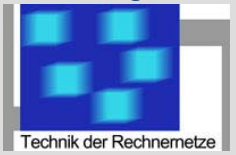

Universität Duisburg-Essen




Communications

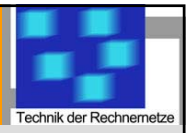
# Paketfilternetze

**Birger Tödtmann**
**Lehrstuhl Technik der Rechnernetze**
**Institut für Experimentelle Mathematik**
**Universität Duisburg-Essen**

A Siemens project supported by BMBF

SIEMENS


## Übersicht




- Motivation und Hintergrund
- Konzept der Paketfilternetze
- Verteilungsmethodik
- Implementierung/Prozessablauf
- Zusammenfassung, Ausblick

## Paketfilter: Motivation

Technik der Rechnernetze

- Absicherung von Kommunikationsbeziehungen traditionell durch Authentisierung, Integritätssicherung, Verschlüsselung
  - Generisch: IPSec, TLS
  - Applikationsspezifisch: SNMP (→ v1: communities, v2/v3: USM, …) Telnet (→ SSH), NFS (→ v2/v3: Kerberos, v4: …)
- Paketfilter dennoch sinnvoll zum Schutz vor
  - Angriffen auf Protokollebenen, die solchen Schutzmechanismen vorgelagert sind (z.B. Xmas-Tree im TCP bei Verwendung von TLS)
  - Angriffen auf die Verfügbarkeit

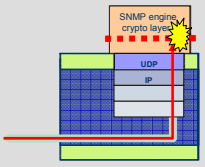




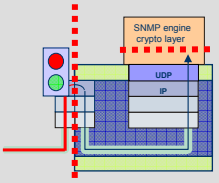
## Motivation: Beispiel Denial of Service

Technik der Rechnernetze

- Management von Netzknoten über SNMPv3 (UDP)
  - Für Authentisierung notwendig: Manager erfragt authoritative EngineID vom Agenten
  - Angreifer kann Agenten (Router) mit SNMP-Anfragenachrichten überfluten
  - SNMP-Engine des Agenten antwortet nicht mehr, Agent ist nicht mehr administrierbar



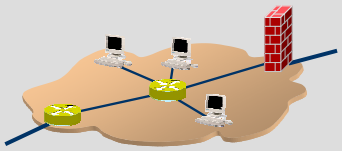

  - Gegenmaßnahme: SNMP nur von vertrauenswürdigen IP-Quelladressen und aus vertrauenswürdigen "Richtungen" erlauben
    → Paketfilter

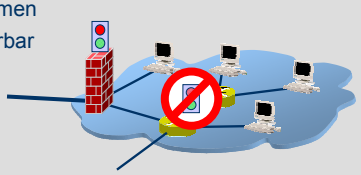


## Firewalls: Probleme

Technik der Rechnernetze

- Einsatz von Paketfiltern traditionell in sog. *Firewalls*
  - Hintergrund organisatorisch/wirtschaftliche Effizienz
  - Höhere Performance der Filtermechanismen
  - Filterrichtlinien waren besser administrierbar





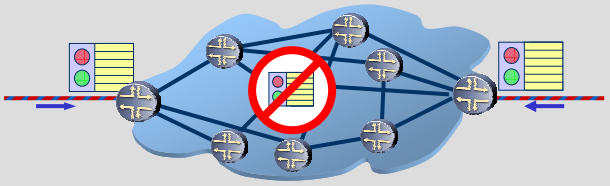
- Problem: Firewalls benötigen klar definierte, wenige Netzränder
  - Trend: Zahl der Kopplungspunkte zu Fremdnetzen nimmt zu
  - Trend: Netzadministration/organisation zunehmend inhomogen
  - Trend: Netzrand zunehmend dynamisch
  - Außerdem: traditionelle Motivation weniger wichtig

