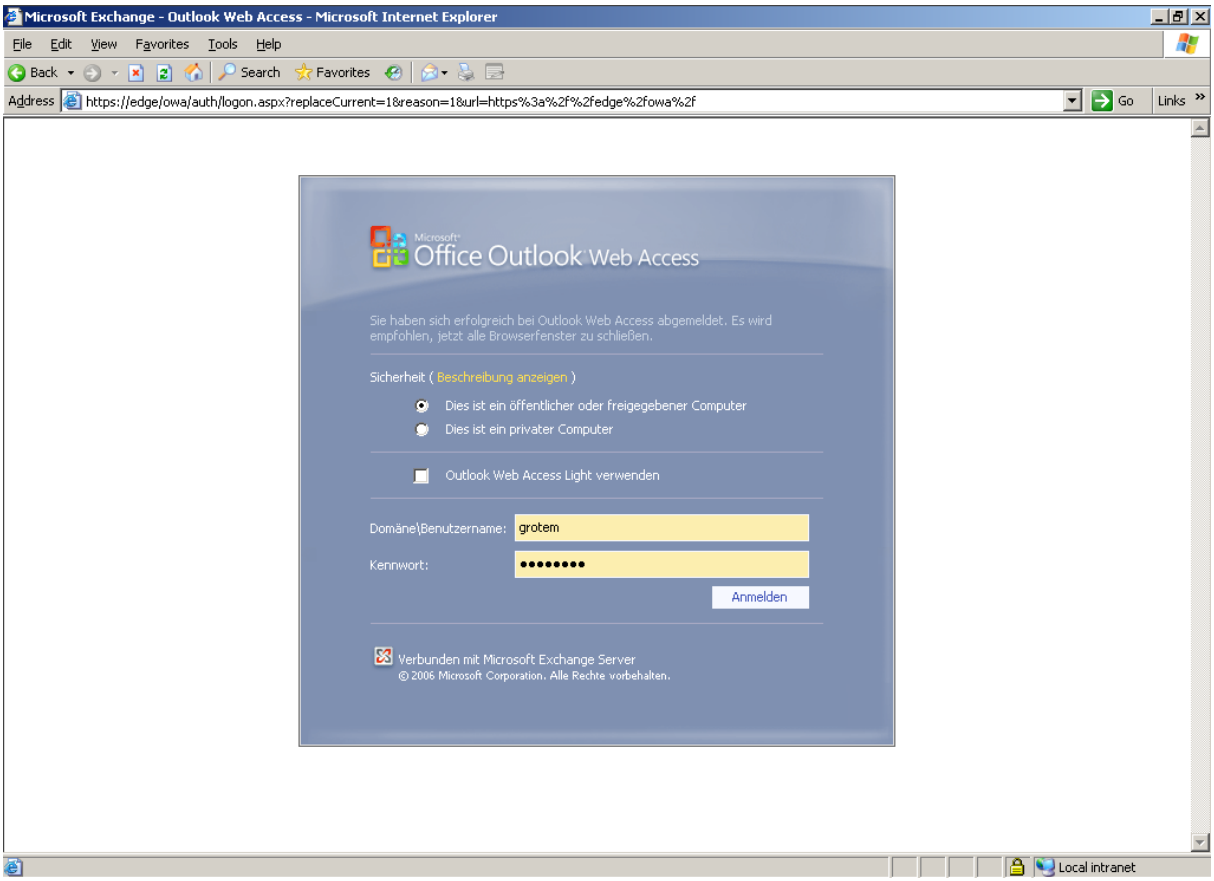
Exchange Server 2007 OWA FBA und ISA Server 2006

Basis:

- Exchange Server 2007 Enterprise Beta 2 Deutsch
- ISA Server 2006 RTM (5.0.5720.100) Standard Deutsch
- Windows XP Professional SP2 Deutsch

