Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Einleitung

Der ISA 2004 bietet als erste Firewall Lösung von Microsoft die Möglichkeit, eine Benutzer Authentifizierung für das Regelwerk über eine RADIUS (Remote Access Dial In Service) Verbindung einzurichten.

Die Microsoft Implementierung von RADIUS nennt sich IAS (Internet Authentication Service) und steht unter Windows 2000 und 2003 für alle Windows Versionen (Ausnahme Windows 2003 Web Editon), zur Verfügung.

Nachteile der IAS Authentifizierung mit dem ISA Server 2004

- RADIUS Traffic ist per Default unverschlüsselt. Die Verwendung von IPSEC wird empfohlen
- Bei jedem matchen der Regel muss RADIUS den Client reauthentifizieren, was bei ausgelasteten Servern mehr Netzwerk- und Verarbeitungslast erzeugt.
- ISA enthält nicht sehr viele Informationen im RADIUS Acces-Request Paket, so dass eine Unterscheidung zwischen ISA und anderen Diensten sehr schwer ist, wenn alle auf derselben Maschine laufen.

Hinweis:

Webbowser verstehen kein RADIUS als Authentifizierungstyp, so dass der ISA Server 2004 den Clint auffordert sich per Basic Authentication zu identifizieren. ISA packt diese Pakete in ein RADIUS Access Request Paket und sendet diese zum ausgewählten RADIUS Server.

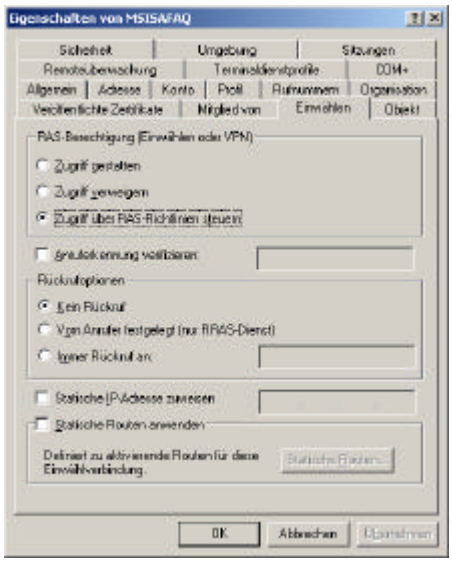
Warum RADIUS/IAS

Ein ISA 2004 Server befindet sich in der Regel in einer DMZ (DeMilitarisierten Zone). Dabei handelt es sich um einen Hochsicherheitsbereich welcher nur die notwendigsten Verbindungen zwischen LAN und WAN (Internet etc.) herstellen soll.

Aus diesem Grund implementiert man einen ISA Server 2004 als Firewall Lösung nicht in das interne Netzwerk – sprich, der ISA Server 2004 wird **KEIN** Mitglied der Domäne. Eine Ausnahme von der Regel ist ein ISA 2004 Server als reine Proxy Lösung. Dort befindet sich der ISA Server 2004 hinter einer anderen ISA 2004 Firewall oder Third Party Firewall und kann so Mitglied der Domäne sein, um z. B. über die integrierte Windows Authentifizierung ein Regelwerk für den Webzugriff abzubilden.

Die Benutzerseite

Stellen Sie sicher, dass die Benutzer eine RAS Einwahlberechtigung haben. Es handelt sich hierbei zwar um keine RAS Einwahl, aber mit diesem Schalter teilen Sie mit, dass jetzt RAS Richtlinien und IAS Richtlinien verwendet werden können, welche ja für den ISA Server 2004 Zugriff über RADIUS erforderlich sind.