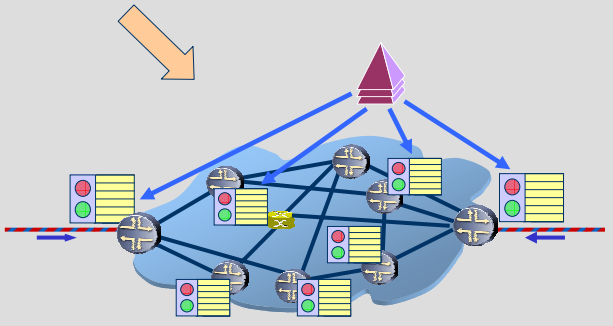




## Lösung: Verteilung der Paketfilter

Technik der Rechnernetze



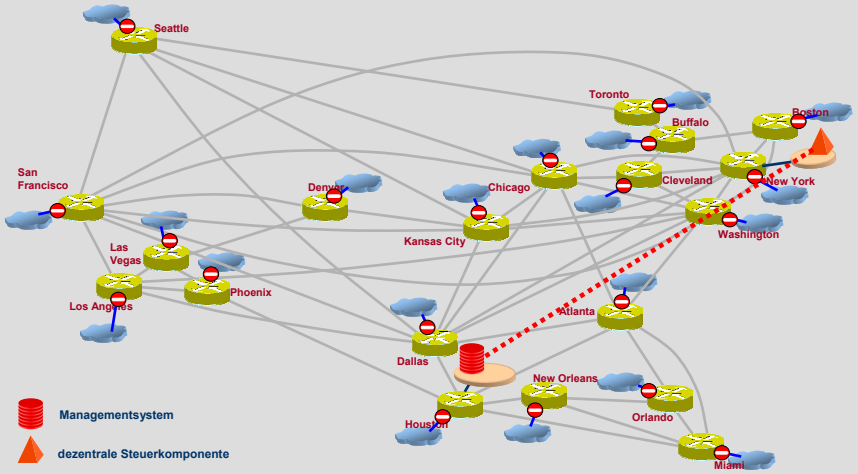


APCP — Access Policy Configuration Point

APEP — Access Policy Enforcement Point

# Beispielszenario

- Netzbetreiber verbindet Städte und Regionen: Anschluss von Fremdnetzen
- Nutzung von Netzmanagementsystemen und abgesetzten Steuerkomponenten



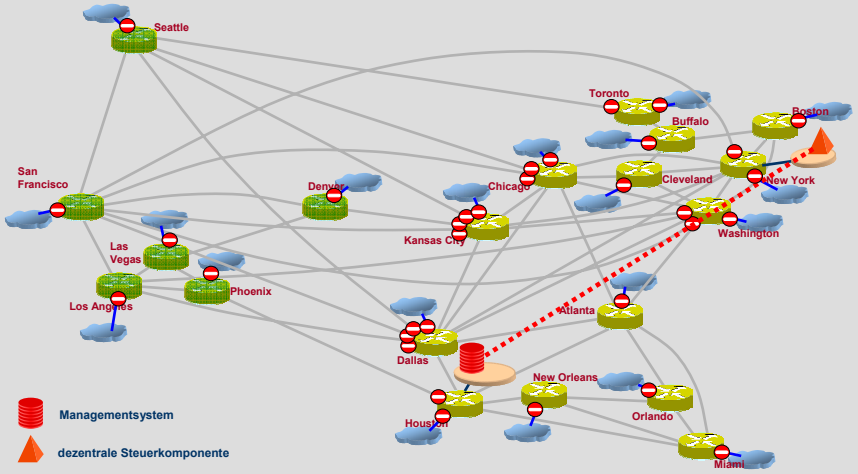

Birger Tödtmann (btoedtmann@ieee.org) PaketRennetze ITG-Workshop 2005 Folie 7



KING
Technik der Rechnernetze

# Beispielszenario

- Durchsetzung einheitlicher Sicherheitsrichtlinien trotz gemeinsamer Nutzung von Ressourcen nicht unbedingt gegeben: Netzranddefinition problematisch

