TO:

FROM: ARND.SPIERING@GON.DE

SUBJECT: ASTARO ESSENTIAL FIREWALL NAT

DATE: 24.11.2011

Inhalt

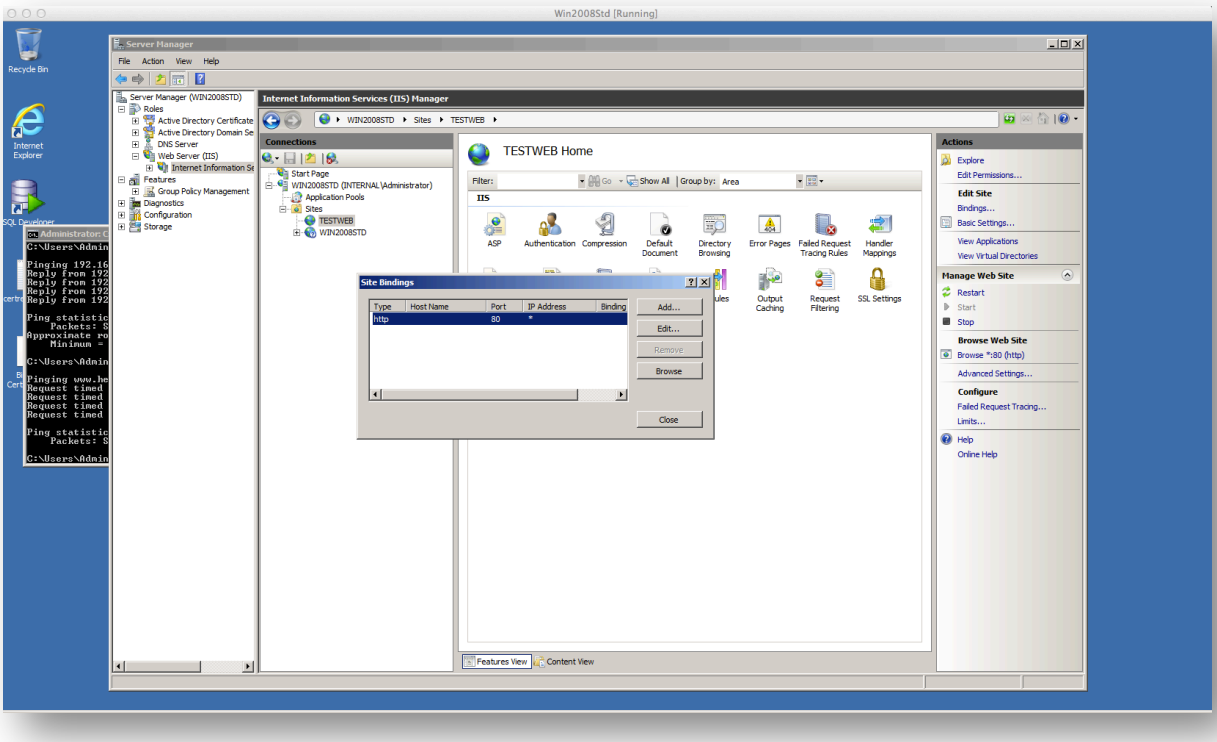
Dieses Dokument beschreibt die Konfiguration einer Weiterleitung des HTTP Dienstes durch die Astaro Firewall in ein internes Netz.

Grundlage ist meine BackTrack 5 R1 Testumgebung. Im internen Netz läuft ein IIS auf der Adresse 192.168.20.244 über Port 80.

Informationen zu der bisherigen Umgebung sind hier zu finden:

1. http://www.as-informatik.net/wordpress/2011/11/24/astaro-essentials-firewall
2. http://www.as-informatik.net/wordpress/2011/11/24/astaro-essential-firewall-scan-mit-nessus/

Aus dem Netz 192.168.0.1/24 soll ein genereller Zugriff auf diese Seite ermöglicht werden.