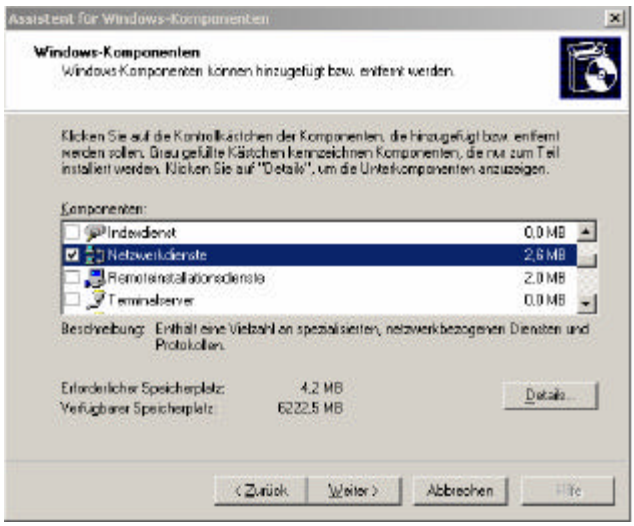


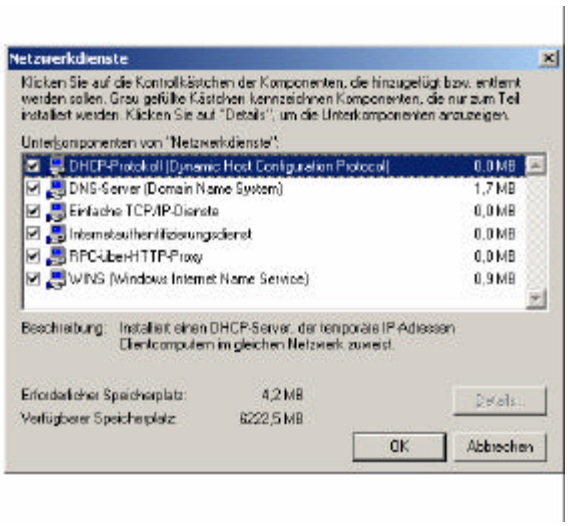
Müssen Sie mehreren Benutzern den Zugriff auf Dienste über den ISA ermöglichen, so empfiehlt sich das Anlegen einer Benutzergruppe um dieser die entsprechenden Berechtigungen zu vergeben und die entsprechenden Benutzer zum Mitglied dieser Gruppe zu machen.

In unserem Beispiel verwenden wir die Gruppe *WWW-Benutzer*.

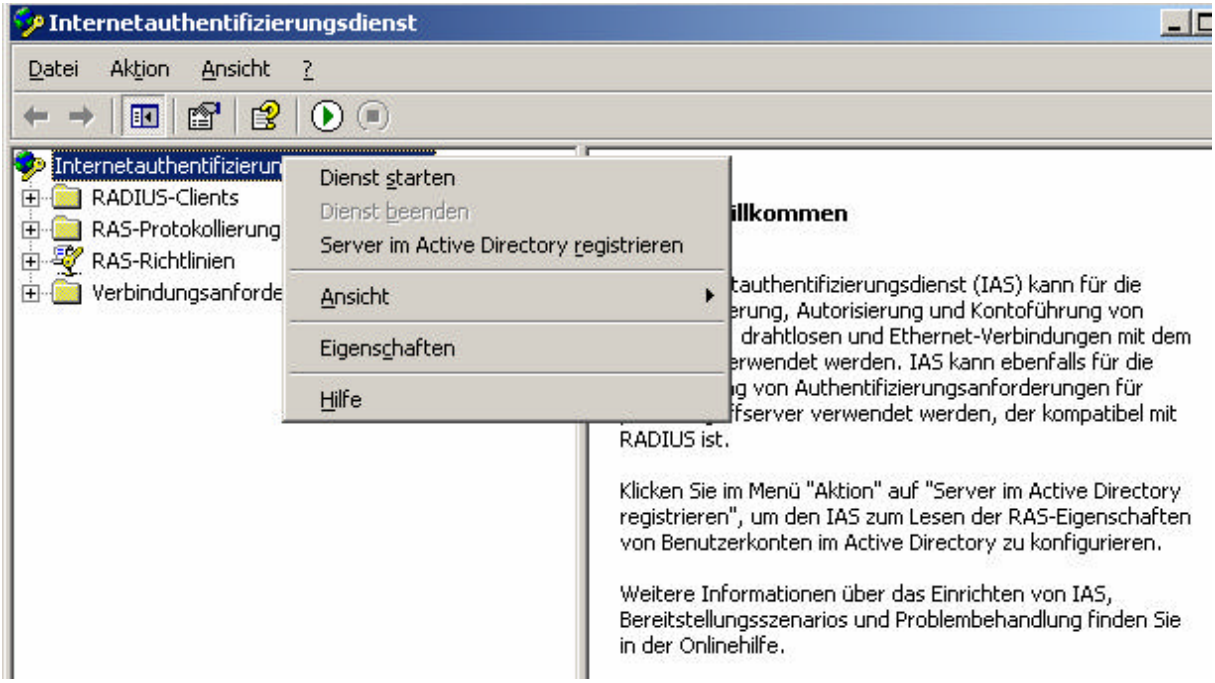
Installation der IAS Servers

Sie installieren den IAS Server wie jede Microsoft Komponente über Start – Systemsteuerung – Software – Windows Komponenten Hinzufügen / Entfernen.
Gehen Sie dann in Netzwerkdienste und wählen dort *Internetauthentifizierungsdienst* aus.