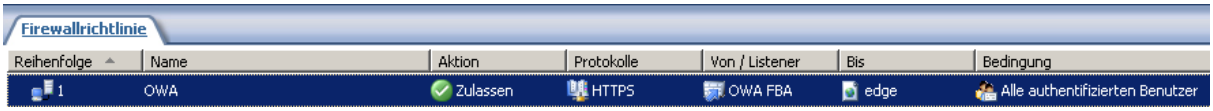
Exchange Server 2007

Auf dem Exchange Server darf die Formularbasierte Authentifizierung (FBA) nicht aktiviert sein, sonst erscheinen beim Client zwei OWA FBA-Anmeldemasken. Der IIS ist mit einem entsprechenden Zertifikat ausgestattet worden. Der lokale OWA FBA Zugriff auf dem Exchange Server und aus dem internen Netzwerk funktioniert einwandfrei (wenn dieser aktiviert ist). Für die Verwendung mit ISA Server 2006 sollte FBA am Exchange wieder deaktiviert werden.



ISA Server 2006

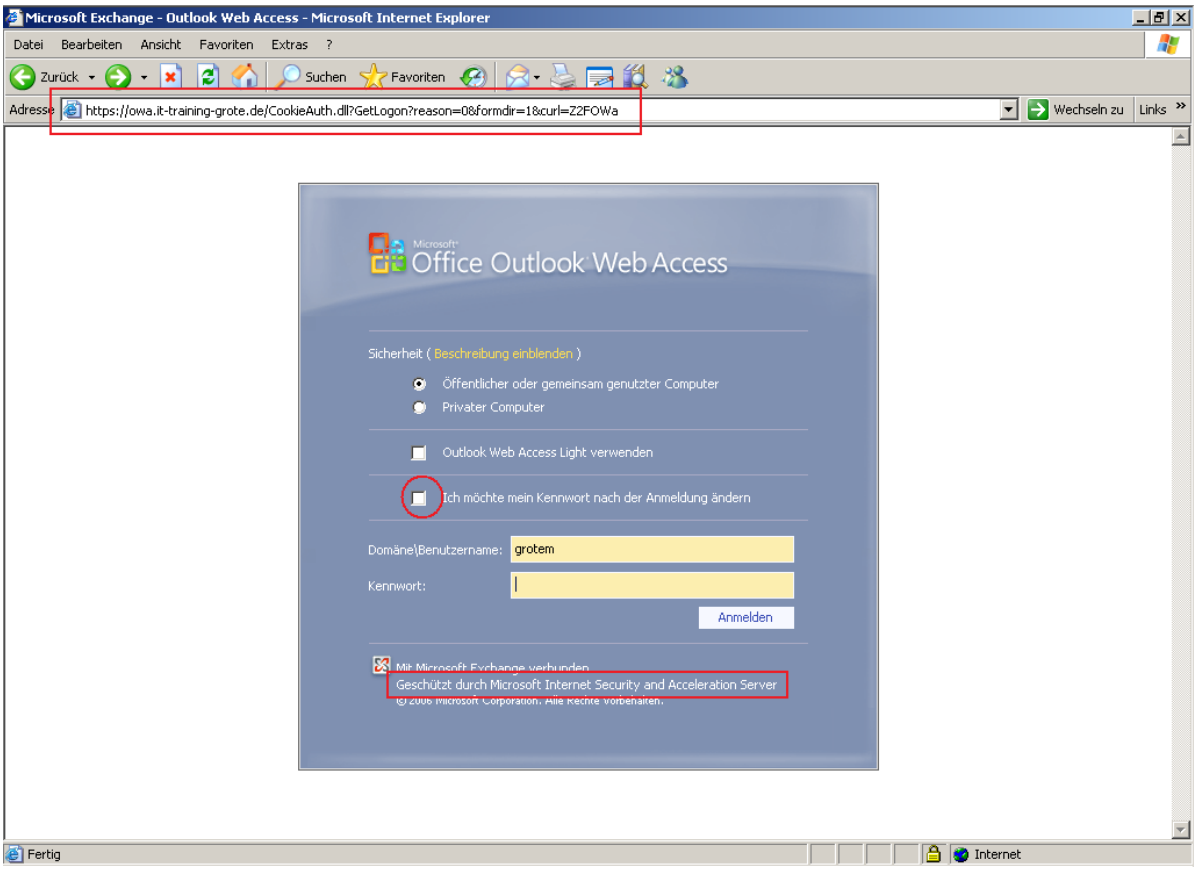
Auf dem ISA Server 2006 wurde eine Exchange-Webclient-Veröffentlichung erstellt. Namensauflösung wurde über Split-DNS gesetzt und die entsprechenden Zertifikate sind ausgestellt. Der OWA FBA Zugriff am ISA Server selbst funktioniert.



