DynFire

An Architecture for Dynamic Firewalling

Alexander Vensmer
Alexander.Vensmer@ikr.uni-stuttgart.de
28.11.2011

Universität Stuttgart
Institut für Kommunikationsnetze
und Rechnersysteme (IKR)
Prof. Dr.-Ing. Andreas Kirstädter

Gliederung

- **Motivation**
- **DynFire – Architektur**
- **Herausforderungen**
- **Erste Ergebnisse**
- **Zusammenfassung**

Future Internet

Zunehmende Vielfalt in der Protokollwelt

- Netzprotokolle (Proxy Mobile IP, HIP, Shim6, ...)
- Verschlüsselungs-Mechanismen
- Authentifizierungs-Mechanismen (EAP-Mechanismen, ...)

Wachsende Flexibilität

- Nutzer wollen von "überall" sicher auf Ihre Ressourcen zugreifen
- Nutzer wollen verschiedene Endgeräte verwenden

Neuartige Netzteilnehmer

Internetfähige Steuerungsgeräte

- Klimaanlagen
- CNC-Maschinen
- Smart Meter

Motivation

Sicherer Betrieb von internetfähigen Legacy-Geräten

- Funktionieren nur mit bestimmter Betriebssystem-Version
- Nutzen proprietäres Betriebssystem ohne Erweiterungsmöglichkeit
- Hersteller hat Support eingestellt

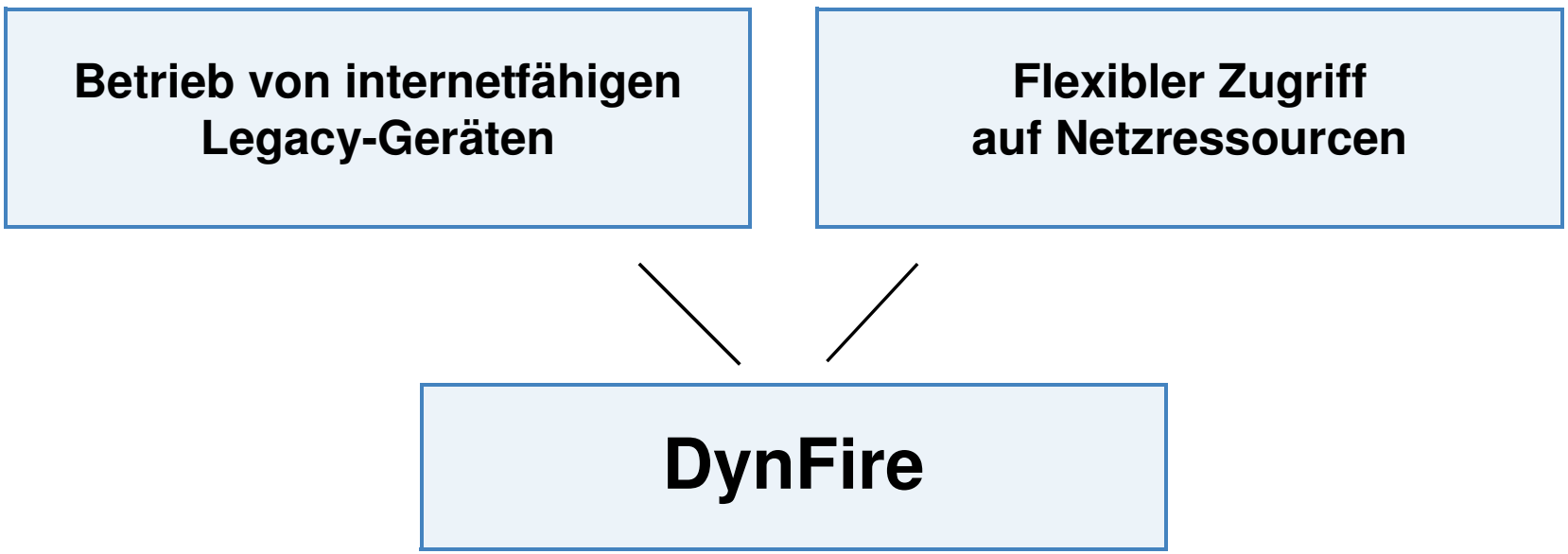
Wie können diese Geräte zukünftig sicher genutzt werden?

Motivation

Flexibler Zugriff auf Netzressourcen unter Gewährleistung der Netzsicherheit

Feingranulare Rechtevergabe

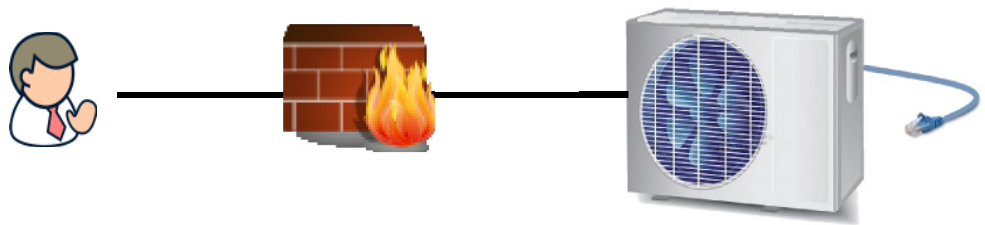
- Nutzerbezogen
- Ortsbezogen
- Zeitbezogen



