwendung von "Strict Source Routing" muss dabei jeder Vermittlungsknoten in der richtigen Reihenfolge angegeben werden. Im Gegensatz zu "Loose Source Routing" welches auch zusätzliche Hops zwischen zwei angegebenen IP – Adressknoten zulässt. Der Datenstrom der Zielstation kann damit problemlos an das Computersystem des Eindringlings "umgeleitet" werden. Dazu simuliert der Angreifer wiederum die IP-Adresse eines internen Systems (IP – Adress – Spoofing) und öffnet unter Aktivierung der Option "Loose Source Routing" eine Verbindung zur Zielstation, wobei als Route für die Antwortpakete ein Pfad, der über das angreifende System führt, angegeben wird. Damit stehen dem Eindringling alle Möglichkeiten der simulierten, internen Station zur Verfügung.

m ISA Server 2004 wird Strict Source Route als IP Option 137 und Loose Source Route als IP Option 131 dargestellt.

Für die Standardinstallationen können Sie die IP-Optionen aktiviert lassen und müssen keine zusätzlichen P-Optionen aktivieren. Aktivieren Sie eine zusätzliche IP-Optionenfilterung nur, wenn Sie deren Bedeutung vollständig verstehen.





Sie haben die Möglichkeit ...

- alle Pakete mit IP-Option zu verweigern
- alle Pakete mit ausgewählten IP-Optionen zu verweigern
- alle Pakete außer die mit ausgewählten IP-Optionen zu verweigern.

Die Default Einstellung ist die Verweigerung aller Pakete mit den ausgewählten IP-Optionen.

Wenn Sie auf ***Nicht definierte IP-Opionen anzeigen*** klicken, werden Ihnen alle IP-Optionsfelder angezeigt.

IP-Fragmente

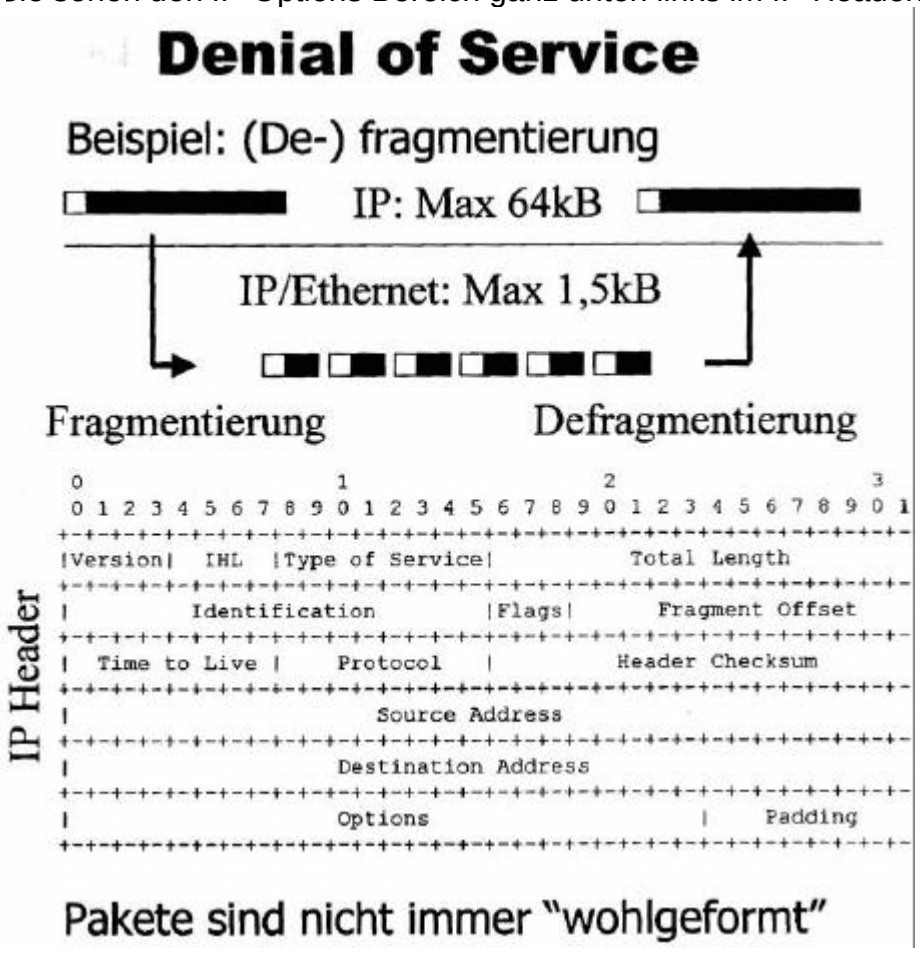
In den unterschiedlichsten Netzwerktypen ist die Länge der übertragenen IP-Pakete immer eingeschränkt und von Netzwerktyp zu Netzwerktyp unterschiedlich. Abhängig von dem verwendeten Netz wird die maximale Größe der IP-Pakete als Maximum Transfer Unit (MTU) in Oktetten (Bytes) angegeben. Beispiele für MTU Werte:

Netzwerktyp	IP-Paket
X.25	576 Byte
IEEE 802.3	1492 Byte
Ethernet	1500 Byte
Token Ring (16)	17914 Byte
min. MTU IPv4	68 Byte
min. MTU IPv6	1280 Byte

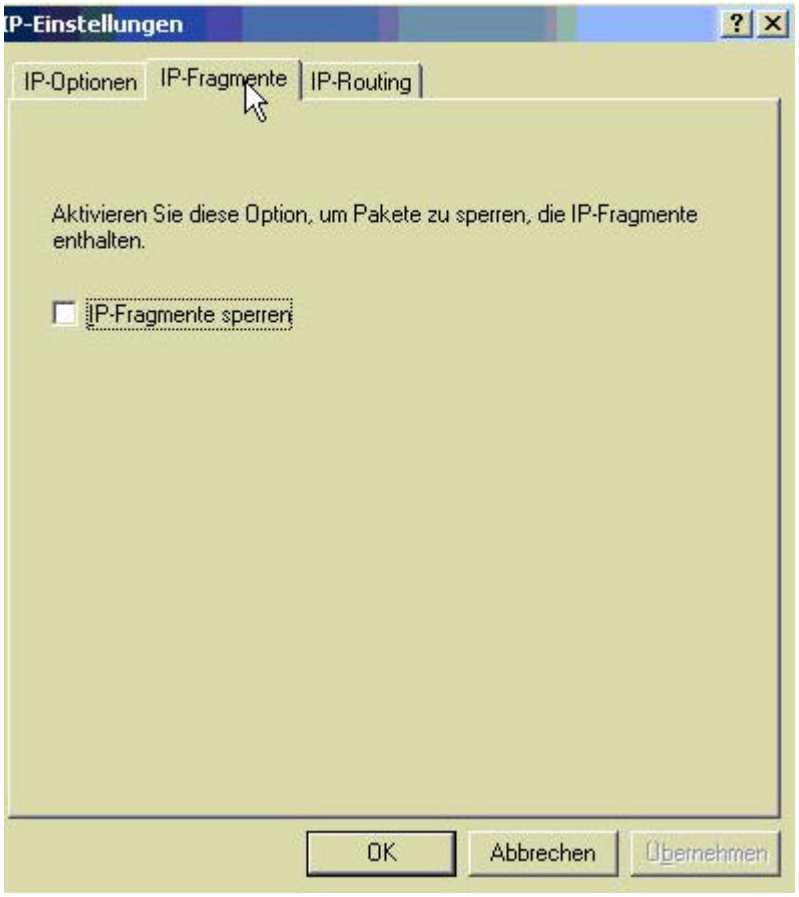
Zur Anpassung der übertragenen IP-Pakete an unterschiedliche MTU-Werte ist das IP-Protokoll in der Lage, Pakete entsprechend den MTU-Werten der einzelnen Netze zu fragmentieren, dass heisst, große IP-Pakete auf eine Reihe von kleineren IP-Teilpaketen (IP-Fragmenten) aufzuteilen. Ein Quellrechner

kann auch verbieten, dass ein IP-Paket fragmentiert werden darf. Hierfür muss der Quellrechner/Router das Bit **DF** (don´t fragment) im Feld Flags des IP-Headers auf 1 setzen. Die Größe des IP-Pakets liegt bei 576 bis 65 536 Oktetten. Wenn man die minimale Länge von 20 Oktetten des IP-Headers berücksichtigt, bleiben für die weiteren Daten und den TCP-Header noch 65 516 Oktette. Die minimale Größe von 576 Oktetts muss von jeder IP-Implementierung unterstützt werden.

Die nächste Grafik zeigt schematisch den Aufbau des IP-Headers und den Prozess der Fragmentierung. Sie sehen den IP-Options Bereich ganz unten links im IP-Header.



ISA Server 2004 deaktiviert das Blocken von IP-Fragementen per Default, weil ein aktviertes Blocken von IP-Fragmenten auch zu unerwünschten Nebeneffekten führen kann, dass zum Beispiel VPN und IPSEC Verbindungen Probleme bereiten, da ja hier bewusst IP-Pakete durch Kapselung vor Veränderung geschützt werden. IP-Fragmente können aber auch die Sicherheit des Systems gefährden. Ein Beispiel für einen Sabotageangriff ist der Ping-of-Death, bei dem ein synthetisches, unzulässig großes IP-Paket (>65535 Bytes) in fragmentierter Form übertragen wird. Das angegriffene System stürzt bei dem Versuch ab, die Fragmente wieder zusammenzufügen. Das ist sicherlich kein aktuelles Beispiel, weil alle aktuellen Firewallsysteme in der heutigen Zeit gegen den Ping of Death gefeit sind, (auch der ISA Server hat einen IDS gegen Ping of Death (lizenziert von ISS)) soll aber als Beispiel ausreichend sein.



P-Routing

Wenn IP-Routing aktiviert ist, sendet ISA Server das ursprüngliche Netzwerkpaket zum Ziel. Durch IP-Routing wird zwar der Durchsatz verbessert, aus Sicherheitsgründen wird jedoch empfohlen, diese Funktion zu deaktivieren. Wenn IP-Routing deaktiviert ist, sendet ISA Server nur die Daten (nicht das gesamte Paket) zum Ziel.
ISA Server 2004 verwaltet sekundäre NAT Verbindungen von komplexen Protokollen (z. B. FTP) direkt im Kernel Mode, welches den Durchsatz für Protokolle mit sekundären Protokollen erheblich beschleunigen kann. Sekundäre Verbindungen für Secure NAT Clients werden allerdings nur unterstützt wenn ein Applikations-Filter für das Protokoll auf dem ISA Server 2004 installiert ist. Sie müssen also hier eine Entscheidung zu Gunsten der Performance (aktiviertes IP-Routing) oder zu Gunsten der Sicherheit (deaktiviertes IP-Routing) treffen. Aufgrund der Tatsache, dass IP Routing per Default aktiv ist und auch andere Firewallimplementationen per Default IP Routing aktivieren, können Sie diese Einstellung unverändert lassen.


IP-Einstellungen
IP-Optionen
IP-Fragmente
IP-Routing
IP-Routing ermöglicht dem ISA Server das Weiterleiten von IP-Paketen im Kernelmodus und verbessert die Leistung.
IP-Routing aktivieren
OK
Abbrechen
Übernehmen