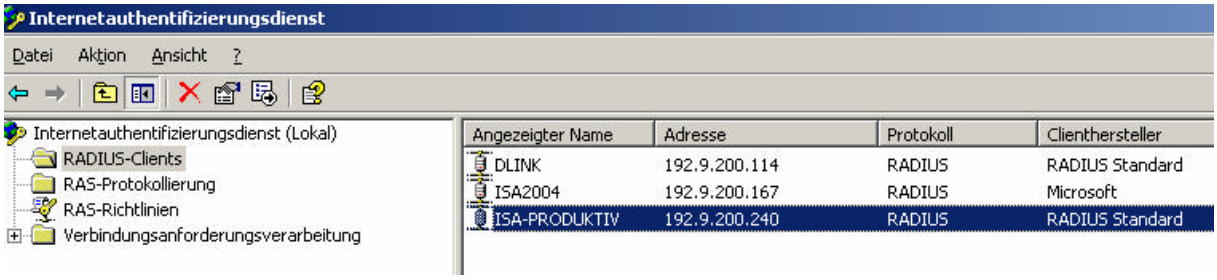


Nach erfolgter Installation des IAS müssen Sie diesen *Server im Active Directory registrieren*, damit der IAS berechtigt ist, Kontenanfragen über LDAP an das Active Directory zu richten.
Klicken Sie dazu in der IAS Konsole mit der rechten Maustaste auf *Internetauthentifizierungsdienst* und wählen im Kontextmenü *Server im Active Directory registrieren* aus.

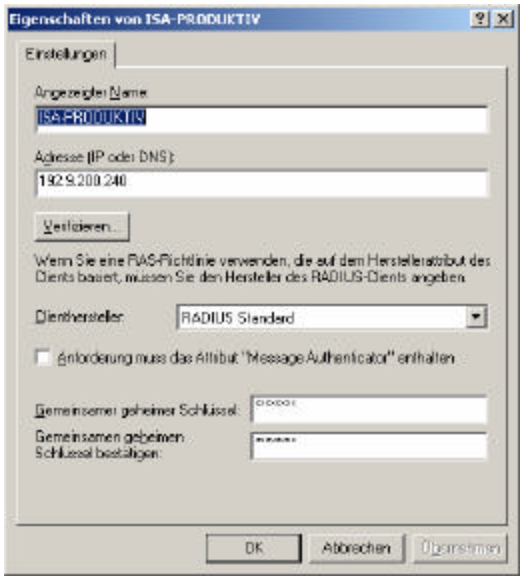


Erstellen des ISA 2004 Servers als IAS Client

Damit der ISA Server 2004 eine Benutzerauthentifizierung über RADIUS nutzen kann, müssen Sie den ISA Server als RADIUS Client einrichten. Hierzu sind zwei Schritte erforderlich. Der erste Schritt ist es im IAS einen neuen RADIUS Client zu erstellen.
Klicken Sie dazu mit de rechten Maustaste in den Container *RADIUS-Client* und fügen einen neuen Client hinzu.



Sie müssen einen Namen für den neuen RADIUS Client angeben. Das muss nicht zwingend der NetBIOS / DNS Name des Clients sein, es handelt sich hierbei nur um den angezeigten Namen.
Als nächstes müssen Sie die IP Adresse oder den DNS Namen des RADIUS Client angeben und den Clienthersteller auswählen. Wir wählen als Clienthersteller *RADIUS Standard*.



Ein sehr wichtiger Punkt ist das so genannte *Shared Secret* – beim IAS *Gemeinsam geheimer Schlüssel* genannt.

Hier bei handelt es sich um eine Methode der Authentifizierung zwischen ISA Server und IAS Client. Ist der gemeinsam geheime Schlüssel identisch, erfolgt eine Kommunikation zwischen Server und Client.

Es wird die Verwendung eines sehr langen und kryptischen Schlüssels empfohlen. Die Qualität steht und fällt mit der Länge und Komplexität des Schlüssels. Ein brauchbarer Schlüssel wäre zum Beispiel: Xd5$1“xSS(&aäsD03?Q.