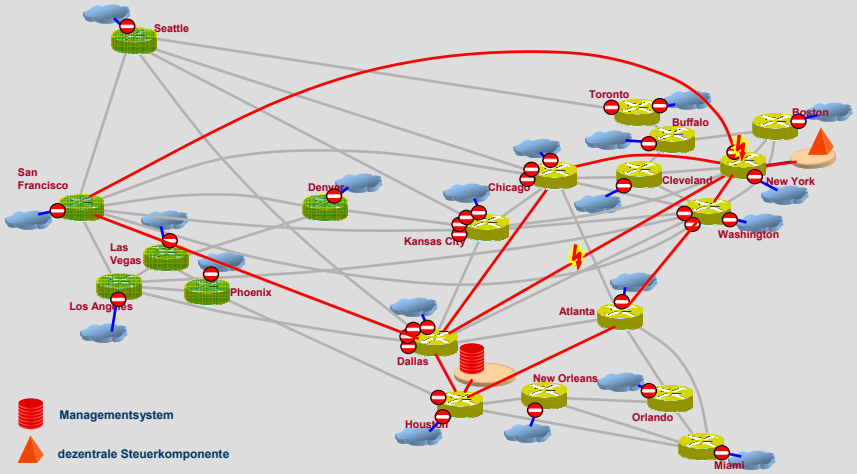



Birger Tödtmann (btoedtmann@ieee.org) PaketRennetze ITG-Workshop 2005 Folie 8

A Siemens project supported by BMBF
Communications
SIEMENS

# Beispielszenario

- Effiziente Filterverteilung nicht trivial durch Abhängigkeit von Fehlerzuständen und Reaktion der Wegesteuerung

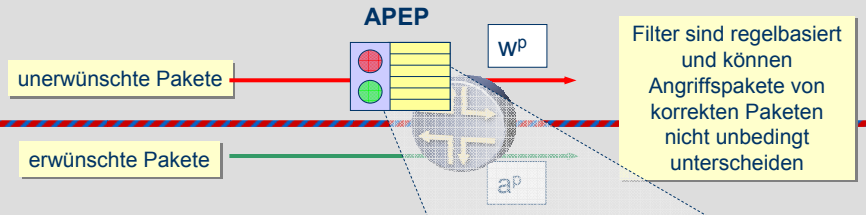








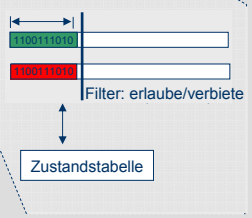

# Paketfiltertechnik




Filter sind regelbasiert und können Angriffspakete von korrekten Paketen nicht unbedingt unterscheiden

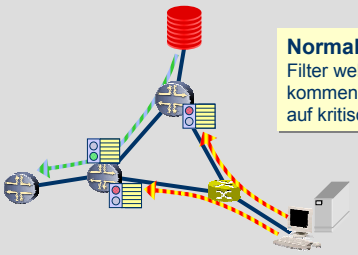
**Falsch-Positive und Falsch-Negative**

- Ein Verbotsfilter kann fälschlich „gute“ Pakete, z.B. von Managementverbindungen, verwerfen: Wahrscheinlichkeit $a^p$
- Erlaubnisfilter können fälschlich Pakete akzeptieren, die zu Angriffsdatenströmen gehören: Wahrscheinlichkeit $w^p$
- Erweiterete Filtertechniken („capabilities“) etwa z.B. durch die Kontrolle von Verbindungszuständen („stateful filters“) reduzieren diese Wahrscheinlichkeiten



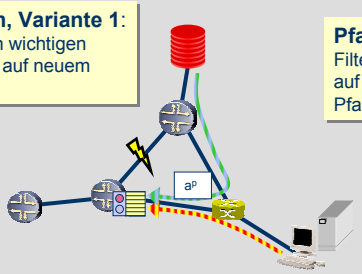
## Filterplazierung: Wegesteuerungsproblematik

Technik der Rechnernetze

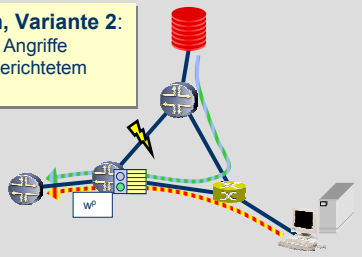


**Normalfall**:
Filter wehren von außen kommende Angriffe auf kritische Pfade ab

**Pfadbruch, Variante 1**:
Filter lehnen wichtigen Verkehr auf auf neuem Pfad ab




**Pfadbruch, Variante 2**:
Filter lassen Angriffe auf neu eingerichtetem Pfad zu








## Verteilungsmechanik

Technik der Rechnernetze

- Input: invariante globale Zugriffsrichtlinien
- Output: vom Netzwerkstatus abhängige (variante) lokale Filterregeln
- Randbedingungen:
  - Netztopologie **N**
  - Verfügbarkeiten **A** aller Komponenten in **N**
  - maximale gleichzeitige Fehler **f**
  - $(N, A, f) \xrightarrow{V} \{\{N_1, a_1\}, \{N_2, a_2\}, \ldots, \{N_n, a_n\}\}$

    $\{N_i, a_i\}$: Netztopologievariante $N_i$ mit Eintrittswahrscheinlichkeit $a_i$, i: 1..n

  - Bedrohungssituation **T**:
    Angriffswahrscheinlichkeiten $w_j$ zu einzelnen, disjunkten Teilnetzen $S_j$, j: 1..m

    $T: \{\{S_1, w_1\}, \{S_2, w_2\}, \ldots, \{S_m, w_m\}\}$; $S_1 \cup S_2 \cup \ldots \cup S_m \equiv N$

  - Wegesteuerungsverfahren **R**

# Verteilungsmechanik

- Input: invariante globale Zugriffsrichtlinien

  Richtlinienmenge **P: {{$p_1$,$b_1$,$x_1$}, {$p_2$,$b_2$,$x_2$}, …, {$p_o$,$b_o$,$x_o$}}**
  **p**: Schutzrichtlinie mit Flussmengenspezifikation, Transportmechanismus
  **b**: Falsch-Positiv-Schaden
  **x**: Falsch-Negativ-Schaden

- Algorithmus:
  (Zweifachfehler)

Einfache Versicherungs-mathematik – andere Bewertungsfunktionen einsetzbar

```
for each {p,b,x} in P
    // calculate path probabilities for p
    calculate best path D = R(N,p)
    calculate probability a^D of D
    for each link l in D
        N+ = N-l
        calculate best path D+ = R(N+,p)
        calculate probability a^D+ of D+
        for each link l+ in D+
            N* = N+-l+
            calculate best paths D* = R(N*,p)
            calculate probability a^D* of D*
        end for
    end for
end for
```

```
// compare with attack probabilities
for each {S,w} in T
    for each link l in {D,D+,D*} ∩ S
        a^total = (a^D if l in D, else 0)
                + (a^D+ if l in D+, else 0)
                + (a^D* if l in D*, else 0)
        if a^total·b > w·x
            place accept filter for p on l
        else
            place drop filter for p on l
        end if
    end for
end for
```

Birger Tödtmann (btoedtmann@iem.uni-due.de) Paketfilternetze ITG-Workshop 2005, Folie 13

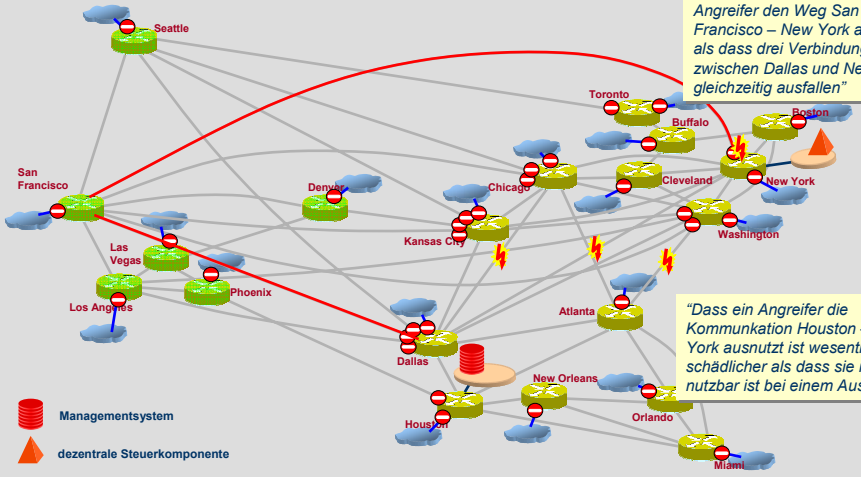




# Beispielszenario

- Rationale Abschätzung von Bedrohungssituation und Wahrscheinlichkeit der Wegewahl

*"Es ist wesentlich wahrscheinlicher, dass ein Angreifer den Weg San Francisco – New York ausnutzt als dass drei Verbindungen zwischen Dallas und New York gleichzeitig ausfallen"*



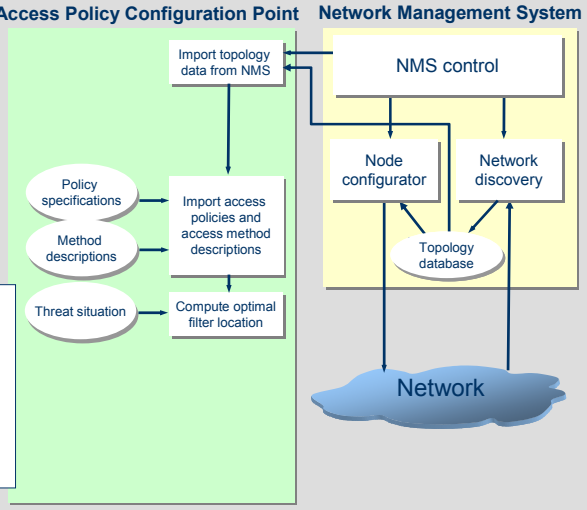

*"Dass ein Angreifer die Kommunkation Houston – New York ausnutzt ist wesentlich schädlicher als dass sie nicht nutzbar ist bei einem Ausfall"*

Birger Tödtmann (btoedtmann@iem.uni-due.de) Paketfilternetze ITG-Workshop 2005, Folie 14

# Implementierung: Prozessablauf



- Topologie- und Gerätedaten werden vom Netz erhoben (oder aus Netzbeschreibung gelesen)
- Richtlinien und Bedrohungs-situation werden eingelesen
- Plazierungsalgorithmus gibt optimale Orte an




```
apcp> load uunet.xml
 network loaded: 20 nodes and 71 segments
apcp> load uu-threats.xml
 threat specifications loaded: 1 default and
 2 segments
apcp> protect from ncs to nacs using snmp
fp_damage 500 fn_damage 50
 source specifier 'ncs' expands to ncs
 destination specifier 'nacs' expands to nac_dallas
  nac_newyork nac_miami
 transport specifier 'snmp' expands to udp port 161

 drop filter placement:
[...]
  node newyork: in at interface 10.2.45.5/30
```

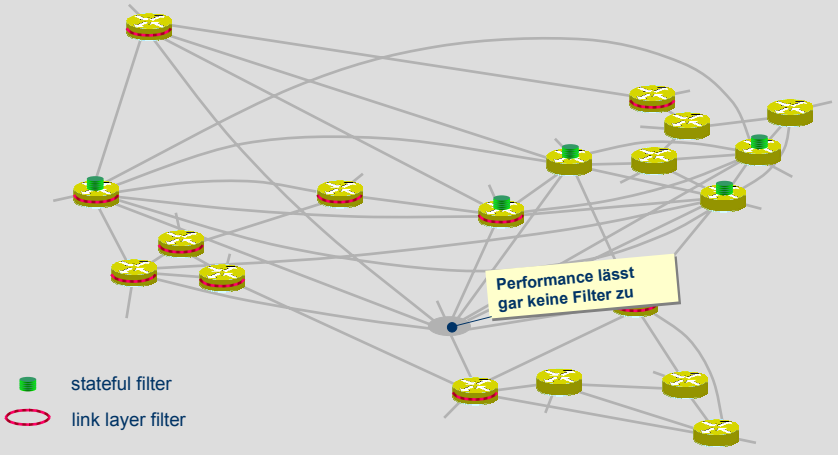
Birger Tödtmann (btoedtmann@iem.uni-due.de) Paketfilternetze ITG-Workshop 2005 Folie 15



# Filtercapabilities



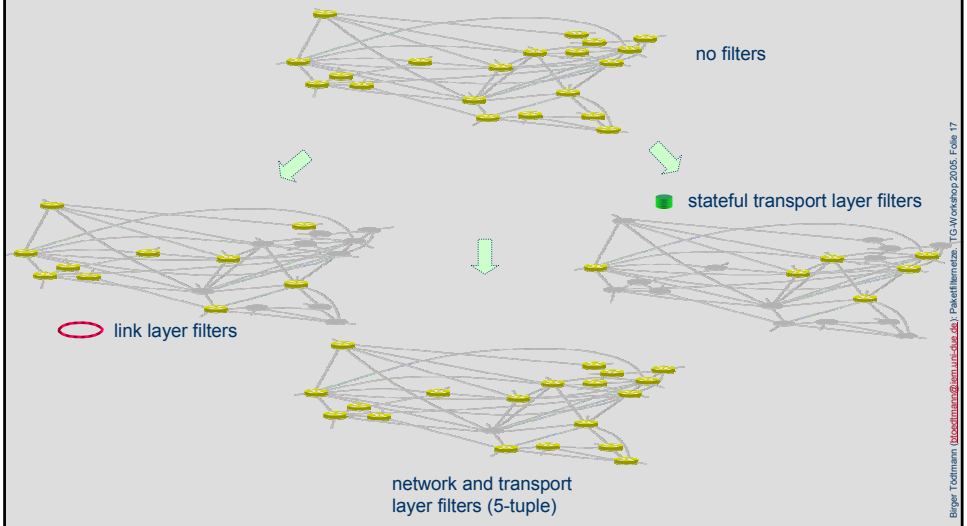
- Heterogene Szenarien: Nicht alle Netzkomponenten unterstützen dieselben Filtertechnikvarianten
- Aufspreizung von Filternetzen nach Verfügbarkeit




Birger Tödtmann (btoedtmann@iem.uni-due.de) Paketfilternetze ITG-Workshop 2005 Folie 16

## Filternetzvarianten im Beispiel

Technik der Rechnernetze



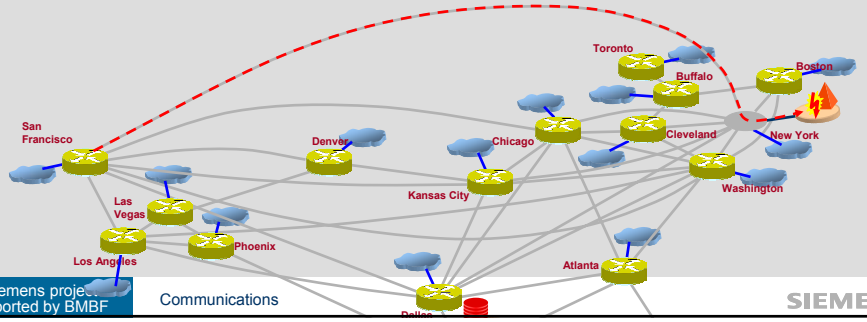





## Verteilungsmechanik mit Capabilities

Technik der Rechnernetze

- Input: invariante globale Zugriffsrichtlinien
- Output: vom Netzwerkstatus abhängige (variante) lokale Filterregeln
- Randbedingungen:
  - Netztopologie N, Wegesteuerungsverfahren R, Richtlinienmenge P, Verfügbarkeiten A
  - Verschiedene Filtertechniken erzeugen neue Topologien $\{N,c\} \xrightarrow{c} N^c$
  - Bedrohungsszenarien **T** (insbesondere Angriffswahrscheinlichkeiten **w**) variieren nach betrachtetem $N^c$
  - Filtermöglichkeiten allerdings nur falls Pfade in $N^c$ liegen



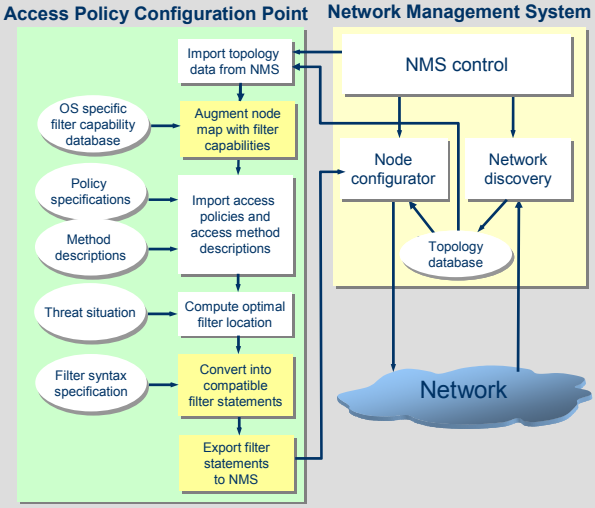
# Implementierung: Prozessablauf



- Gerätedaten geben Aufschluss über verfügbare Filtertechniken
- Plazierungsalgorithmus kalkuliert neu mit Hinblick auf Anforderung der Richtlinien
- Syntaxanpassung auf Hersteller und OS-Version

„protect from houston to newyork using snmp“

```
permit udp host 10.2.52.34
      host 10.2.101.4 port 161
```




Birger Tödtmann (btoedtmann@iem.uni-due.de) PaketFilternetze, ITG-Workshop 2005, Folie 19



# Ergebnisse



- Werkzeug zur Erzeugung von Filterkonfigurationen
  - Einsatz in größeren, heterogenen IP-Netzen
  - mit großen, evtl. unscharfen Randzonen
  - mit dezentralen Administrationsformen
- *Ohne Angabe des Bedrohungsszenarios*:
  Werkzeug zur Ermittelung kritischer Filterpunkte im Netz
  - Planungstool: wo können/sollten Filtersysteme optimal stehen?
    (bei gegebener Management- und Steuerkomponentenverteilung)
  - Welche Bedrohungen können bestimmte Filternetzvarianten abfangen?
  - Wo sind Steuerkomponenten am besten zu platzieren?
    (bei gegebener Filterverteilung)
- Implementierung in Java, Netzdiscovery via ICMP (Linux) und SNMP, Netzbeschreibungen in XML

Birger Tödtmann (btoedtmann@iem.uni-due.de) PaketFilternetze, ITG-Workshop 2005, Folie 20


## Ausblick

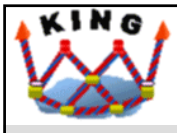

- Einsatz des Konzeptes in Netzen mit Traffic Engineering
  - Berücksichtigung von weiteren Parametern bei der Wegewahl, Integration der Paketfiltererzeugung
- Nicht-lineare Risikobewertung
- Schutzzielmetriken
  - Bei gegebenem Schutzziel (etwa: Kommunikationsbeziehungen zwischen Steuerkomponenten in einem Carrier-IP-Netz):

    Wie viel “besser” unterstützt eine Filternetzkonfiguration X dieses Schutzziel gegenüber einer Filternetzkonfiguration Y?
  - Bei einer Schutzzielmenge:

    Gibt es Konflikte in der Schutzzielmenge, die von keine Filternetzkonfiguration gelöst werden können?








## Backup

# Verteilungsmechanik

- Input: invariante globale Zugriffsrichtlinien

  $P = \{\{p_1,q_1, r_1\}, \{p_2,q_2, r_2\}, \ldots, \{p_o,q_o, r_o\}\}$
  p: Schutzrichtlinie mit Flussmengenspezifikation, Transportmechanismus
  q: Falsch-Positiv-Schaden
  r: Falsch-Negativ-Schaden

Einfache Versicherungs-mathematik – andere Bewertungsfunktionen einsetzbar

- Trivialer Algorithmus:

```
for each {p,q,r} in P
          for each {N,a} in V
                    extract best paths D of p in {N,a}
                    for each link l in D
                              add a of {N,a} to l in N
                    end for
          end for
          for each {S,w} in T
                    for each link l in {S,w}
                              if a(N,l)·q > w·r
                                        place accept filter for p on l
                              else
                                        place drop filter for p on l
                              end if
                    end for
          end for
end for
```

Birger Tödtmann (btoedtmann@ieee.org) Paketfiltersetze ITG-Workshop 2005 Folie 23



KING
Technik der Rechnernetze

# Verteilungsmechanik

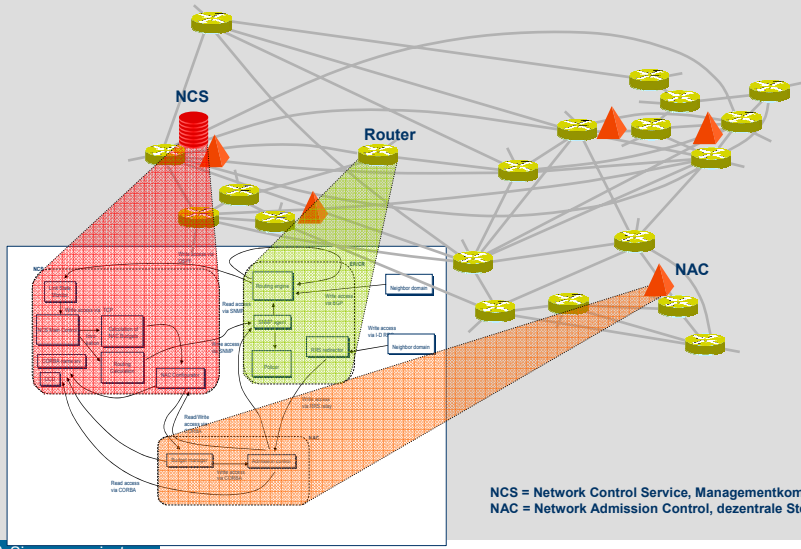
- Beispielnetz enthält 20 Knoten und 71 Kanten
  - bei möglichen Zweifachfehlern entstehen ~8200 Netztopologievarianten
  - Pro Zugriffsrichtlinie shortest path-Bestimmung für alle Varianten erforderlich
- Modifizierter Algorithmus:

```
for each {p,q,r} in P
          extract all possible paths D*={D1,M1},{D2,M2}…{Dk,Mk}} of p in N
          sort paths in D* by metric M
          for each path D in D*
                    calculate probability cp for D to be chosen as best path
                    // nicht abschließend geklärt
          end for
          for each {S,w} in T
                    …
          end for
end for
```

Birger Tödtmann (btoedtmann@ieee.org) Paketfiltersetze ITG-Workshop 2005 Folie 24

# Beispiel Komplexität KING

Technik der Rechnernetze




NCS = Network Control Service, Managementkomponente
NAC = Network Admission Control, dezentrale Steuerkomponente