Für die Anforderung wird folgende Konfiguration auf der Firewall durchgeführt:

GROUP: Anlegen einer Neuen Gruppe WEBSERVER

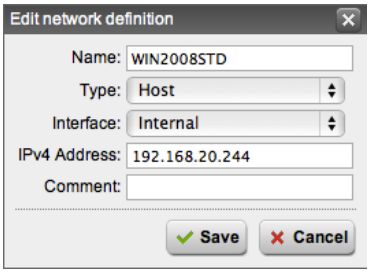
Traffic Source: ANY

Traffic Service: HTTP

Traffic Destination: External (WAN) Address 192.168.0.66

NAT mode: Full NAT

Destination:

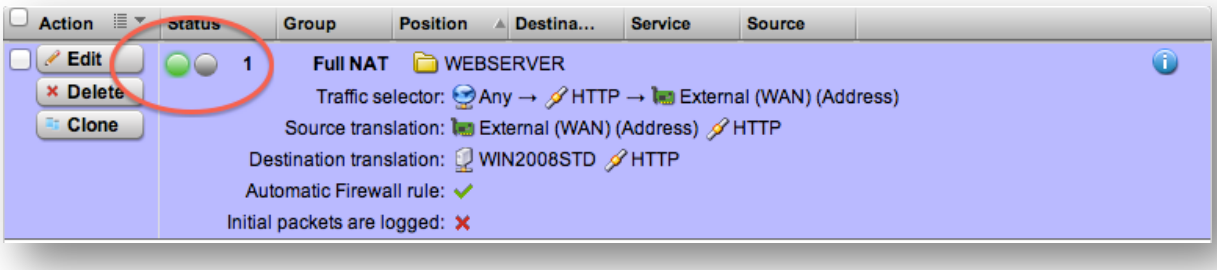


Destination Service: HTTP

Source: External (WAN) Address 192.168.0.66

Source Destination: HTTP

Nachdem die Regel gespeichert wurde, muss diese noch aktiviert werden.