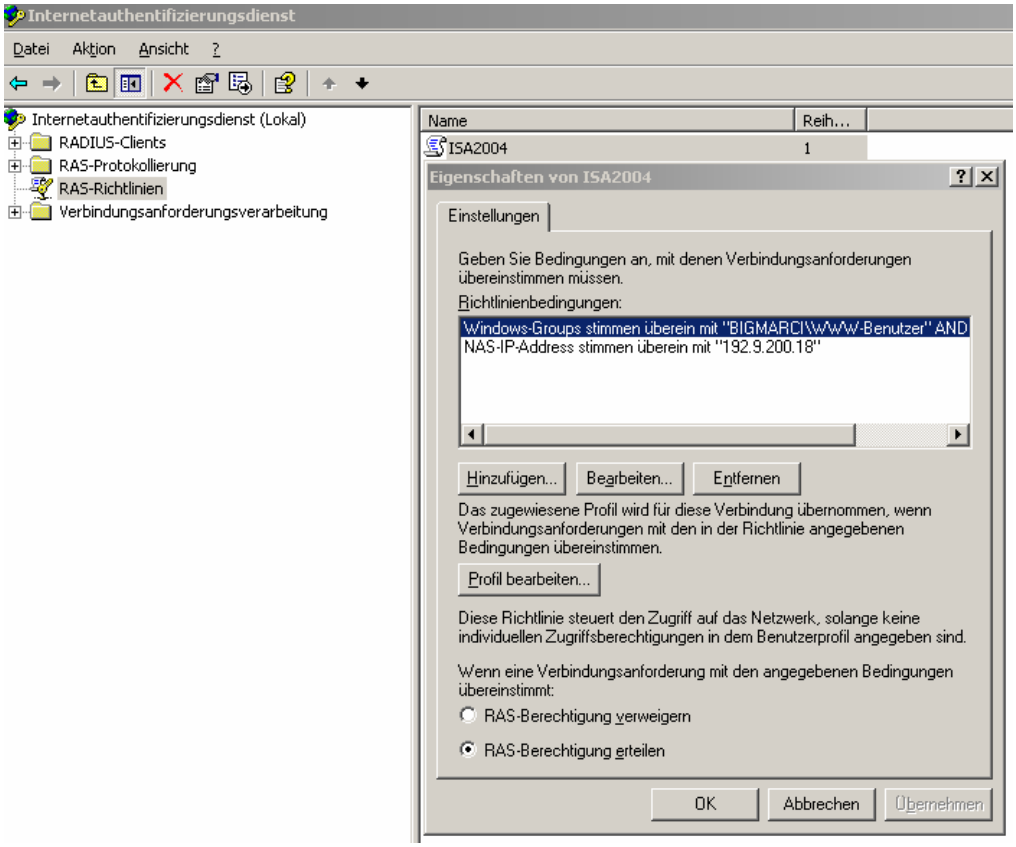
Wichtig:

Bei der Vergabe des geheimen Schlüssels ist die Groß- und Kleinschreibung zu beachten.

Den hier gewählten Schlüssel müssen Sie später auch noch beim ISA Server verwenden, also merken Sie sich den Schlüssel gut ✍

RAS Richtlinie

Erstellen Sie eine neue RAS-Richtlinie mit welcher Sie einer neu zu erstellen Active Directory Benutzergruppe *WWW-Benutzer* das Recht geben, den mit IP Adresse angegebenen ISA Server nutzen zu dürfen.



