Plattformunabhängiges Visualisierungstool zur Darstellung typisierter IP-Adressbereiche

IPMapViewer - Getting started

September 2010

Autoren

Christian J. Dietrich
E-Mail: dietrich [at] internet-sicherheit.de

Alexander Schuch
E-Mail: schuch [at] internet-sicherheit.de

Institut für Internet-Sicherheit, FH Gelsenkirchen
https://www.internet-sicherheit.de

Inhaltsverzeichnis

1 Getting started....2
1.1 Virtual Appliance importieren und nutzen....2
1.2 Installation von PostgreSQL mit ip4r....4
2 Starten des IPMapViewers....6
2.1 Darstellen von IP-Adressen....6
Abbildungsverzeichnis....13

1 Getting started

Um den IPMapViewer verwenden zu können, wird eine installierte PostgreSQL[1]-Datenbank mit dem Datentypen ip4r[2] benötigt. Hierzu gibt es 2 Möglichkeiten. Auf der Webseite des Instituts für Internet-Sicherheit unter http://www.internet-sicherheit.de/service/tools/ipmapviewer/ eine Virtual Appliance für VirtualBox[3] zur Verfügung gestellt, die die benötigte Funktionalität auf Serverseite enthält (PostgreSQL-Server mit ip4r). Wenn Sie die Appliance nutzen, fahren Sie mit Kapitel 1.1 fort.

Für ein RedHat oder CentOS-basiertes Linuxsystem ist die Installation von PostgreSQL mit ip4r vergleichsweise einfach durchführbar. Unter Windows ist PostgreSQL zwar verfügbar, allerdings ist die Installation des Datentypens ip4r undokumentiert. Kapitel 1.2 enthält beispielhafte Erläuterungen, um PostgreSQL mit ip4r unter CentOS zur Verwendung mit dem IPMapViewer zu installieren.

1.1 Virtual Appliance importieren und nutzen

Führen Sie die folgenden Schritte durch:

- Oracle VirtualBox herunterladen (http://www.virtualbox.org/)
- VirtualBox mit Standardeinstellungen installieren
- Die IPMapViewer Appliance von http://www.internet-

1 http://www.postgresql.org/
2 http://pgfoundry.org/projects/ip4r
3 Http://www.virtualbox.org

sicherheit.de/service/tools/ipmapviewer/ herunterladen und entpacken (z.B. mit 7-zip[4])

- VirtualBox starten
- Die Appliance in die VirtualBox importieren über den Menüpunkt "Datei" --> "Appliance importieren"
    - Button "Auswählen" --> *.ovf der IPMapViewer Appliance auswählen
    - Button "Weiter" und im folgenden Dialog die Appliance Import durch das Betätigen des Buttons "Abschließen" starten.

Nach dem Import ist die IPMapViewer Appliance in VirtualBox verfügbar (siehe Abbildung 1):

