

SMTP Relay mit ACL auf Citrix ADC konfigurieren

Vor knapp zwei Jahren erstellte ich hier einen Artikel, wie man grundsätzlich einen SMTP Relay mit NetScaler konfigurieren kann ([hier](#)). Im Rahmen einer Datacenter Migration kam das Thema ACL für diesen Relay auf. Im genannten Artikel wurde sauber beschrieben, wie man den Exchange auf den ADC als Quelle konfigurieren kann. Wie kann man nun aber die Quellen seitens Loadbalancer einschränken?

Wer schon mit dem ADC gearbeitet hat weiss, dass dieser Access Control List (ACL) als Funktion bietet, jedoch ist die Konfiguration dieser eher statisch als dynamisch. Ich arbeite jedoch in einem Umfeld, in welchem die zugelassenen Server immer wieder mal ändern können (bei über 1000 Servern kein Wunder). Daher habe ich ein wenig Recherchiert und bin auf einen Lösungsansatz mittels Responder Policies gestossen, welchen ich hier dokumentiere.

Als erstes muss das Loadbalancing für den SMTP Relay konfiguriert werden. Ich nehme dazu als Basis den letzten Artikel und schmücke diesen mit ein wenig mehr Backend-Servern aus:

```
add server pitex01 192.168.100.31
add server pitex02 192.168.100.32
add service svc-smtp-pitex01 pitex01 TCP 25
add service svc-smtp-pitex02 pitex02 TCP 25
```

```
add lb vserver lb-vsrv-mailrelay.domain.pit-SMTP TCP
192.168.100.90 25 -persistenceType SOURCEIP -timeout 10 -
netprofile NP-192.168.100.12
bind lb vserver lb-vsrv-mailrelay.domain.pit-SMTP svc-smtp-
pitex01
bind lb vserver lb-vsrv-mailrelay.domain.pit-SMTP svc-smtp-
pitex02
```

Nun bauen wir unsere Responder Policy. Damit die Pflege der Quell IPs ein wenig einfacher ist, nutzen wir dazu die sogenannten Data Sets (ähnlich wie Pattern Sets, jedoch für Daten wie IP Adressen) und verweisen in unserer Policy darauf. Als Aktion nehmen wir die vordefinierten „RESET“ Aktion.

```
add policy dataset DS_MailRelay ipv4
bind policy dataset DS_MailRelay 192.168.100.21 -index 1
bind policy dataset DS_MailRelay 192.168.100.22 -index 2
add responder policy rs_pol_ACLMailRelay
"CLIENT.IP.SRC.TYPECAST_TEXT_T.CONTAINS_ANY(\"DS_MailRelay\").
NOT" RESET
```

Schlussendlich müssen wir nur doch die neu erstellte Policy dem SMTP Relay Loadbalancer zuweisen und ab sofort nimmt dieser nur noch Anfragen von IPs an, welche im Data Set „DS_MailRelay“ definiert sind.

```
bind lb vserver lb-vsrv-mailrelay.domain.pit-SMTP -policyName
rs_pol_ACLMailRelay -priority 100 -gotoPriorityExpression END
-type REQUEST
```

[ADS-SMTPRelayACL.txtHerunterladen](#)