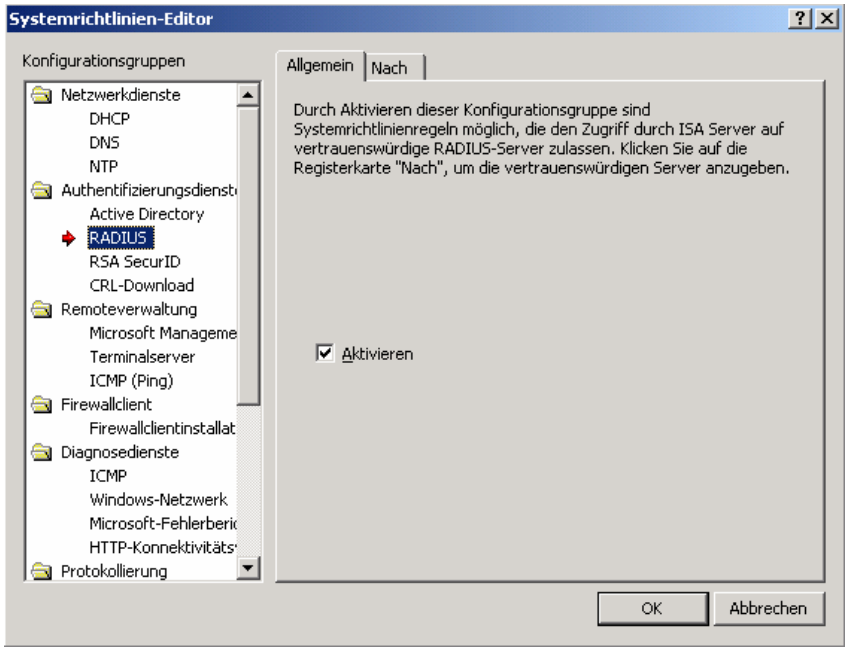
Auf dem ISA Server

Auf dem ISA Server 2004 müssen Sie verschiedene Konfigurationsänderungen vor nehmen, damit der ISA eine Benutzerauthentifizierung über IAS durchführt.

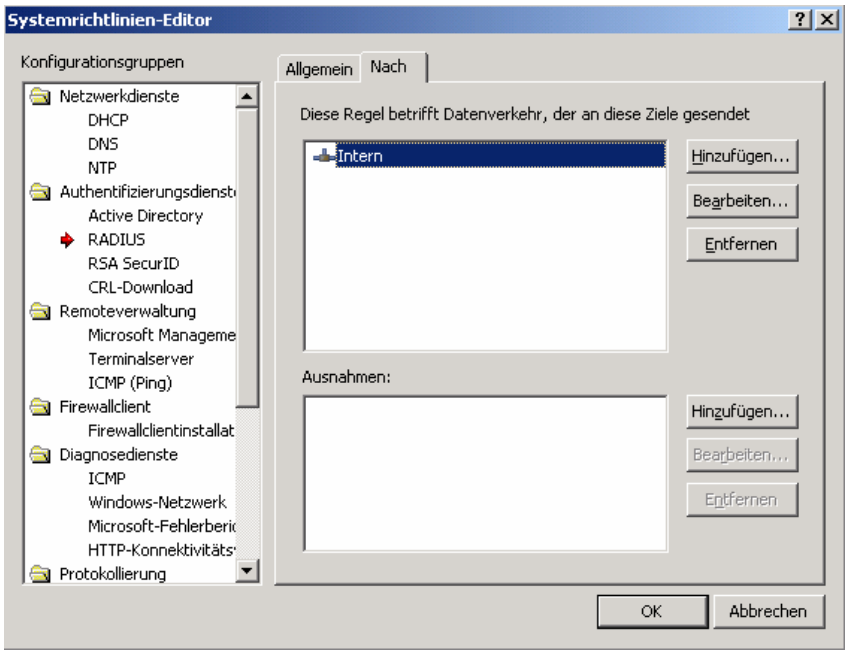
Als erstes müssen Sie überprüfen ob die ISA Server 2004 Firewall Systemrichtlinie den RADIUS Zugriff auf das interne Netzwerk zulässt.

Starten Sie dazu die ISA Server Verwaltungskonsole und klicken Sie mit der rechten Maustaste auf *Firewallrichtlinie* und wählen im Kontextmenü *Systemrichtlinie bearbeiten* aus.