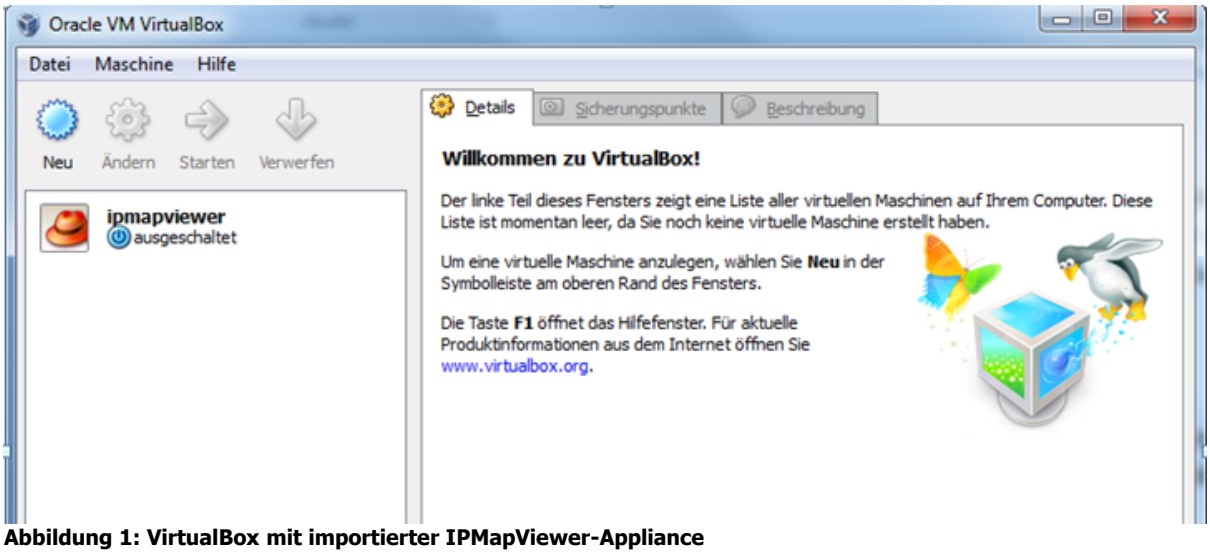

Abbildung 1: VirtualBox mit importierter IPMapViewer-Appliance

- Starten sie sie durch einen Doppelklick oder durch Betätigen des Buttons „Starten“
- Warten Sie, bis die Virtual Appliance vollständig hochgefahren ist. Dies ist daran zu erkennen, dass der Login-Prompt erscheint (vgl. Abbildung 2):

4 http://www.7-zip.org/

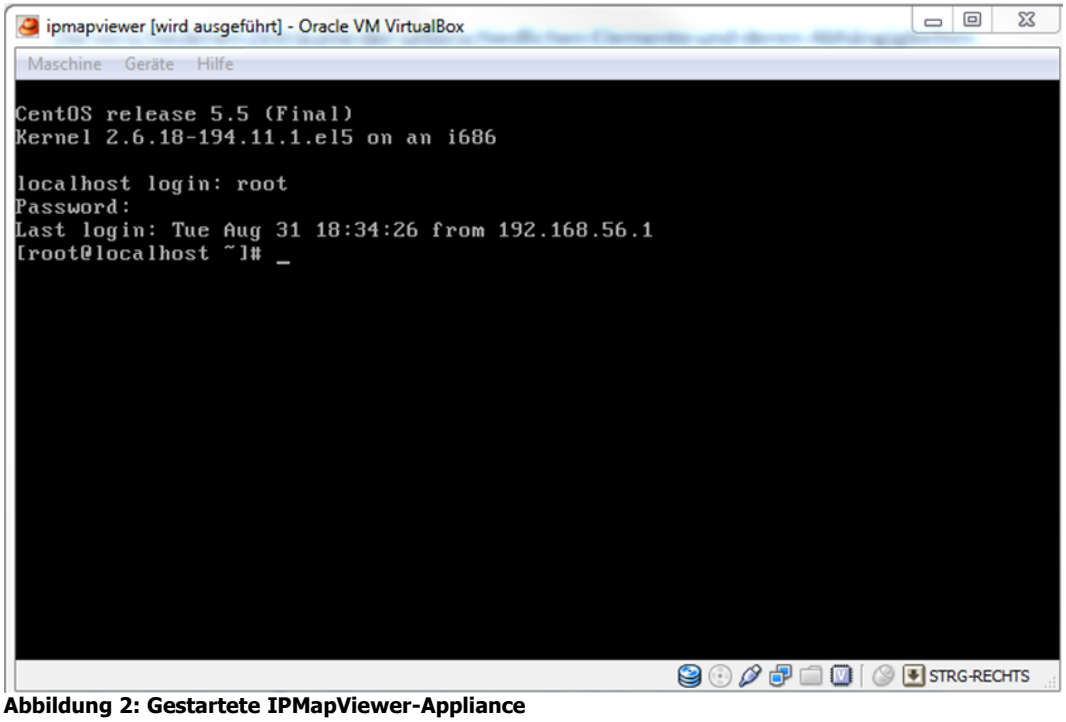

Abbildung 2: Gestartete IPMapViewer-Appliance

Im Grunde ist es für den weiteren Verlauf dieser Anleitung nicht notwendig, sich in die Appliance einzuloggen. Sollte dies jedoch erforderlich sein, hier die Zugangsdaten:

- Benutzername: root
- Passwort: ipmapviewer

In der Default-Konfiguration benutzt die Virtual Appliance das sog. Host-Only-Networking von Virtual Box.[5] Auf diese Weise ist die Virtual Appliance vor Zugriffen außer vom lokalen Host-PC geschützt. Andererseits erreicht die Virtual Appliance in der Regel auch das Internet nicht, dies ist aber für diese Anleitung auch nicht erforderlich.

Fahren Sie nun mit Kapitel 2 fort.