Idee

Nutzung externer Sicherheitsmechanismen

→ Zugriffskontrolle auf Netzressourcen per dynamisch konfigurierbarer Firewalls

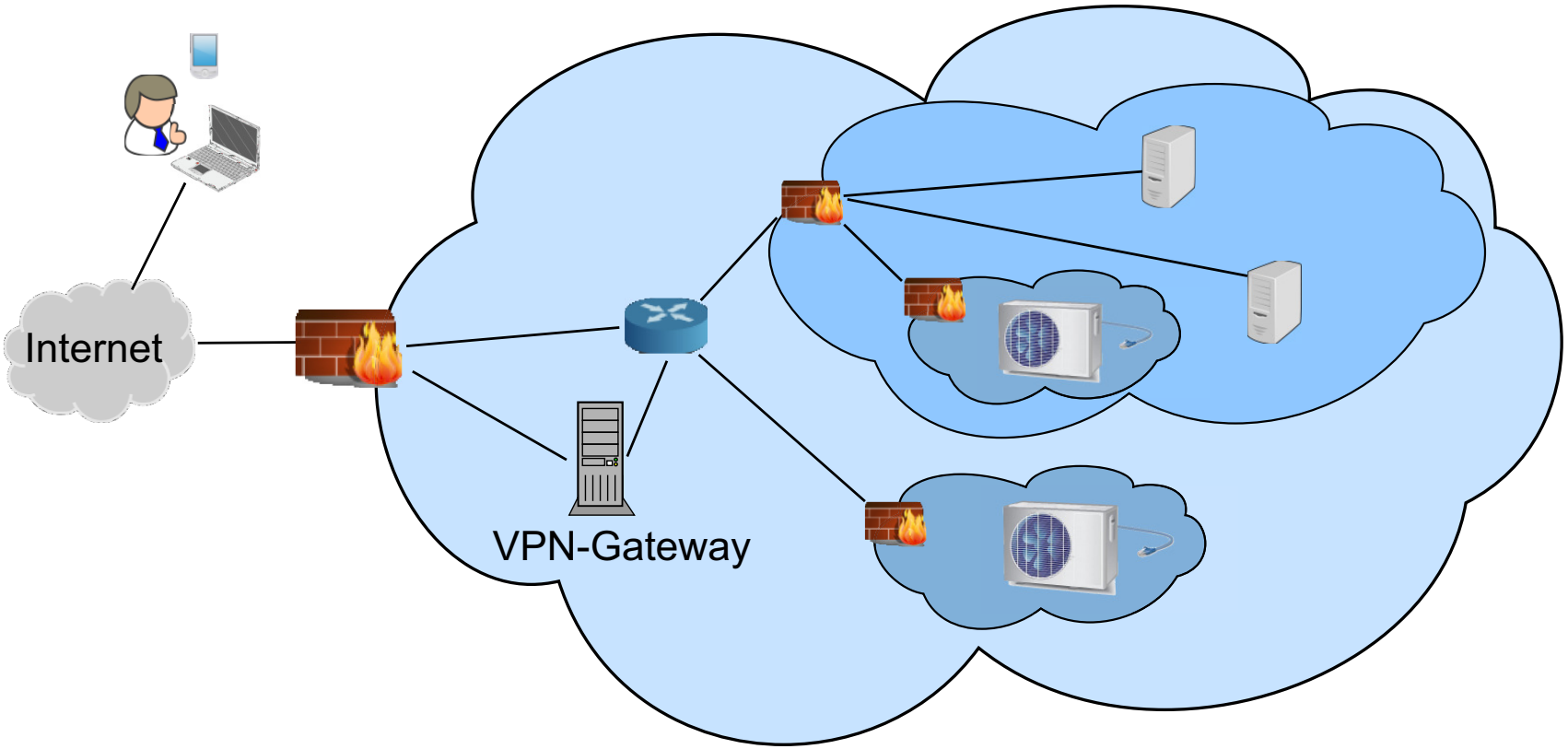


Nutzer Firewall Legacy-Gerät

Firewallbasierte Sicherheit

Szenario

Struktur aktueller Netze

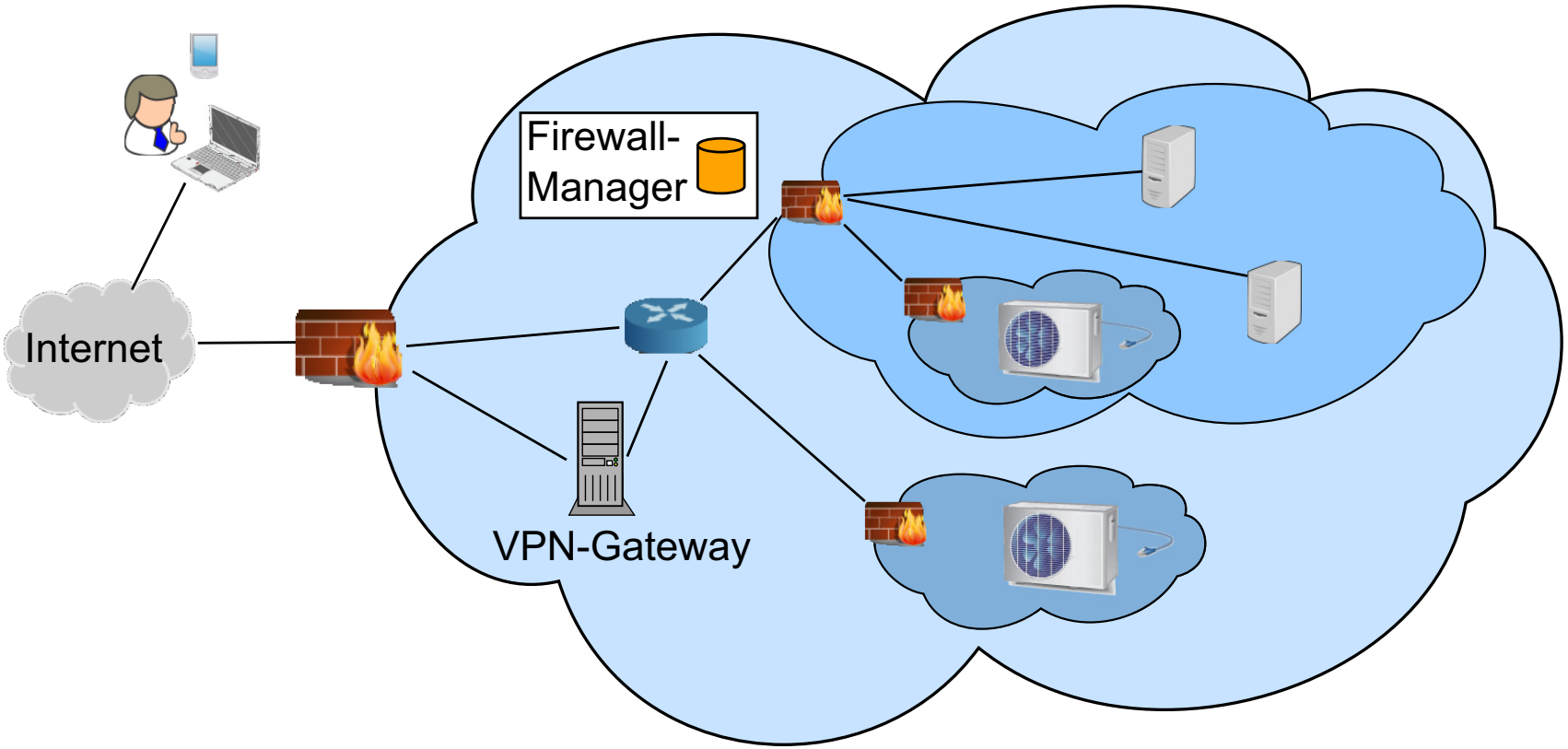


Bisherige Lösungen basieren auf statischer Addressvergabe

Feine Granularität der Zugriffsrechte kann nur aufwendig erreicht werden

Szenario

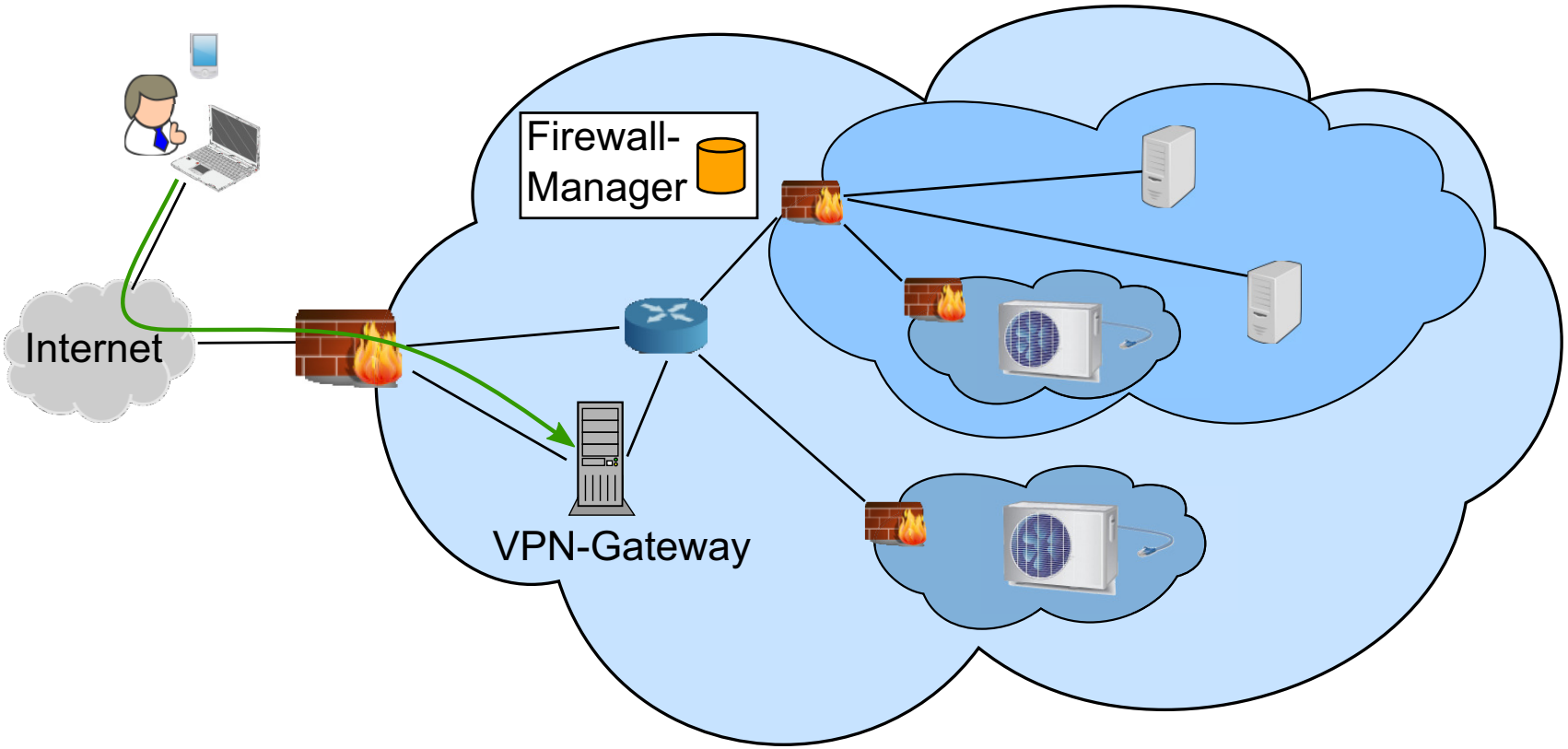
Lösungsansatz DynFire



Erweiterung des Netzes um die Instanz "**Firewall-Manager**"

Szenario

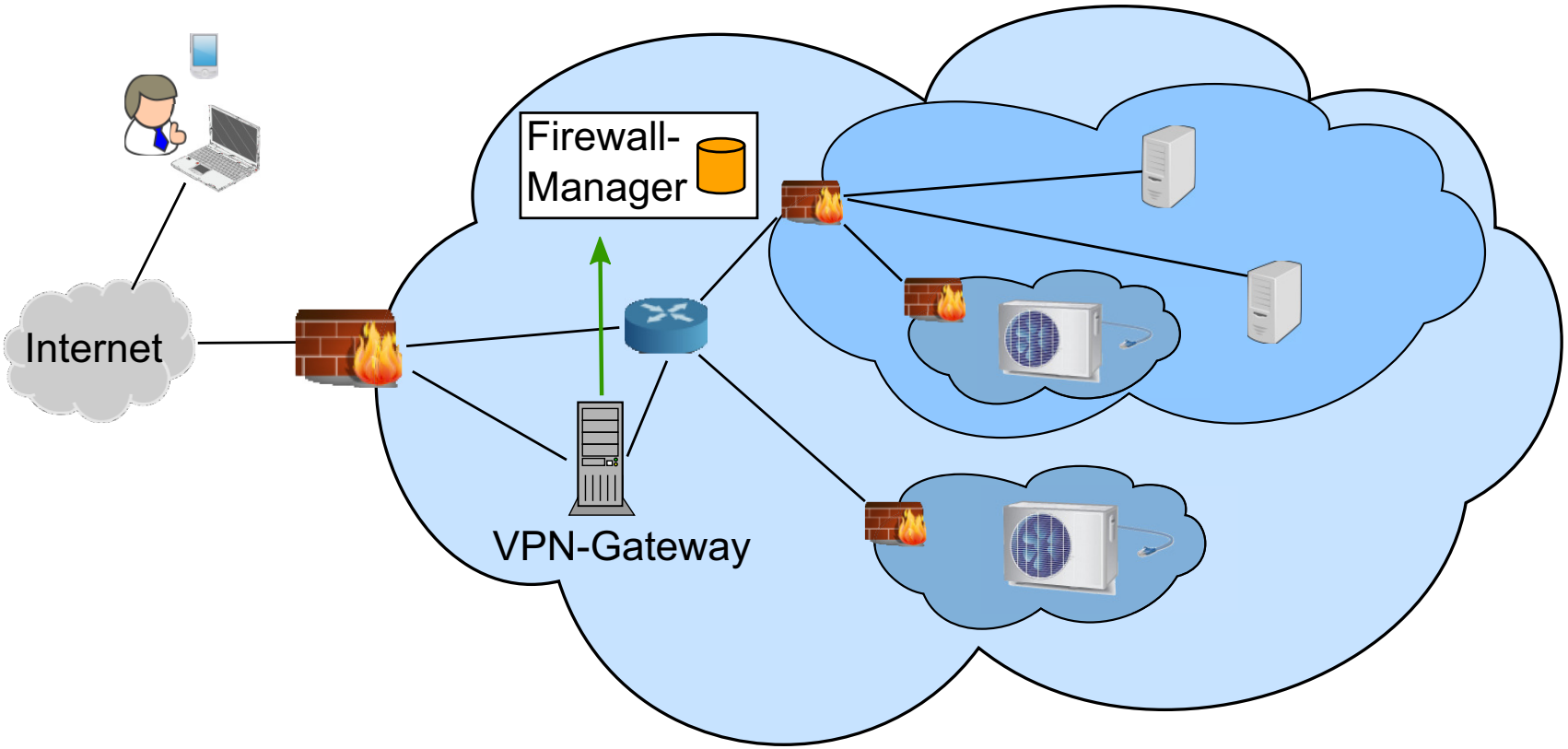
Lösungsansatz DynFire



Nutzer meldet sich am VPN-Gateway an und bekommt eine IP-Adresse zugewiesen

Szenario

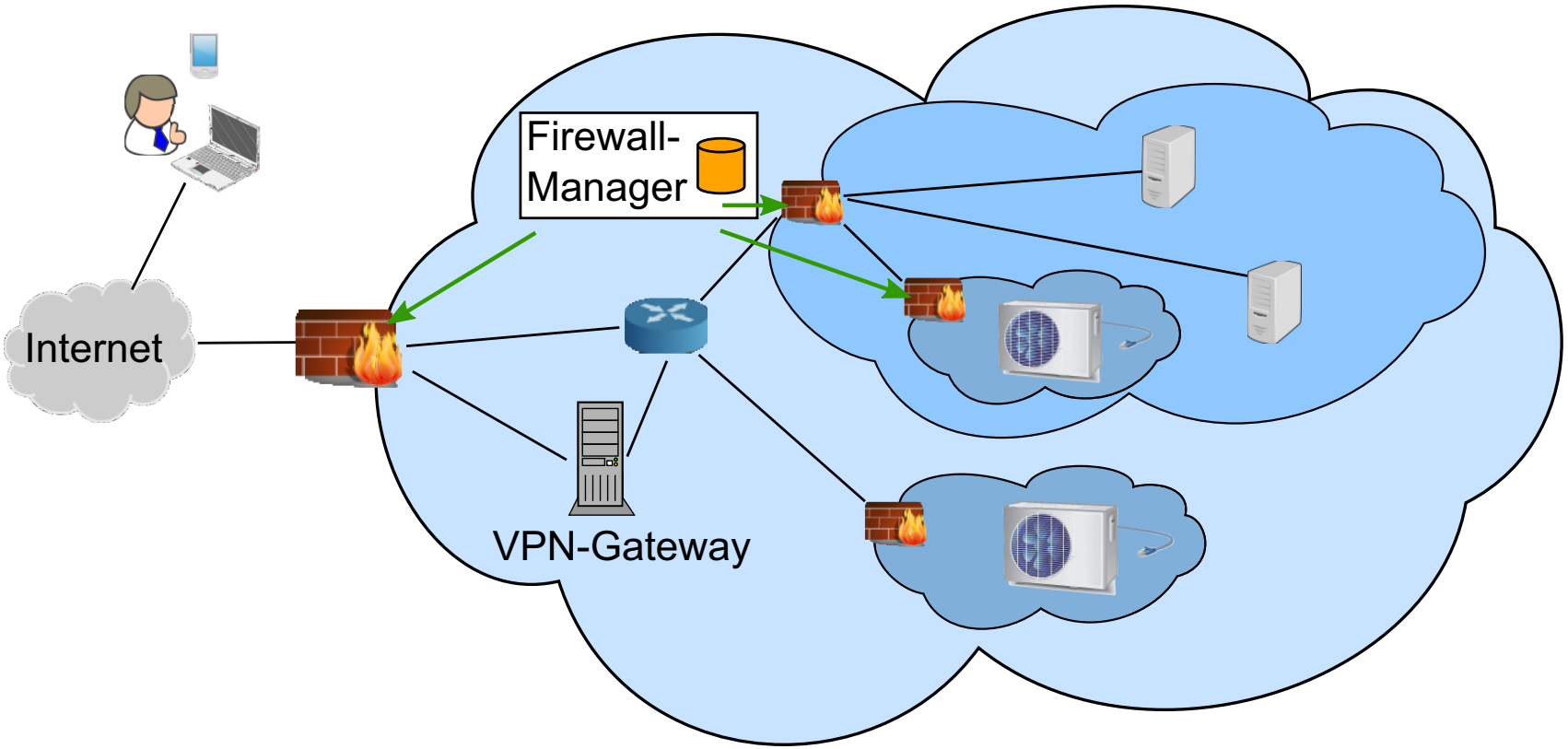
Lösungsansatz DynFire



Zugewiesene IP-Adresse und Nutzer werden dem Firewall-Manager mitgeteilt

Szenario

Lösungsansatz DynFire

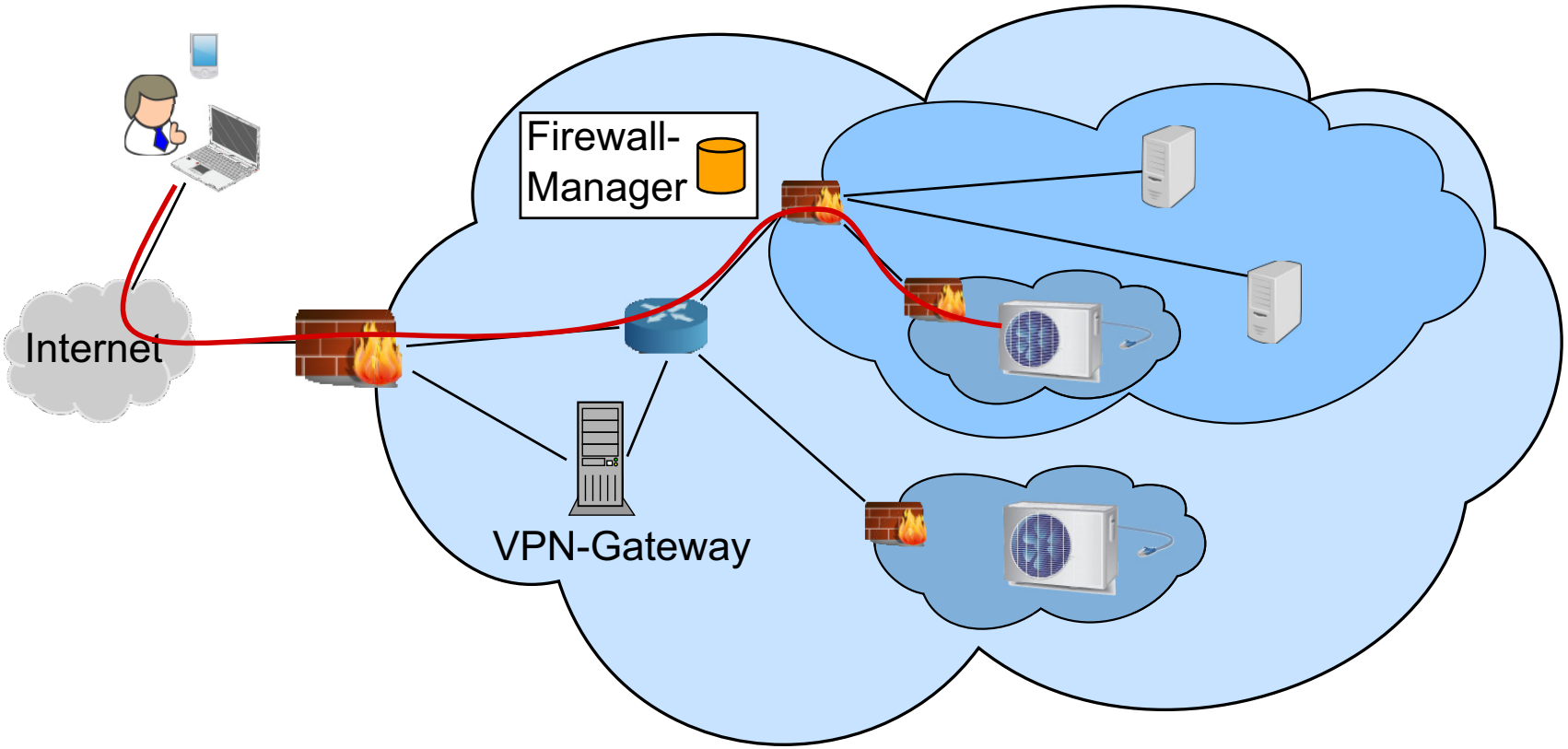


Firewallmanager

- Kennt die Ressourcen, auf die ein Nutzer zugreifen darf
- Kennt die Netz-Topologie
- Konfiguriert die Firewalls entlang der betroffenen Pfade

Szenario

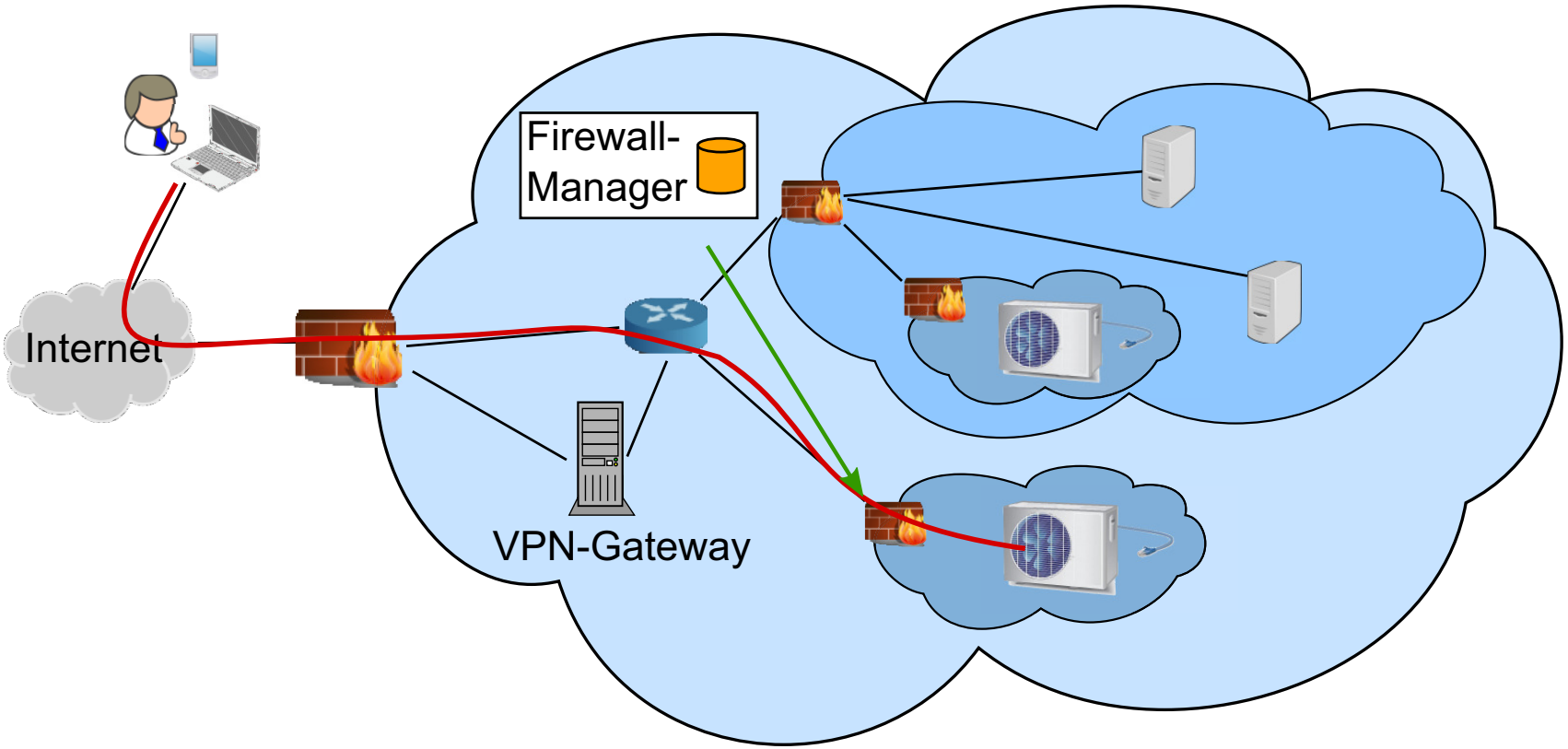
Lösungsansatz DynFire



Der Nutzer kann jetzt auf die für ihn freigebenen Netzressourcen zugreifen

Szenario

Lösungsansatz DynFire



Alle Pfade auf dem Weg zu den benötigten Ressourcen werden freigeschaltet

Herausforderungen

Skalierbarkeit der Architektur

- Verschiedene Anzahl an Loginvorgängen
- Verschiedene Anzahl an vorhandener Firewalls

Geeignete Schnittstellen zur Kommunikation

- Zwischen Netzanschlusspunkt und Firewall-Manager
- Zwischen Firewall-Manager und Firewalls

Protokollierung und Vorfallsbehandlung

- Nachvollziehbarkeit
- Reaktion auf Fehlerfälle

Funktionale Komponenten

Policy-Framework

- Wie werden die Zugriffsrechte an Nutzer delegiert
- Wer darf Zugriffsrechte vergeben

Topologie-Erkennung

- Wie wird die Topologie festegestellt
- Welche Firewalls müssen freigeschaltet werden
- Was passiert bei Link-Ausfälle

Policy-Framework

Anforderungen

Defintion der Nutzerrechte

Zusammenhang zwischen Nutzer und seinen Zugriffsrechten

→ Gruppenbasiert

Definition der Administrationsrechte

- Wer darf Zugriffsrechte erstellen
- Wie können Verantwortungen delgiert werden

  Dezentralisierung der Verantwortung

Bedienoberfläche

- Web-basiert
- Dezentraler Zugriff

Policy-Framework

Kern-Elemente

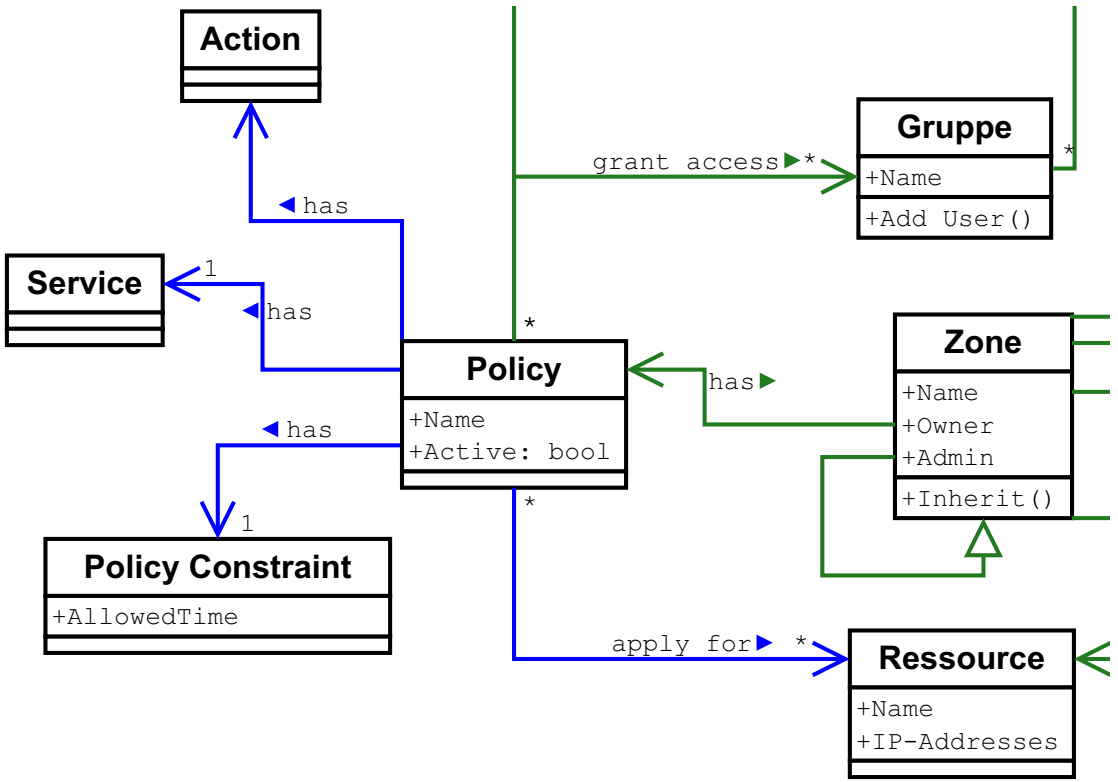
Policy verknüpft

Gruppe, Nutzer, Service, IP-Adresse, Policy-Constraints

Zone

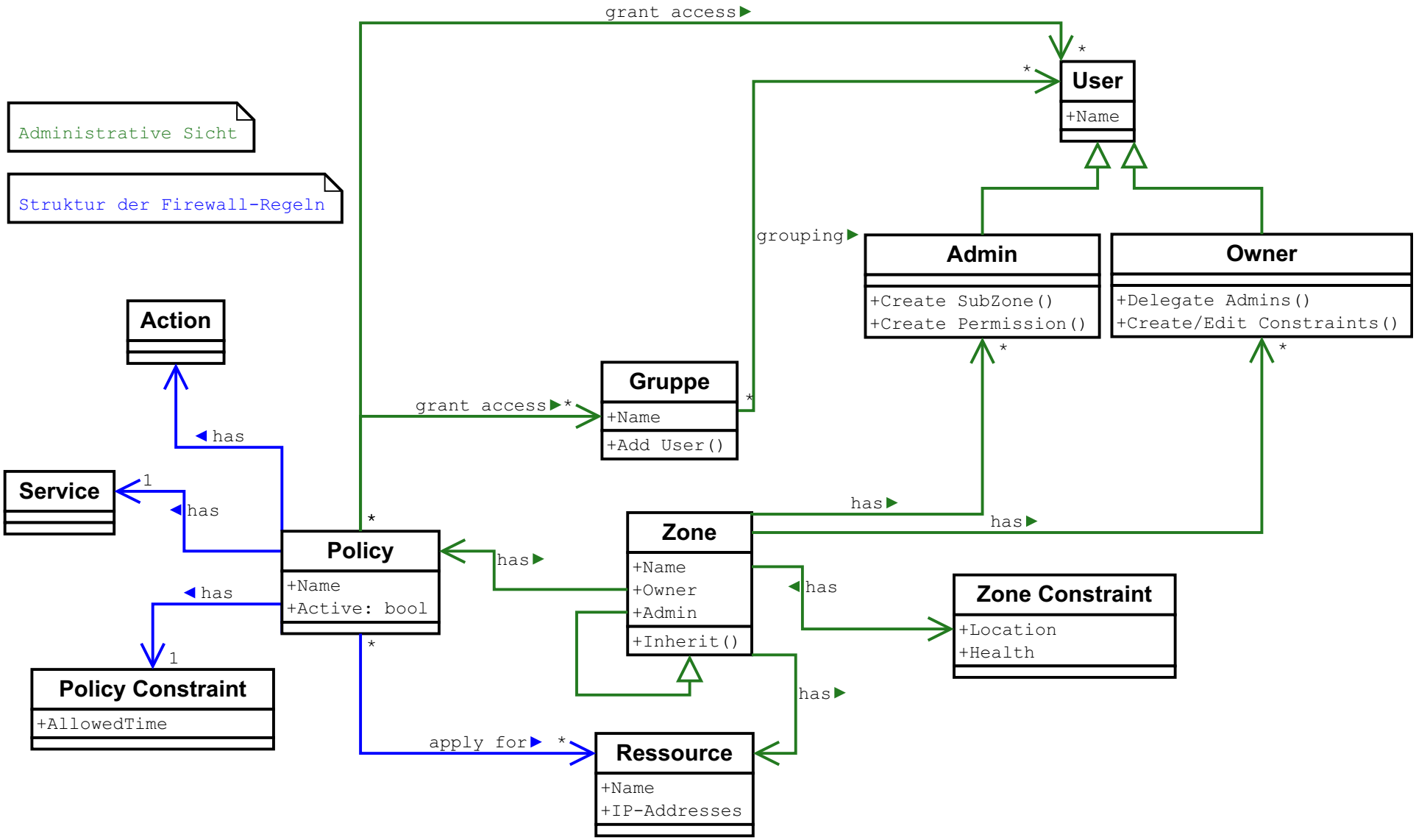
- IP-Addressbereich
- Gruppenstruktur
- Policies
- Sub-Zonen

→ Ermöglicht verteilte Administration



Policy-Framework

Überblick



DynFire

Übersicht

Projektpartner

- Astaro GmbH & Co. KG – a Sophos company
- Fraunhofer Gesellschaft – Institut für Sichere Informationstechnologie
- Universität Stuttgart
  - Rechenzentrum
  - Institut für Kommunikationsnetze und Rechnersysteme

Zeitraum

Mai 2011 - Mai 2013

Förderung

Bundesministerium für Bildung und Forschung (Förderkennzeichen 01BY1151)

Zusammenfassung und Ausblick

DynFire – Architektur

- Netzsicherheit
- Unterstützung von Flexibilität der Nutzer
- Netzbasierte Sicherheit
- Nutzerbasiertes Freigeben
- Nutzung bestehender Infrastruktur

DynFire ermöglicht sicheren Betrieb und sicheres Zugreifen auf IP-kommunikationsfähige Steuerungsgeräte und Netzwerkressourcen

Ausblick

- Prototypische Implementierung der Basisarchitektur bis Mai 2012
- Einsatz und Bewertung der Funktionalität im Datennetz der Uni Stuttgart
- Weitergehende Mechanismen (Topologieerkennung, Optimierung der Firewall-Provisionierung) in Arbeit
- Bewertung mit Verbesserungsoptionen in Arbeit

Backup

Administrierbarkeit der Firewalls

Realisierung

SIMCO Protokoll (IETF-RFC 4540)

- Middleware-Kommunikation
- Transport von Firewall-Regeln

Implementierung

Simco-Server auf einem Juniper-Router