Die Firewallrichtlinie ist per Default aktiviert …

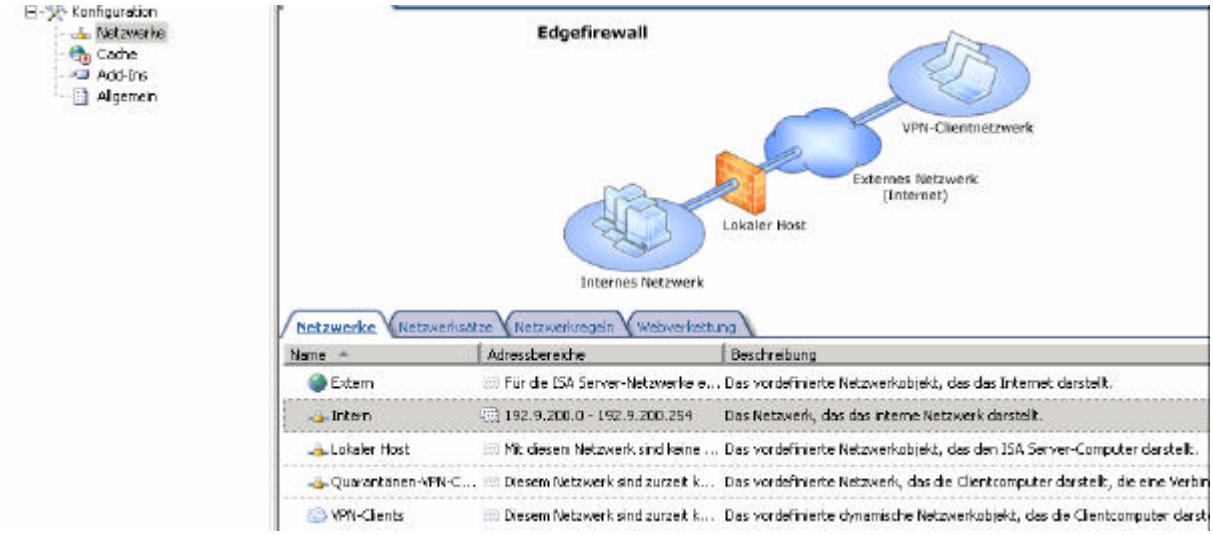


… mit Zugriff auf das Netzwerkobjekt *Intern*.



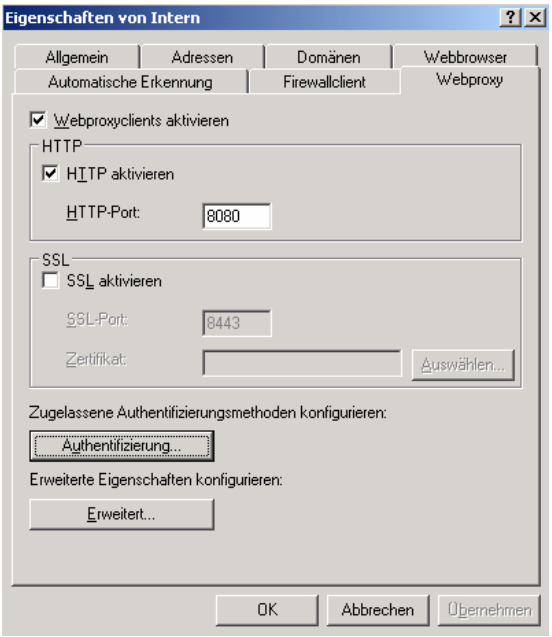
Als nächstes müssen wir dem Netzwerkobjekt *Intern* mitteilen, dass ab sofort eine Authentifizierung der Benutzer erfolgen muss und die Authentifizierungsmethode RADIUS ist.

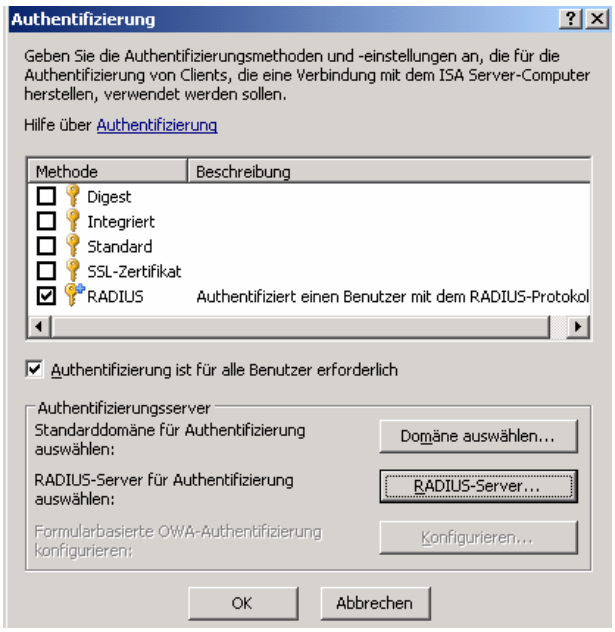
Starten Sie dazu die ISA Verwaltungskonsole und navigieren Sie über die *Konfiguration* zum Container *Netwerke* und wählen dort das Netzwerkobjekt *Intern* aus und gehen in dessen Eigenschaften.



Klicken Sie auf den Reiter *Webproxy* und wählen dort bei der zugelassenen Authentifizierungsmethode *Authentifizierung* aus.

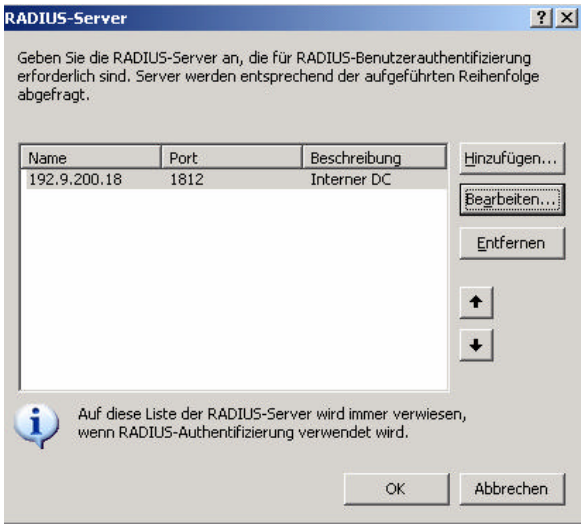
Im nun erscheinenden Fenster wählen Sie die Authentifizierungsmethode *Integriert* (Standardmethode) ab und klicken stattdessen auf *RADIUS*.



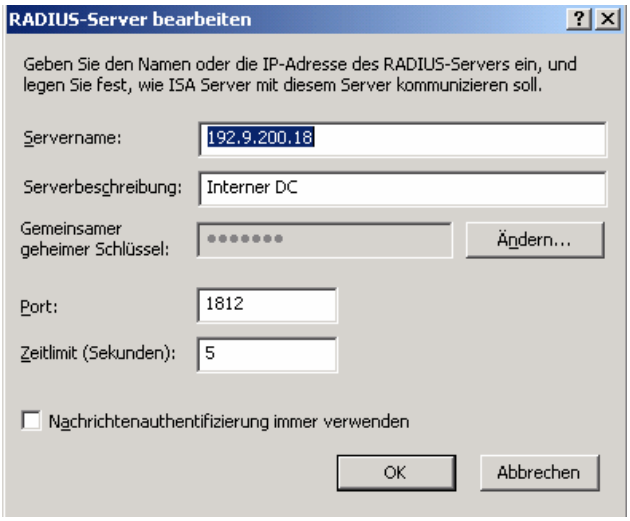


Als nächstes aktivieren Sie *Authentifizierung ist für alle Benutzer erforderlich*. Damit wird sichergestellt, dass nicht autorisierte Benutzer zur Authentifizierung aufgefordert werden.

Im Feld Authentifizierungsserver wählen Sie bitte *RADIUS-Server* aus.
Es erscheint folgendes Fenster (in diesem Beispiel ist bereits ein RADIUS Server konfiguriert). Klicken Sie auf *Hinzufügen*.



Geben Sie unter Servername die IP Adresse oder den Namen des IAS Servers an. Die Serverbeschreibung ist optional, jedoch zur besseren Orientierung und zur Dokumentation sinnvoll.



Im Feld *Gemeinsamer geheimer Schlüssel* geben Sie den im IAS erstellen Schlüssel an. Sie erinnern sich: Xd5$1“xSS(&aäsD03?Q. Bestätigen Sie den Schlüssel noch einmal.

Tipp: Verwenden Sie **NICHT** den Schlüssel in diesem Beispiel.

Der Standard *Port* für RADIUS ist 1812,1645 für die Authentifizierung und 1813,1646 für die Kontoführung. Ändern Sie die Ports nicht. Wenn ja, müssen die Änderungen auch am IAS erfolgen.

Das *Zeitlimit (Sekunden)* sollten Sie nur verändern, wenn der ISA Probleme hat in dieser Zeit den IAS zu kontakten. Das sollte aber nur sehr selten bis gar nicht der Fall sein.

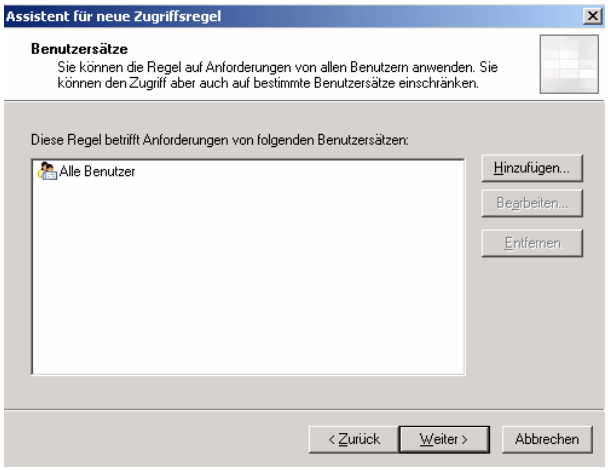
Den Punkt *Nachrichtenauthentifizierung immer verwenden* können Sie unverändert lassen.

Firewallregel auf dem ISA Server

Der nächste Schritt ist die Erstellung eine Firewallregel mit der Verwendung von RADIUS als Benutzerauthentifizierung. In diesem Beispiel verwenden wir eine Firewallregel für den HTPP/HTTPS Zugriff für einen Active Directory Benutzer namens MSISAFAQ.