1.2 Installation von PostgreSQL mit ip4r

Dies sind die grundsätzlichen Schritte:

- PostgreSQL unter Linux installieren
- ip4r Datentyp herunterladen: http://pgfoundry.org/projects/ip4r
- ip4r Datentyp in PostgreSQL hinzufügen
- Datenbank anlegen, die aus dem IPMapViewer heraus verwendet wird

5 http://www.virtualbox.org/manual/ch06.html#network_hostonly

– Es wird die Berechtigung benötigt, Tabellen anlegen zu dürfen

Am Beispiel von CentOS werden die Kommandos gezeigt. Für CentOS steht PostgreSQL als zusätzliches Repository bereit. Dies wird wie folgt installiert:

```
# Testen, ob das RPM installiert werden kann
rpm -Uhv --test http://yum.pgsqlrpms.org/reporpms/8.4/pgdg-centos-8.4-2.noarch.rpm

# postgresql repository per RPM installieren
rpm -Uhv http://yum.pgsqlrpms.org/reporpms/8.4/pgdg-centos-8.4-2.noarch.rpm

# postgresql und Datentypen ip4r installieren
yum install postgresql-server ip4r

# PostgreSQL initialisieren
service postgresql initdb

# Falls PostgreSQL nicht gestartet wurde, starten
service postgresql status
service postgresql start

# README von ip4r anschauen
less /usr/share/doc/ip4r-1.04/README

# ip4r wird in diesem Fall für alle Datenbanken defaultmaessig installiert
psql -U postgres -f /usr/share/ip4r/ip4r.sql template1

# Die Konfiguration von PostgreSQL muss möglicherweise angepasst werden, z.B.
#   die Direktive listen = '*' abändern, damit der Dienst auf allen
#     Schnittstellen lauscht
vi /var/lib/pgsql/data/postgresql.conf

# Zugriff von dem Host erlauben, auf dem der IPMapViewer ausgeführt wird
vi /var/lib/pgsql/data/pg_hba.conf

# Benutzer und Datenbank anlegen
# alle eingerückten Schritte erfolgen als Benutzer postgres
[root@localhost ~]# su postgres

    # Datenbankbenutzer anlegen
    bash-3.2$ createuser ipmapviewer
    could not change directory to "/root"
    Shall the new role be a superuser? (y/n) n
    Shall the new role be allowed to create databases? (y/n) y
    Shall the new role be allowed to create more new roles? (y/n) n

    # Datenbank ipmapviewer anlegen
    bash-3.2$ createdb -U ipmapviewer ipmapviewer
    bash-3.2$ exit
```

```
# PostgreSQL neu starten
service postgresql restart

# Datenbank-Zugriff mit dem PostgreSQL-Konsolenclient testen
psql -U ipmapviewer ipmapviewer
```

2 Starten des IPMapViewers

Der IPMapViewer wird per Java WebStart[6] von der Webseite des Instituts für Internet-Sicherheit gestartet:

http://www.internet-sicherheit.de/service/tools/ipmapviewer/

2.1 Darstellen von IP-Adressen

Um den IPMapViewer verwenden zu können, ist es notwendig, dass die darzustellenden IP-Adressen in einer Tabelle in der PostgreSQL-Datenbank abgelegt sind. Eine solche Tabelle dient dem IPMapViewer als Datenquelle zum Generieren von IP-Maps.
Der IPMapViewer verfügt über eine Importfunktion, die das Anlegen einer Tabelle sowie das Hinzufügen von IP-Informationen automatisiert durchführt.
Die Struktur und der Inhalt der Tabelle, wird der Applikation durch eine simpel aufgebaute Textdatei vorgegeben. In der ersten Zeile dieser Textdatei stehen die Spaltennamen der Tabelle, jeweils durch einen Tabulator voneinander getrennt. In den folgenden Zeilen befinden sich die Daten der Tabellenzeilen, auch durch jeweils einen Tabulator voneinander getrennt.

Zur Verdeutlichung des Aufbaus dieser Datei folgt ein Beispiel:
Die Textdatei für eine Tabelle mit den zwei Spalten „ipaddress“ und „iptype“ und drei beispielhaften Datensätzen sieht folgendermaßen aus:

```
ipaddress<TABULATOR>iptype
10.10.10.10<TABULATOR>type A
20.20.20.20<TABULATOR>type B
30.30.30.30<TABULATOR>type A
```

6 Hierzu wird eine installierte Java Runtime Environment benötigt, etwa von http://www.oracle.com/technetwork/java/

Anstelle von einzelnen IP-Adressen können auch IPv4-Adressbereiche in der CIDR-Schreibweise[7] verwendet werden.