Die Standard-OWA Veröffentlichung sieht vor, dass nur „Alle authentifizierten Benutzer“ Zugriff haben.

Aufruf der OWA-Seite vom Client

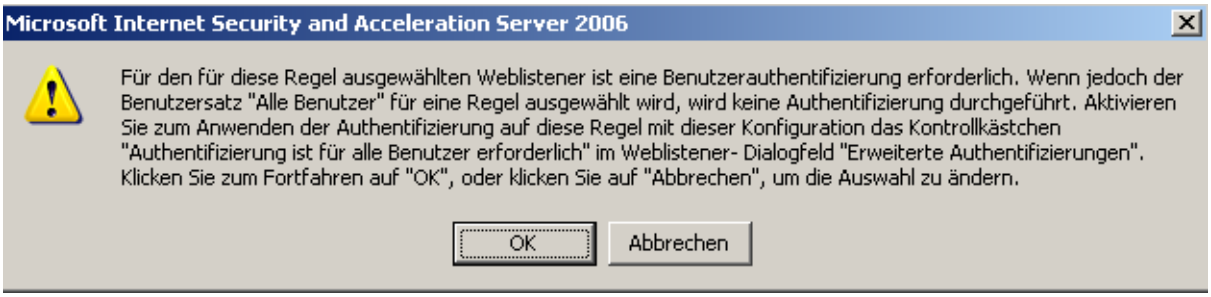
Der Aufruf der OWA Seite über einen externen Client sieht wie folgt aus:



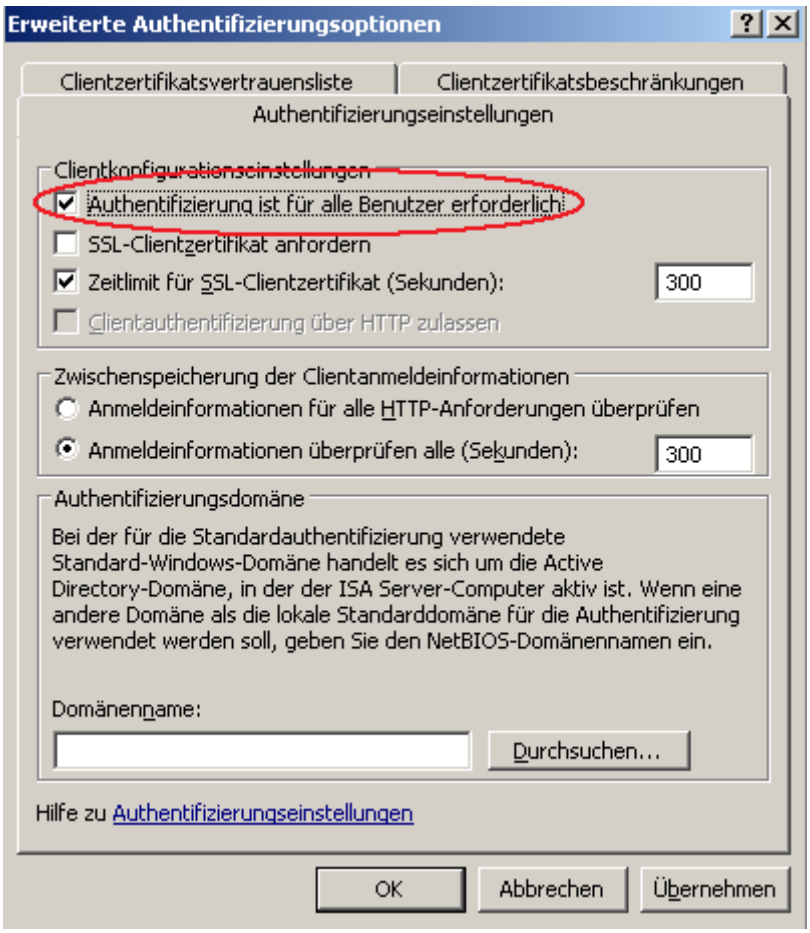
Soweit so gut.