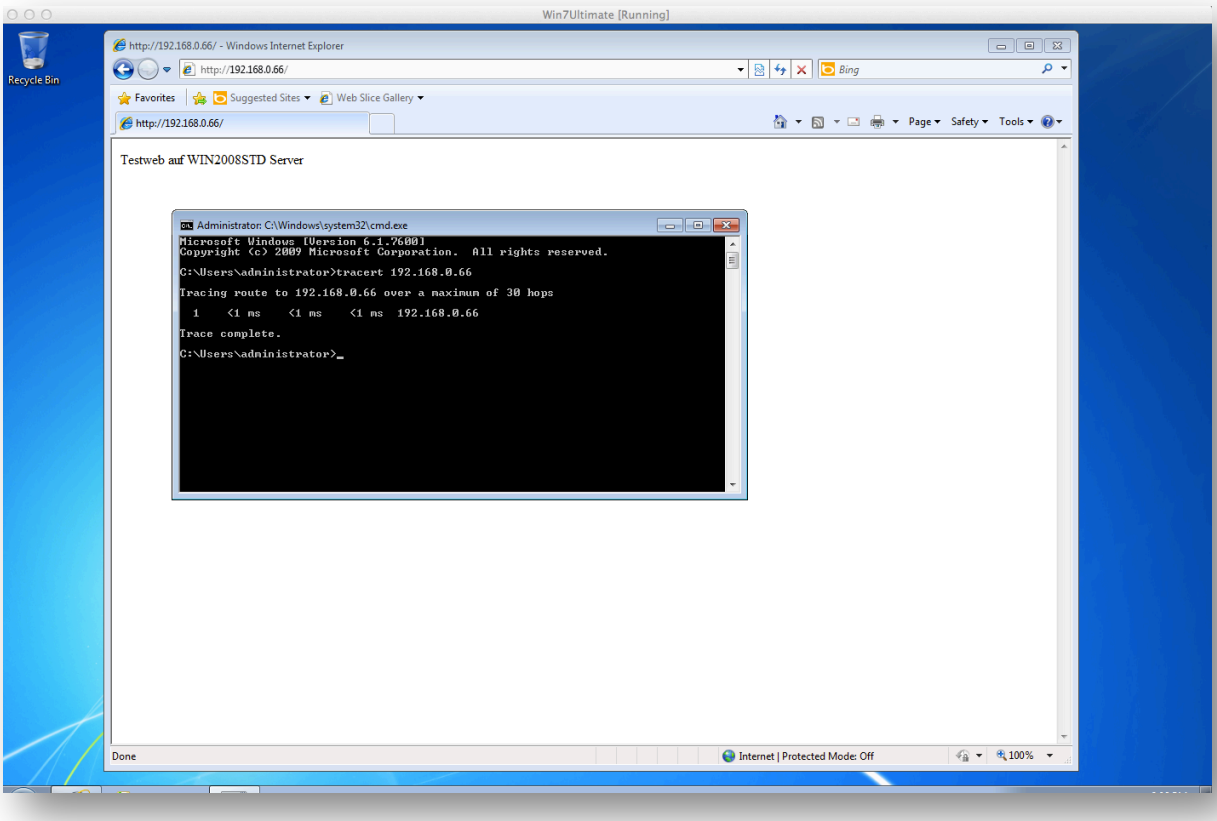


HINWEIS:

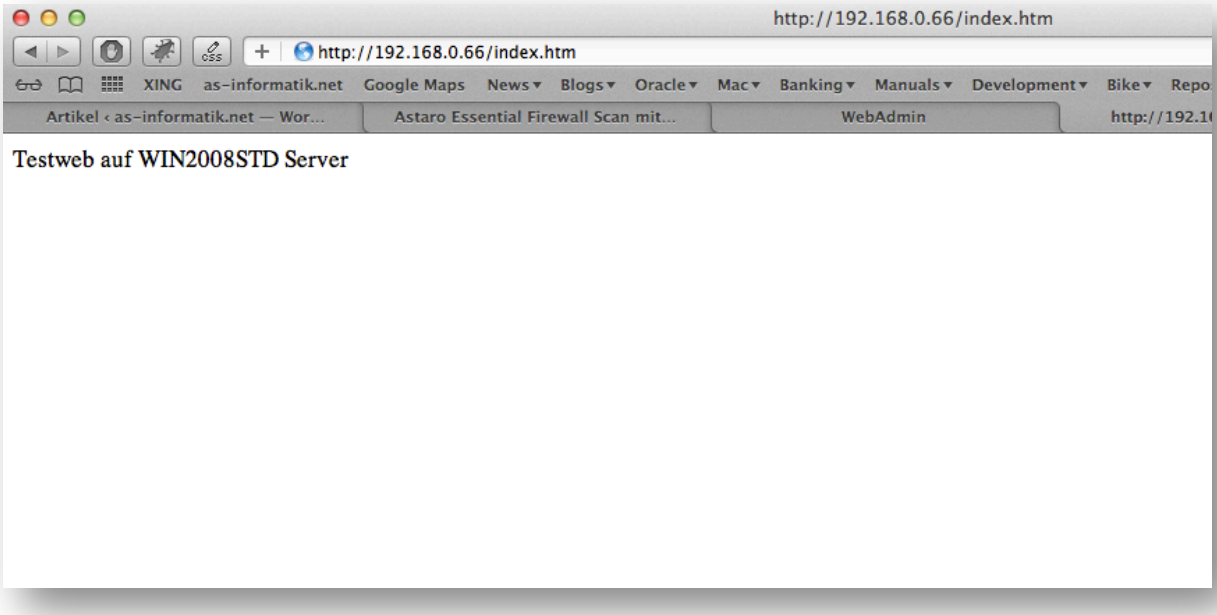
Häufig werden für Traffic Service mehrere Dienste (HTTP, HTTPS, FTP,...) in einer Gruppe zusammen gelegt.

Ich halte maximal eine gruppe pro Server für eine Gute Idee, da so sehr schnell über Clone (Duplizieren einer Regel mit späterer Anpassung) für andere Dienste im internen Netz „ungewollt“ Zugriffe aus externen Ressourcen geöffnet werden. So wird direkt gegen die BSI Empfehlung „Minimaltät“ verstoßen.

Nach der Aktivierung der Regel ist ein externer und interner Zugriff auf http://192.168.0.66 möglich.



Zugriff aus dem internen Netz Windows 7 Client



Zugriff aus dem externen Netz (Mac)

Erneuter Nessus Scan

Nach solchen Konfigurationen sollte zur Sicherheit nochmals ein Scan durchgeführt werden.

Wie erwartet, findet Nessus die neu geöffneten Ports und gibt entsprechende Informationen: