Panda GateDefender eSeries

Inhaltsfilter (Webfilter) How-To

Die Inhaltsfilterfunktionen der Panda GateDefender-Appliance basieren auf der URL-Filterlösung von Commtouch. Von dieser werden zwei Filtertechniken verwendet, die für Filterprofile definiert werden können.

Die erste besteht aus erweiterten Methoden für die Kategorisierung von Webseiten basierend auf dem Inhalt. Die zweite Methode verwendet eine Kombination aus White- und Blacklist-URLs und Domains: Alle von Clients angeforderten URLs werden in der Liste nachgeschlagen und nur bereitgestellt, wenn sie in der Whitelist gefunden werden.

Für die Verwendung des Inhaltsfilters wird ein Profil benötigt. Ein Standardprofil, durch das der Zugriff für alle Webseiten erlaubt wird, und das nicht gelöscht werden kann, ist bereits verfügbar. Zusätzliche Profile, die bei der Definition einer Zugriffsrichtlinie benötigt werden, können leicht erstellt werden. Deshalb können Zugriffsrichtlinien, die ein bestimmtes Profil benötigen, nur nach dem Profil erstellt werden.

Diese Anleitung führt Sie Schritt für Schritt durch die Konfiguration des Profils sowie der Zugriffsrichtlinie und veranschaulicht dies Anhand eines Beispiels. Eine ausführliche Dokumentation zur Panda GateDefender eSeries Appliance finden Sie unter folgendem Link: http://acs.pandasoftware.com/eSeries/Appliance/5.00/manual/de/

1. HTTP Proxy aktivieren

1. Öffnen Sie die Konfigurationskonsole Ihrer Panda GateDefender eSeries Appliance

Diese erreichen Sie Standardmäßig unter https://192.168.0.15:10443

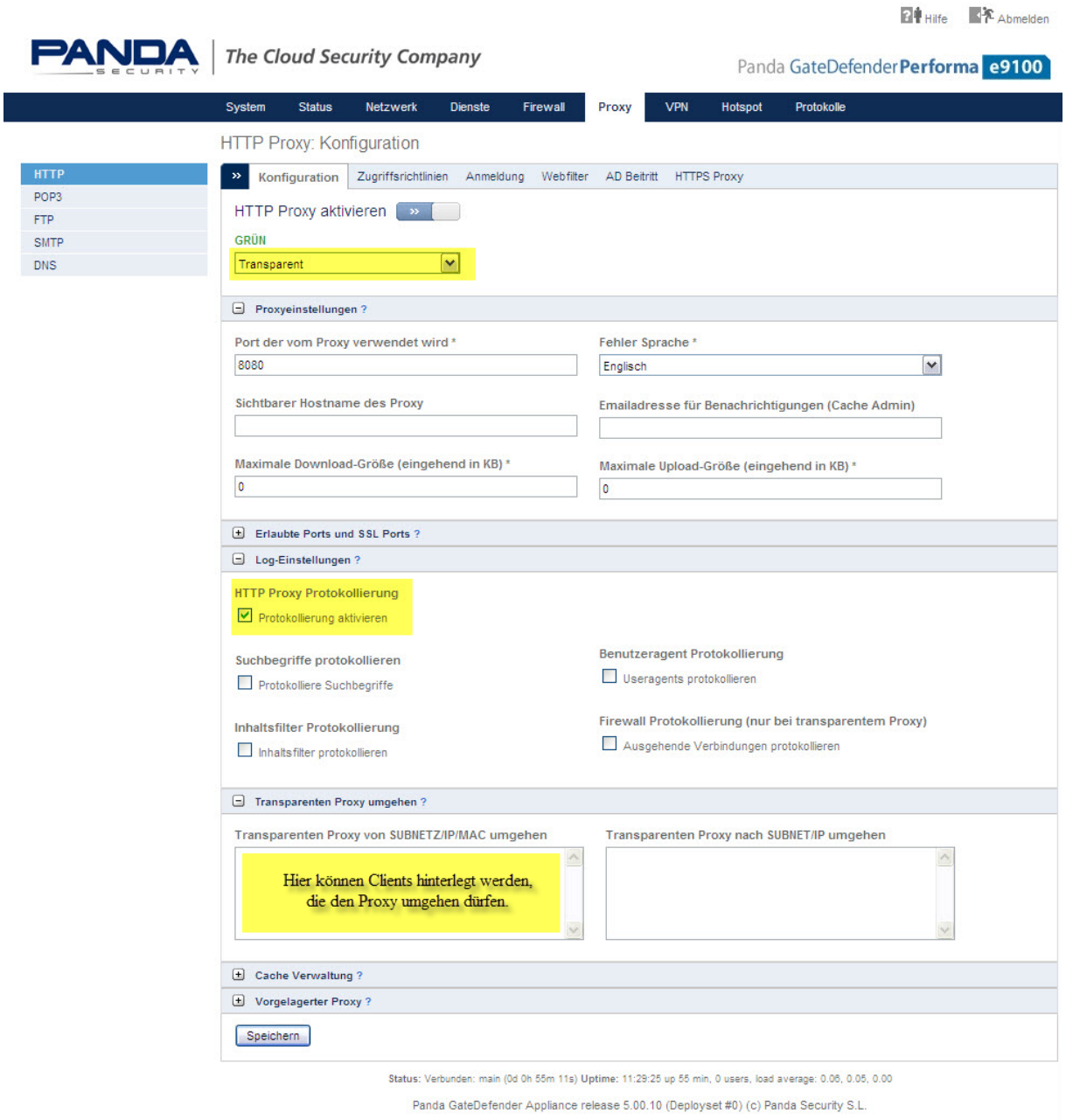
2. Wechseln Sie auf den Reiter „Proxy“

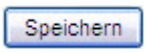
Aktivieren Sie den HTTP Proxy mit Klick auf

3. HTTP Proxy Konfiguration

Nachdem Sie den http Proxy aktiviert haben, können Sie diesen entsprechend Ihren Anforderungen konfigurieren.

- Stellen Sie den HTTP Proxy je nach Bedarf auf „**Transparent**“ oder „**nicht Transparent**“
- Hinterlegen Sie den **Port**, den Sie für den Proxy nutzen möchten
- Zusätzlich können Sie die **HTTP Proxy Protokollierung** aktivieren (empfohlen). Dies kann bei der Einrichtung behilflich sein etwaige Fehlerquellen ausfindig zu machen.
- Haben Sie Clients in Ihrem Netzwerk, die den Proxy nicht nutzen sollen (z.B. Geschäftsführer), können diese unter „**Transparenten Proxy umgehen**“ ausgeschlossen werden.

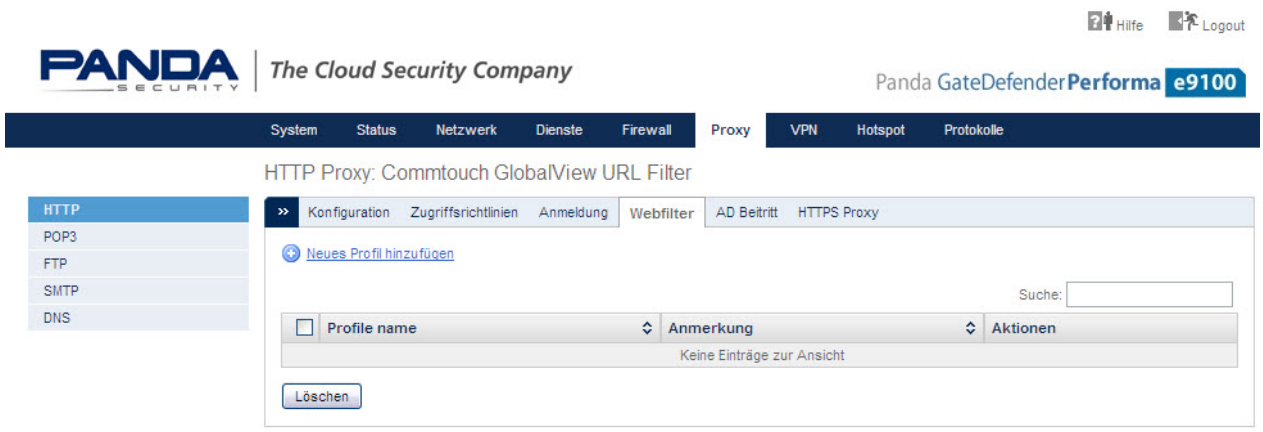


Speichern Sie Ihre Konfiguration mit Klick auf 

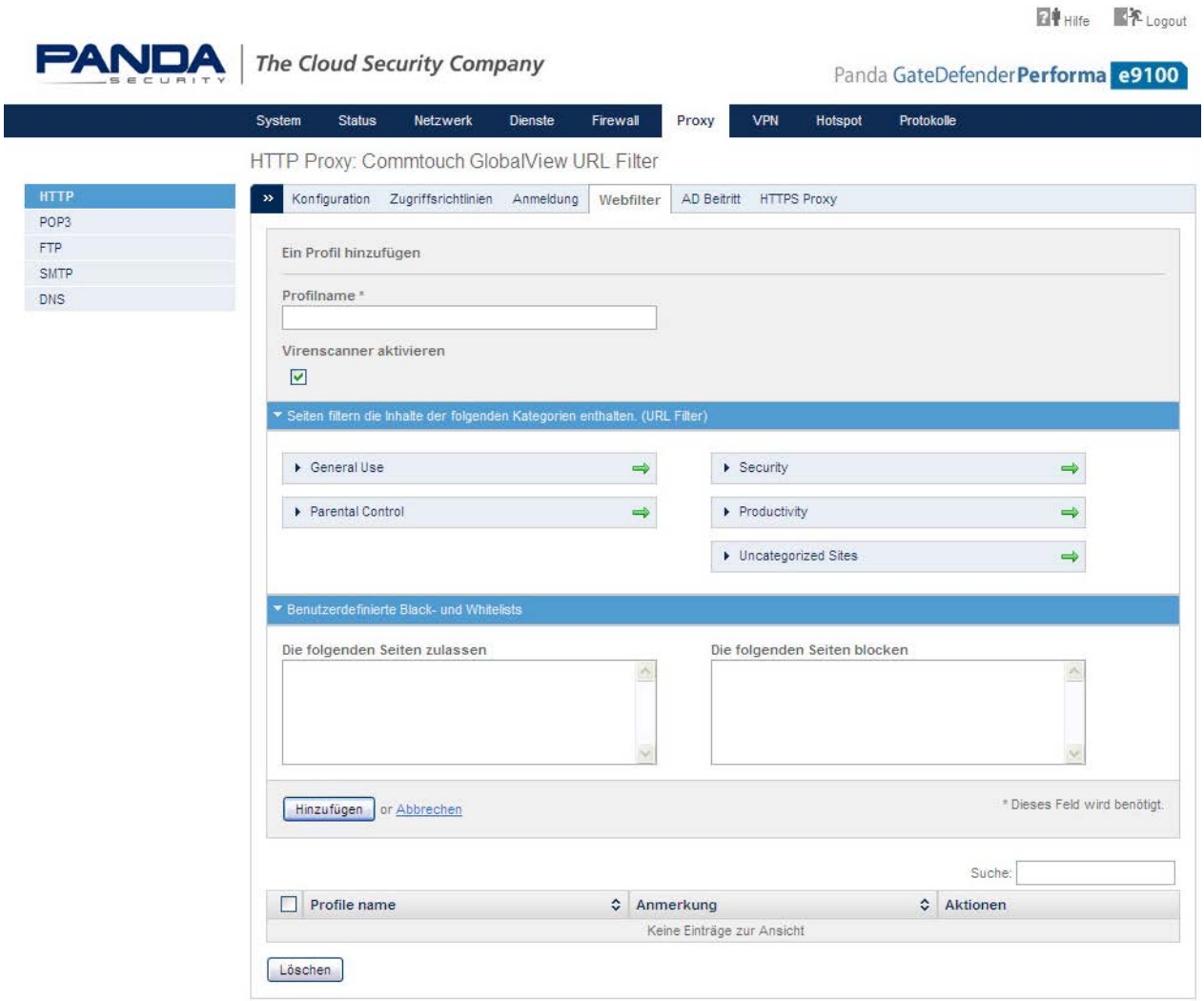
Bitte beachten Sie, dass nachdem die Konfiguration gespeichert wurde diese noch übernommen werden muss. Klicken Sie auf Übernehmen.