Wenn man jetzt die ISA Regel dahingehend ändert dass „Alle Benutzer“ Zugriff haben, ändert sich das Verhalten:

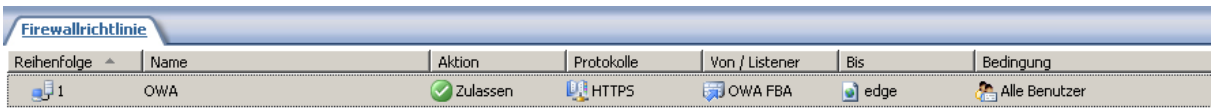
ISA beschwert sich das „Alle Benutzer“ ausgewählt sind…



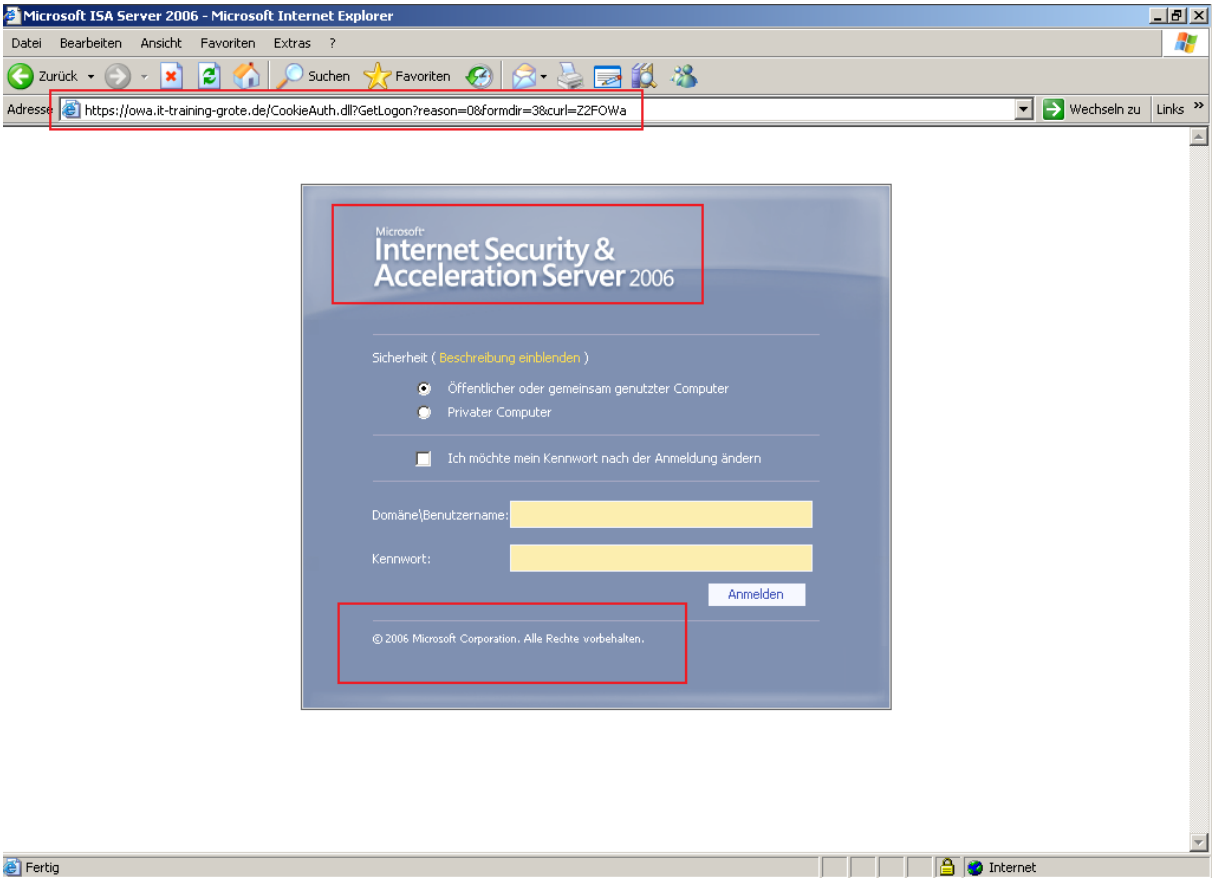
Auch kein Problem, das entsprechende Kontrollkästchen aktiviert …