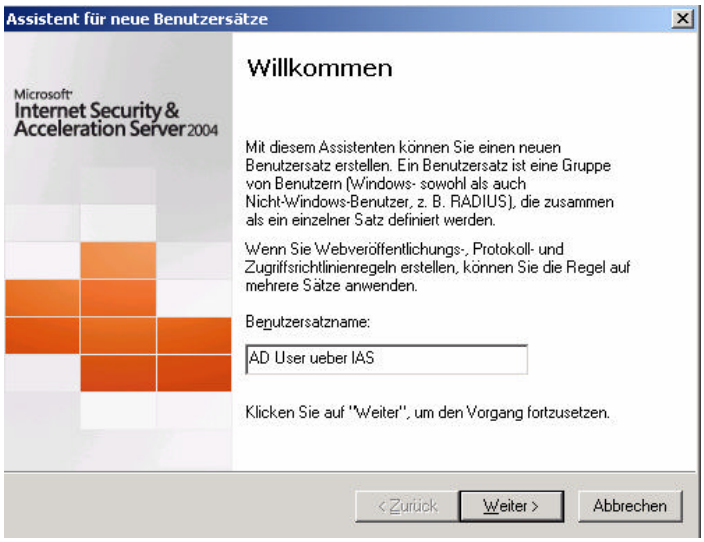
Die ersten Schritte des Wizards zur Erstellung einer Firewallregel erspare ich mir, weil diese sich nicht von der Erstellung einer normalen Regel unterscheiden.

Wir steigen bei dem Punkt *Benutzersätze* des Assistenten für neue Zugriffregeln ein. Entfernen Sie *Alle Benutzer* und klicken Sie auf *Hinzufügen* um einen neuen Benutzersatz zu erstellen.

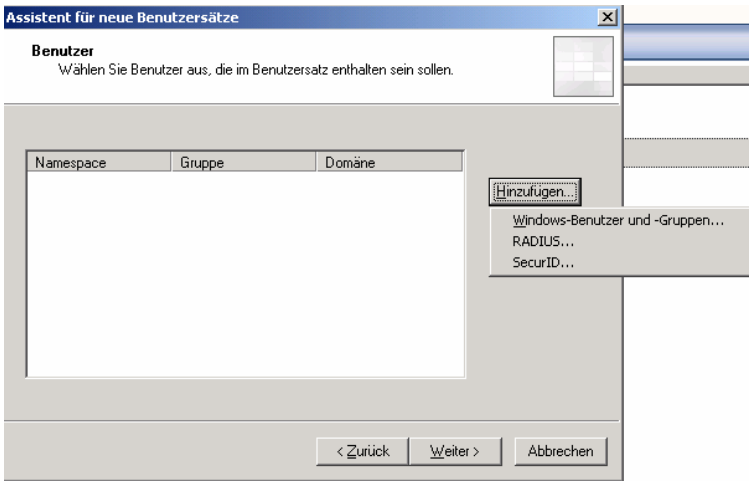


Klicken Sie auf *Neu*

Im Assistenten für Benutzersätze vergeben Sie einen Namen für den neuen Benutzersatz.



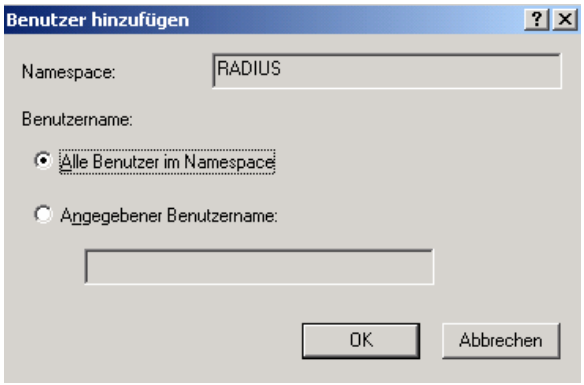
Im Fenster *Benutzer* klicken Sie auf *Hinzufügen* und wählen *RADIUS* aus.



Der Namespace ist RADIUS.

Als Benutzername stehen zur Wahl:

- Alle Benutzer im Namespace – entspricht der Gruppe JEDER der Active Directory Domäne
- Angegebener Benutzername – entspricht dem Active Directory Benutzernamen.



Wir wählen *Alle Benutzer im Namespace*

Das Regelwerk ist fast fertig. Wählen Sie jetzt noch den neu erstellten Benutzersatz aus und bestätigen Sie die neu erstellte Firewallregel.

Sie können diese Regel jetzt verwenden um dem Benutzer das Surfen über den ISA Server 2004 zu erlauben.