2. Profil anlegen

Wechseln Sie auf den Reiter „Webfilter“ und klicken den Link Neues Profil hinzufügen an.



Es öffnet sich der Profil Konfigurationsdialog



Bitte vergeben Sie hier zunächst einen Aussagekräftigen **Profilnamen**. Des Weiteren haben Sie die Möglichkeit den Inhaltsfilter nach bereits vordefinierten Kategorien zu konfigurieren.

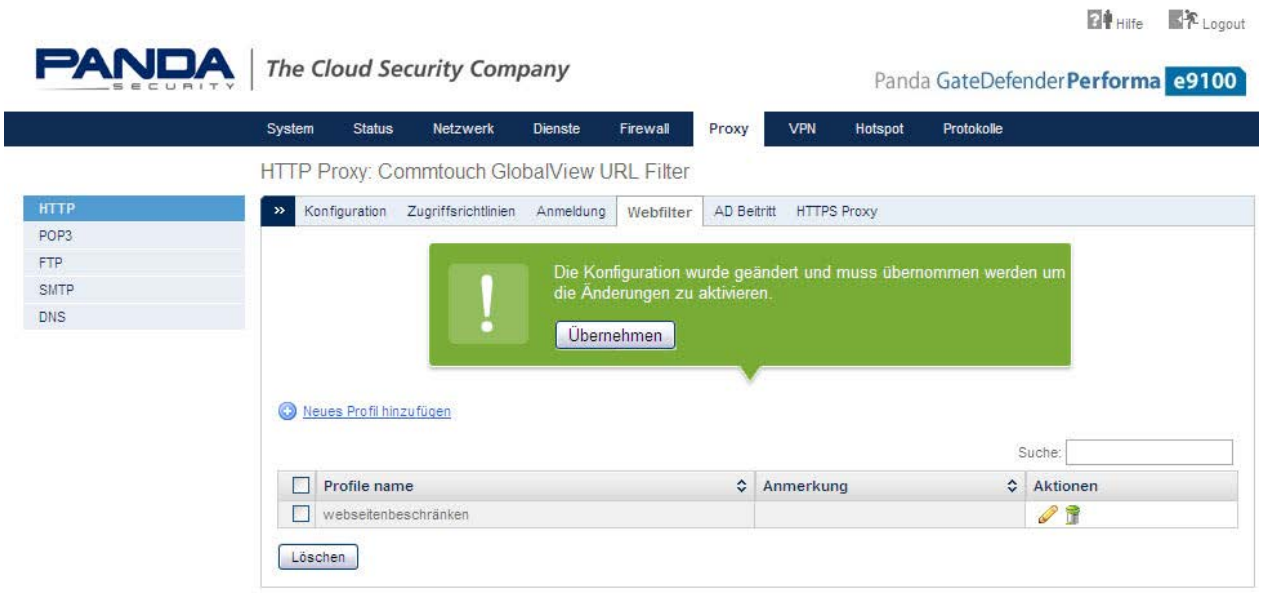
Es stehen Ihnen folgende vordefinierte Kategorien zur Verfügung:

- Eine bereits ausgewählte Kategorie wird Ihnen mit Hilfe des Symbols signalisiert.

- Bitte beachten Sie, dass einzelne Kategorien in mehreren Gruppen vorkommen können.

Nachdem Sie das Profil Wunschgemäß konfiguriert haben speichern Sie das Profil mit Klick auf Hinzufügen

Auch hier müssen die Änderungen übernommen werden, um das neuangelegte Profil zu aktivieren.



Klicken Sie auf Übernehmen.

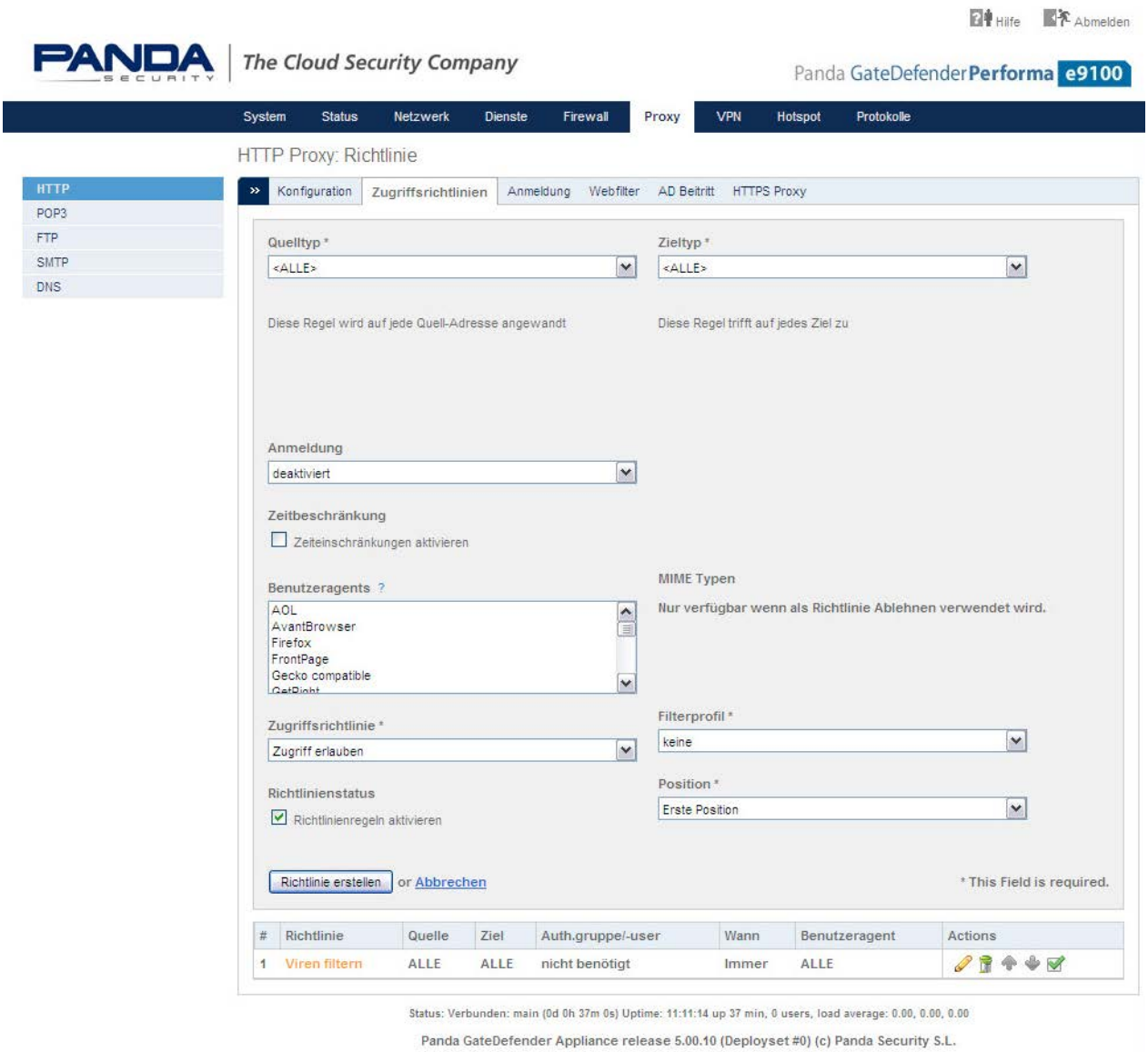
Sie haben nun ein Profil angelegt und können mit dem Anlegen der Zugriffsberechtigung fortfahren.

3. Zugriffsrichtlinie anlegen

Um das zuvor angelegte Profil anwenden zu können benötigt es noch einer entsprechenden Zugriffsrichtlinie. Wechseln Sie hierzu auf den Reiter „**Zugriffsrichtlinien**".

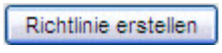
Um eine neue Zugriffsrichtlinie hinzuzufügen klicken Sie auf den Link Zugriffsrichtlinie hinzufügen

Im folgenden Dialog können Sie die Zugriffrichtlinie entsprechend Konfigurieren:



- Sie haben die Möglichkeit Quell- und Zieltyp festzulegen
  - Beim **Quelltyp** haben Sie folgenden Auswahlmöglichkeiten: **ALLE** | **ZONE** | **NETZWERK/IP** | **MAC**
  - Beim **Zieltyp** haben Sie folgende Auswahlmöglichkeiten: **ALLE** | **ZONE** | **NETZWERK/IP** | **DOMÄNE**

- Unter „**Filterprofil**" wählen Sie das zuvor angelegte Profil aus. In diesem Beispiel ist es das Profil „**webseitenbeschränken**".

Speichern Sie die Zugriffsrichtlinie über die Schaltfläche 

Auch die Zugriffsrichtline bedarf einer Aktivierung. Klicken Sie auf Übernehmen.

Nachdem die Zugriffsrichtlinie aktiviert wurde, ist der Inhaltsfilter sofort aktiv. Sie erhalten dann im Browser folgende Meldungen, wenn eine URL der Konfiguration im Profil entspricht.

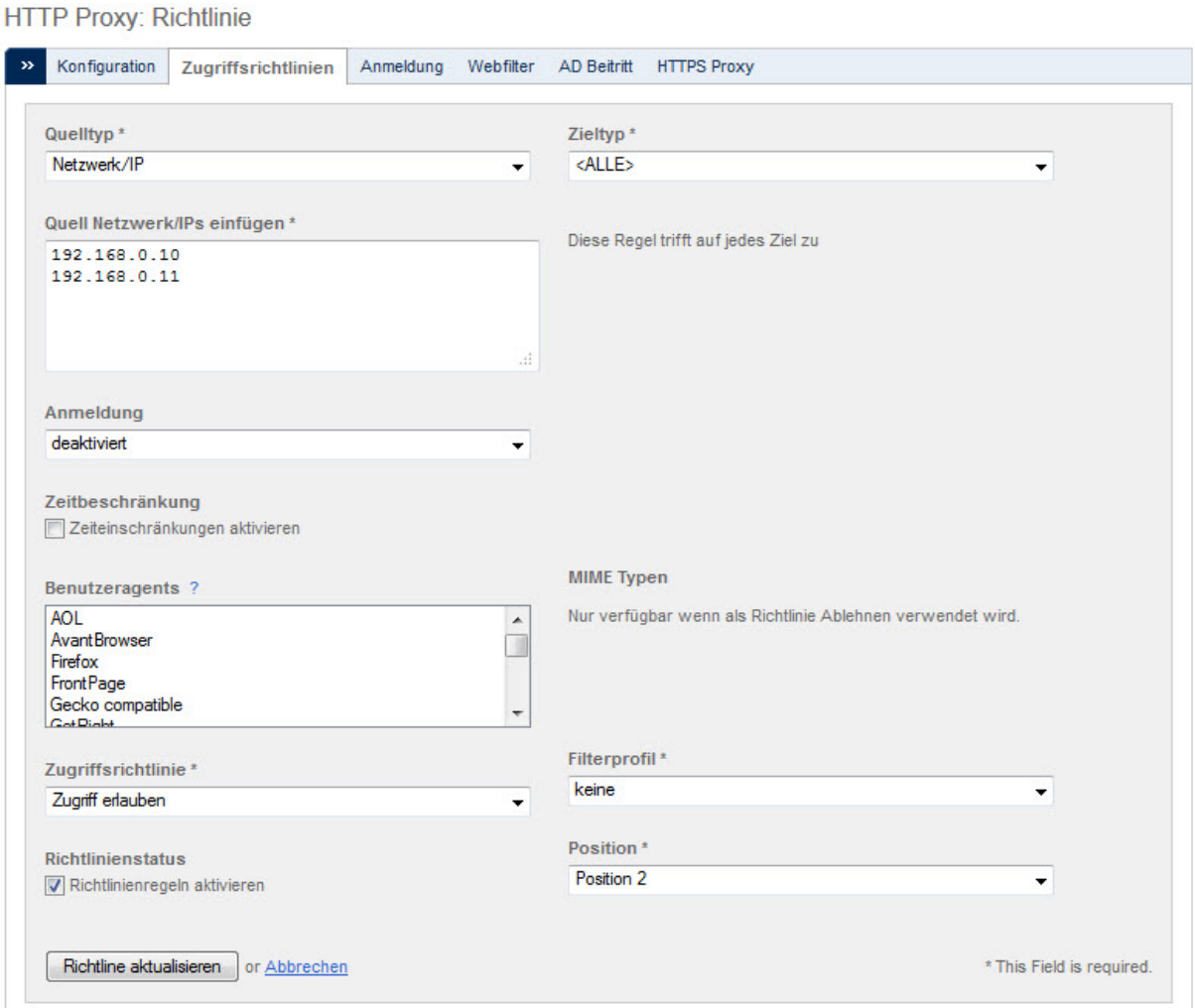
Blockierung anhand vordefinierter Konfiguration. Hier Social Networking

Blockierung anhand der Blacklist.

Nachfolgend zwei Beispiele

1. Beispiel

Zugriffsrichtlinie, die zwei Netzwerk IP Adressen (192.168.0.10 / 192.168.0.11) uneingeschränkten Zugriff auf das Internet gewährt.



2. Beispiel

Nutzung mehrerer Zugriffsrichtlinien. Die Richtlinien werden von oben nach unten priorisiert abgearbeitet.

- Jeder Client hat uneingeschränkten Zugriff auf folgende Domains (Richtlinie #1): **pandasecurity.com / pandasoftware.de / microsoft.com**
- 2 durch IP-Adressen definierte Clients haben uneingeschränkten Zugriff (Richtlinie #2)
- Alle Clients aus der grünen Zone nutzen das Profil „**webseitenbeschränken**“ (Richtlinie #3)
- Alle Aufrufe werden auf Viren geprüft (Richtlinie #4)
- Zugriff auf Webseiten, die auf keine der vorangegangenen Zugriffsrichtlinien zutreffen, wird gesperrt (Richtlinie #5)

HTTP Proxy: Richtlinie

#	Richtlinie	Quelle	Ziel	Auth.gruppe/-user	Wann	Benutzeragent	Actions
1	ungefilterter Zugriff	ALLE	.pandasecurity.com .pandasoftware.de .microsoft.com	nicht benötigt	Immer	ALLE	
2	ungefilterter Zugriff	192.168.0.10 192.168.0.11	ALLE	nicht benötigt	Immer	ALLE	
3	filter using 'webseitenbeschränken'	GREEN	ALLE	nicht benötigt	Immer	ALLE	
4	Viren filtern	ALLE	ALLE	nicht benötigt	Immer	ALLE	
5	Zugriff verweigert	ALLE	ALLE	nicht benötigt	Immer	ALLE	