Danach sieht die Regel oberflächlich so aus:



Das Ergebnis auf dem Client sieht so aus:

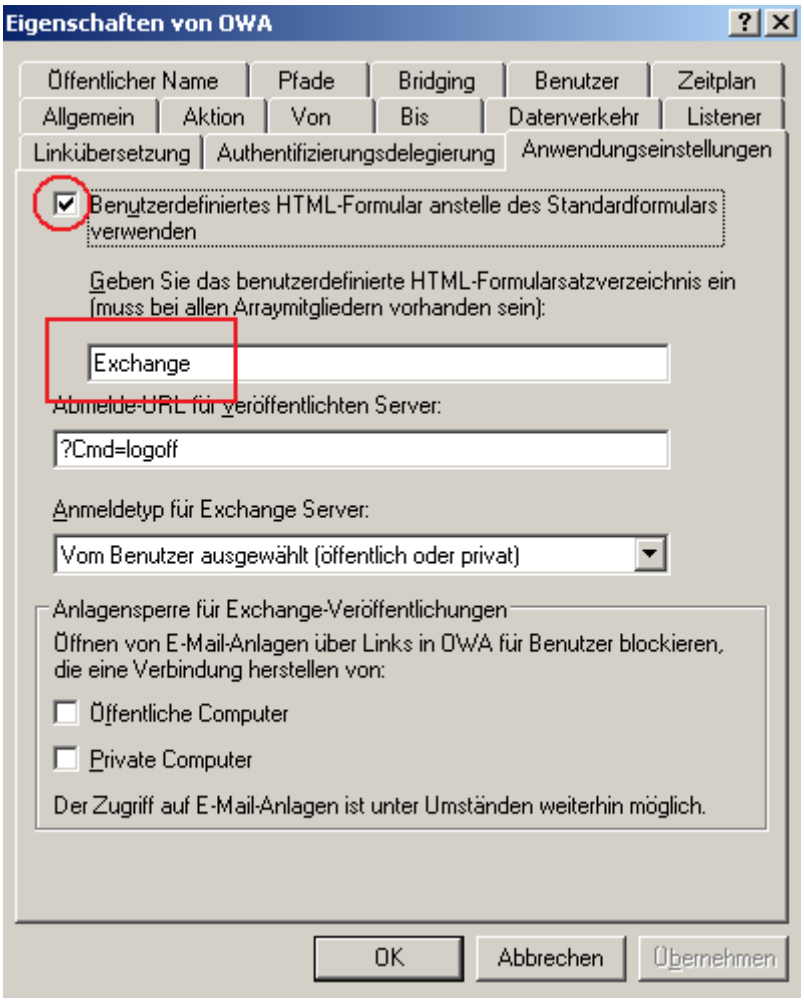


Wo ist die FBA Anmeldemaske wie im Beispiel mit Authentifizierung geblieben?