Eine Textdatei `iptable.txt` mit beispielhaften IP-Adressdaten können Sie unter der Internetadresse
http://www.internet-sicherheit.de/service/tools/ipmapviewer/
herunterladen. Diese Textdatei enthält IP-Adressen der NiX Spam Blacklist (http://www.dnsbl.manitu.net/download/nixspam-ip.dump.gz). Die IP-Adressen wurden beispielhaft typisiert. Die Typisierung kann in einer IP-Map durch farbliche Kennzeichnung dargestellt werden.

Die Datei kann mithilfe des IPMapViewers in die Datenbank importiert und danach mit dem IPMapViewer visualisiert werden.
Gehen Sie dazu wie folgt vor:
Starten Sie den IPMapViewer über die folgende Internetadresse: http://www.internet-sicherheit.de/service/tools/ipmapviewer/

Nun muss zunächst eine Datenquelle (Datasource) angelegt werden. Dies wird im Datasource-Management des IPMapViewers vorgenommen, welches über das Menü „IPMap“ → „Datasources“ oder alternativ über das Tastenkürzel „Strg + D“ geöffnet wird. Über den Button „Add“ wird ein Dialog zum Anlegen einer Datenquelle geöffnet:

7 http://de.wikipedia.org/wiki/CIDR

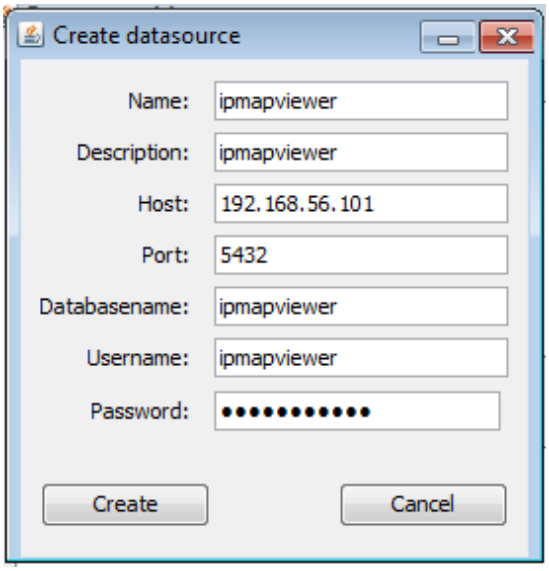

Abbildung 3: Dialog zum Anlegen einer Datenquelle

Hier geben Sie die Zugangsdaten zu Ihrer angelegten Datenbank an. Der Name und die Beschreibung (Description) kann dabei frei vergeben werden. Sie dienen lediglich als Hilfestellung zu Ihrer persönlichen Übersicht. Für diese Anleitung nehmen wir als Name `ipmapviewer`. Unter Host muss bei der Verwendung der Appliance die IP-Adresse der Appliance eingetragen werden, ansonsten Hostname oder IP-Adresse des PostgreSQL-Servers. Die IP-Adresse der Appliance wird per DHCP vergeben und ist somit dynamisch, in den meisten Fällen ist es jedoch einfach die erste IP-Adresse des DHCP-Adressbereichs 192.168.56.101.[8] Der Standardport von PostgreSQL-Datenbanken ist 5432. Der Benutzername sei `ipmapviewer` und das Passwort ist bei Verwendung der Appliance beliebig.

Haben Sie den Dialog ausgefüllt, so speichern Sie die Informationen über das Betätigen des Buttons „Create“. Die Datenquelle ist nun im Datasource-Management-Dialog aufgeführt. Markieren Sie sie mit der Maus und starten Sie die Importfunktion über den Button „Import table from *.txt“.
Wählen Sie in dem sich öffnenden Dateiauswahl-Dialog die o.g. Textdatei, welche die IP-Informationen enthält, aus. Es öffnet sich der Import-Dialog:

8 Die IP-Adresse der Appliance eruieren Sie, indem Sie sich auf der Konsole als root einloggen mit dem Passwort `ipmapviewer` und den Befehl `ifconfig eth0` eingeben.

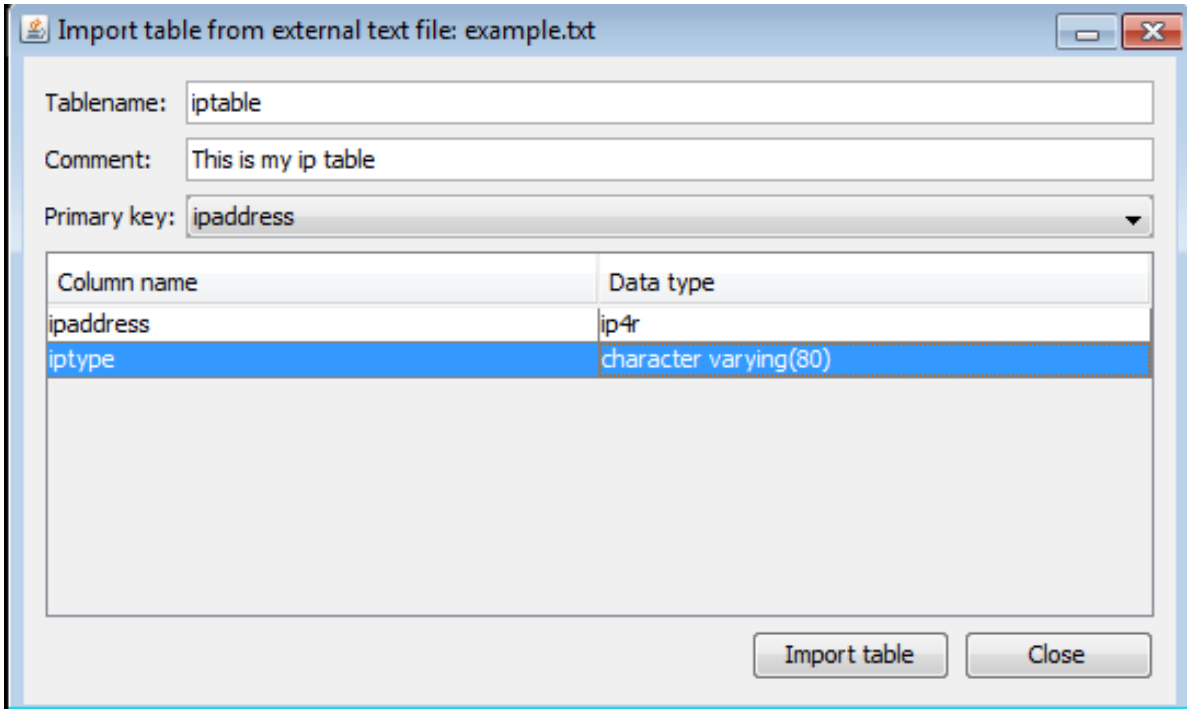

Abbildung 4: Der Dialog zum Importieren einer IP-Tabelle

In diesem Dialog geben Sie den Namen der Tabelle an, die in Ihrer Datenbank erzeugt werden soll. Zudem kann optional ein Kommentar für die Tabelle vergeben werden. In dem Kombinationsfeld „Primary key“ werden alle Spaltennamen aus der Textdatei angezeigt. Über dieses Kombinationsfeld wird der Primärschlüssel der Tabelle, der einen Datensatz eindeutig identifiziert, festgelegt. Dieser ist in den meisten Fällen die IP-Adresse, weshalb die IP-Adress-Spalte in dem Kombinationsfeld entsprechend voreingestellt ist. In der Tabelle im unteren Bereich des Dialogs findet die Zuordnung von Spalte und Datentypen statt. Wählen Sie für die IP-Adress-Spalte den ip4r-Datentypen aus. Enthält die Textdatei weitere Spalten, z.B. zur Typisierung der IP-Adressen, so wählen Sie für diese den Datentypen „character varying(80)“ aus. Die Spalten dürfen eine maximal 80 Zeichen lange Zeichenkette enthalten.
Über den „Import table“-Button wird der Importvorgang abgeschlossen:
Die Tabelle wird den Angaben entsprechend erstellt und mit den IP-Informationen aus der Textdatei gefüllt. Dies kann je nach Anzahl der Datensätze einen Moment dauern.
Um sich die IP-Adressen in Form einer IP-Map anzeigen lassen zu können, muss nun noch eine Sicht (View) auf diese IP-Tabelle erstellt werden. Auf Basis einer solchen View

wird festgelegt, welche Spalten in einer IP-Map dargestellt werden sollen und welche Aufgabe diese Spalten haben. Für eine Datenquelle können beliebig viele Views auf beliebig unterschiedliche Tabellen angelegt werden.

Markieren Sie Ihre Datenquelle und klicken Sie auf den Button „Manage views“. Es öffnet sich ein Dialog, in dem Sie den Button „New view“ betätigen, um eine neue View anzulegen. Der Dialog sieht nun folgendermaßen aus:

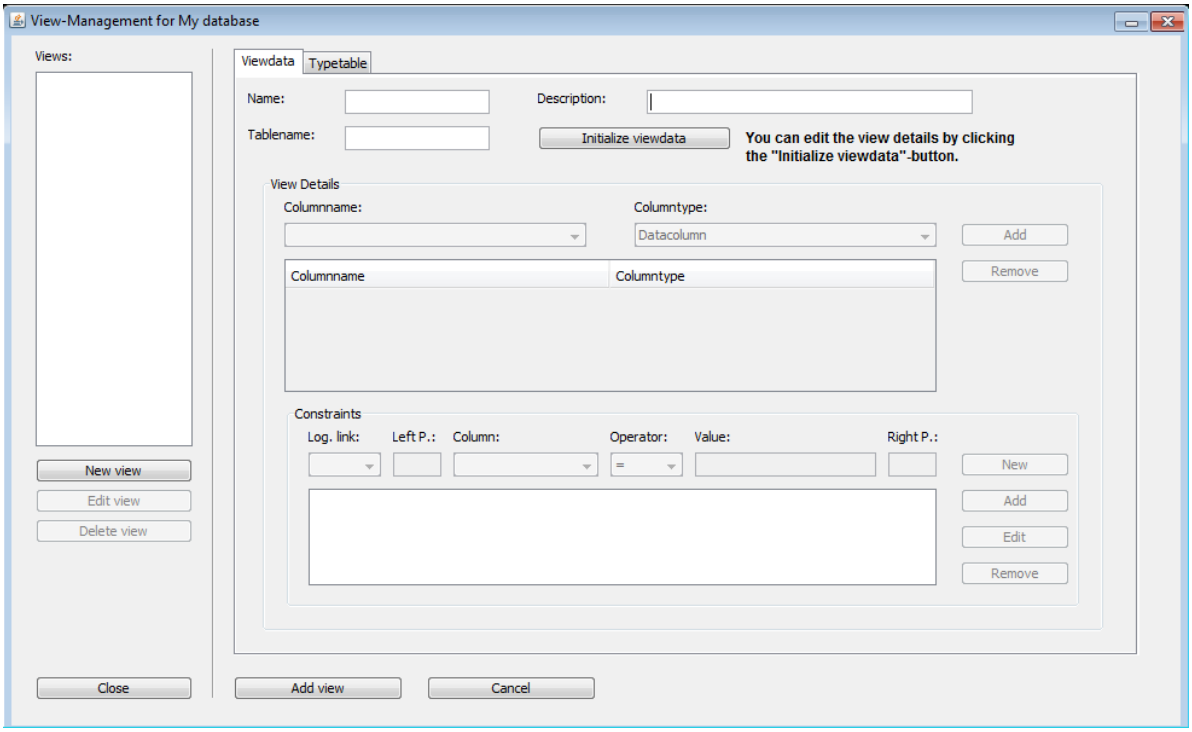

Abbildung 5: Dialog zur Erstellung einer View

Für die View können Sie einen beliebigen Namen und eine optionale Beschreibung vergeben. In dem Textfeld „Tablename“ muss der Tabellennamen, den Sie bei dem Import der IP-Informationen angegeben haben, eingetragen werden. Durch das Betätigen des Button „Initialize viewdata“ werden die Spaltennamen aus der angegebenen Tabelle ausgelesen. Diese können Sie nun durch die Kombinationsfelder auswählen. Wählen Sie als Spaltennamen (Columnname) zunächst die IP-Adress-Spalte aus. Im Kombinationsfeld „Columntype“ wird nun angegeben, welche Aufgabe diese Spalte hat. In dem Fall der IP-Adress-Spalte wird „Datacolumn“ ausgewählt. Dadurch wird indiziert, dass diese Spalte die Daten (in Form von IP-Adressen), die dargestellt

werden sollen, beinhaltet. Betätigen Sie den Button „Add“, um diese Spaltenkonfiguration zu speichern. Sind die IP-Adressen typisiert, so ist es möglich die IP-Adressen gruppiert nach diesen Typen darstellen zu lassen. Dazu fügen Sie eine weitere Spaltenkonfiguration hinzu. Wählen Sie dazu im Kombinationsfeld „Columnname“ den Namen der Spalte aus, welche die Typisierungsinformationen enthält. Im Kombinationsfeld „Columntype“ wählen Sie den Eintrag „Groupingcolumn“ aus. Speichern Sie die Spaltenkonfiguration durch Betätigen des Buttons „Add“.
Die folgende Abbildung stellt dar, wie Ihre Eingaben ungefähr aussehen könnten:

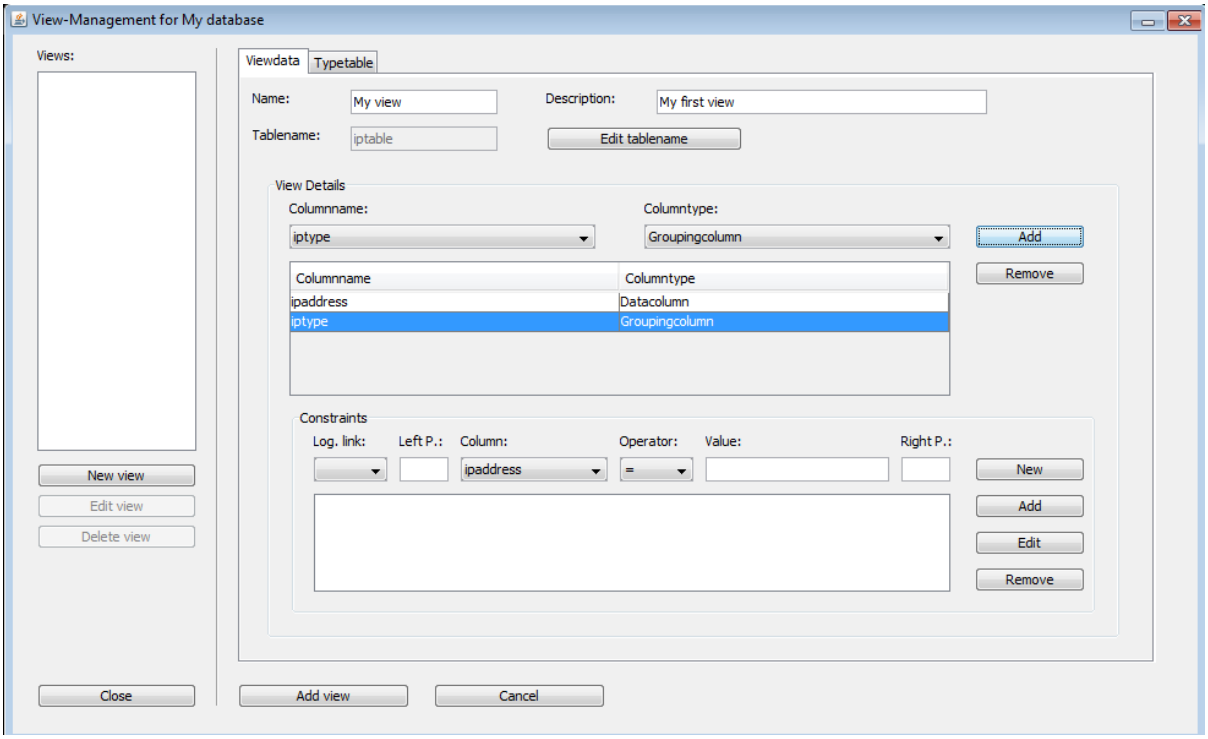

Abbildung 6: Erstellung einer View (Beispiel)

Betätigen Sie den Button „Add view“, um die View zu speichern. Schließen Sie nun den Dialog. Die View ist nun im Datasource-Management-Dialog aufgeführt. Markieren Sie die View und betätigen Sie den Button „Show ip-map“. Daraufhin öffnen sich zwei Dialoge:

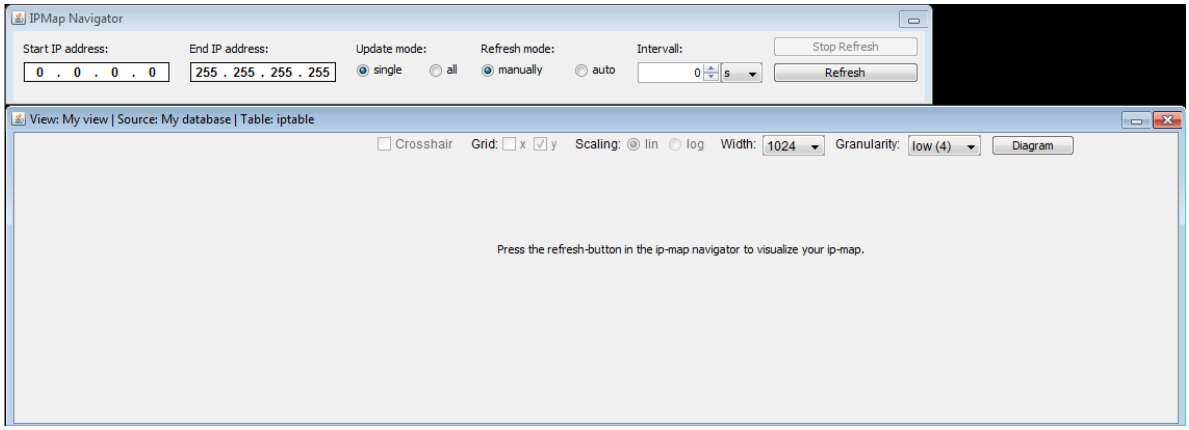

Abbildung 7: IPMap Navigator und leere IP-Map

Im IPMap Navigator können Sie nun angeben, welchen IP-Adressraum in der IP-Map dargestellt werden soll. Standardmäßig ist dort der gesamte IP-Adressraum von 0.0.0.0 bis 255.255.255.255 eingetragen. Durch Betätigen des „Refresh“-Buttons wird die IP-Map geladen und dargestellt:

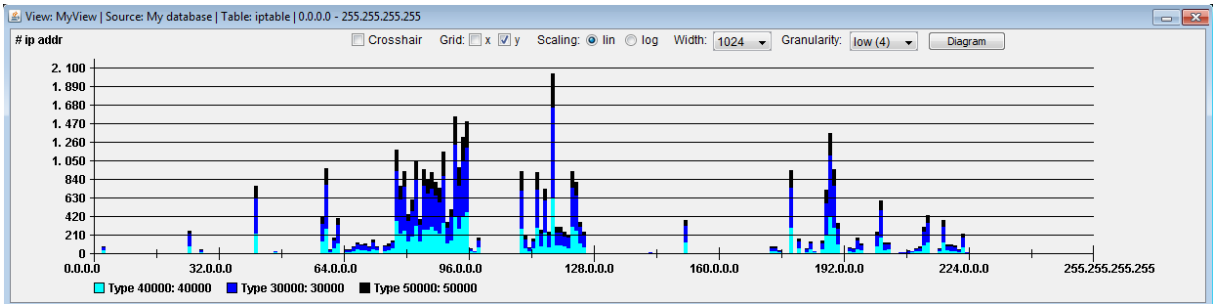

Abbildung 8: Beispielhafte IP-Map

In der IP-Map haben Sie die Möglichkeit weitere Hilfslinien einblenden zu lassen und zwischen der linearen und logarithmischen Darstellung zu wechseln. Auch die Breite und Granularität der IP-Map in Pixeln kann angegeben geändert werden. Klicken Sie auf einen IP-Bereich, so werden detaillierte Informationen zu diesem Bereich in Form einen Tooltips eingeblendet.

Innerhalb der IP-Map kann in Bereiche hineingezoomt werden. Markieren Sie dazu den gewünschten Bereich bei gedrückter linker Maustaste. Es wird ein Rechteck aufgespannt, welches den IP-Bereich umfasst, der beim Loslassen der linken Maustaste vergrößert dargestellt wird.

Anhang

Abbildungsverzeichnis

Abbildung 1: VirtualBox mit importierter IPMapViewer-Appliance....3
Abbildung 2: Gestartete IPMapViewer-Appliance....4
Abbildung 3: Dialog zum Anlegen einer Datenquelle....8
Abbildung 4: Der Dialog zum Importieren einer IP-Tabelle....9
Abbildung 5: Dialog zur Erstellung einer View....10
Abbildung 6: Erstellung einer View (Beispiel)....11
Abbildung 7: IPMap Navigator und leere IP-Map....12
Abbildung 8: Beispielhafte IP-Map....12