Selbst wenn man in der Registerkarte Benutzer die „Authentifizierten Benutzer“ wieder rein nimmt, ändert sich die Anmeldemaske am Client nicht. Erst wenn das Kontrollkästchen „Authentifizierung ist für alle Benutzer erforderlich“ am OWA Listener raus nimmt ist die gewohnte Anmeldemaske wieder da!

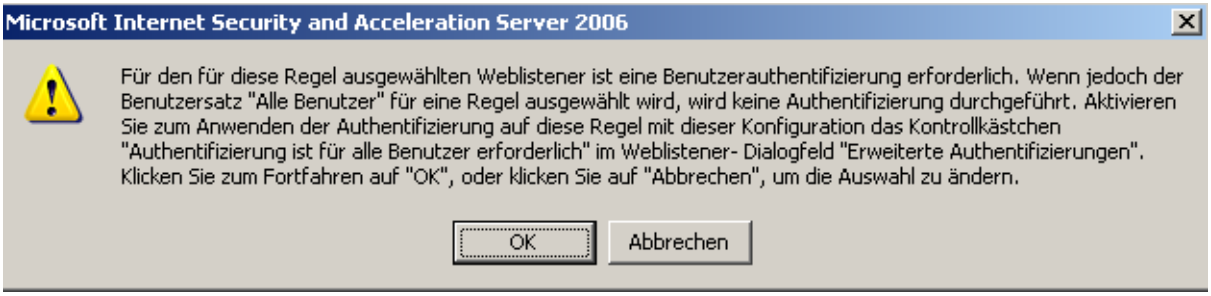
Dieses Verhalten entspricht genau dem wenn man in der OWA FBA Regel in der Registerkarte Anwendungseinstellungen das Kontrollkästchen „Benutzerdefiniertes HTML-Formular anstelle des Standardformulars verwenden“ deaktiviert ist. Die Option wird aber nicht deaktiviert wenn man die Authentifizierung für alle Benutzer fordert und in der OWA FBA Regel „Alle Benutzer“ statt „Alle authentifizierten Benutzer“ einträgt.

Anmelden kann man sich aber übrigens auch mit dieser OWA-Anmeldemaske.



Ist das jetzt ein Bug oder ein Feature? Das Verhalten ist auch unabhängig von der verwendeten Exchange Version da es sich nur auf dem ISA Server und der formularbasierten Authentifizierung abspielt.

Man kann das Problem aber auch „elegant“ zu Lasten der Sicherheit umgehen. Einfach in der OWA FBA Regel „Alle authentifizierten Benutzer“ raus nehmen, die Meldung …



.. ignorieren und dann hat man wieder die ISA FBA OWA Anmeldemaske.

ACHTUNG:

Jetzt macht der ISA Server 2006 allerdings keine Präauthentifizierung mehr. Weder in der Registerkarte „Benutzer“ noch im OWA FBA Listener wird jetzt eine

Authentifizierung gefordert. ISA nimmt die Anfrage entgegen und leitet die Anfrage nach Prüfung an den Exchange Server weiter, der sich dann um die weitere Authentifizierung der Benutzer kümmern muss.

In der Regel macht diese Vorgehensweise keinen Sinn. Wenn sich ISA Server 2006 in der Domäne befindet, kann auch in der OWA FBA Regel Authentifizierung für „Alle authentifizierten Benutzer“ gefordert werden. Befindet sich ISA Server 2006 nicht in der Domäne kann zum Beispiel das mit ISA Server 2006 eingeführte LDAP-Authentifizierungsverfahren im OWA FBA-Listener verwendet werden. Die beschrieben Vorgehensweise macht nur Sinn wenn man auf diese Funktionen verzichten will.