

# Reduzierte Komplexität im Netzwerk dank dem „ZoneBuilder“

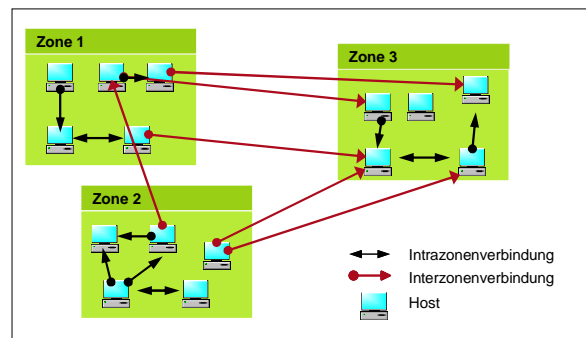
Mit dem „ZoneBuilder“ hat at rete ein findiges Tool entwickelt, das die Umsetzung von Zonenkonzepten entscheidend erleichtert. Aufgrund der Analyse der vorhandenen Verkehrsbeziehungen zwischen Endgeräten in einem IP-Netzwerk unterstützt es den Entscheid, welches Gerät in welche Zone zu stellen ist. Das Resultat ist ein sicheres Netzwerk mit minimaler Komplexität.

von Philippe Bourquin

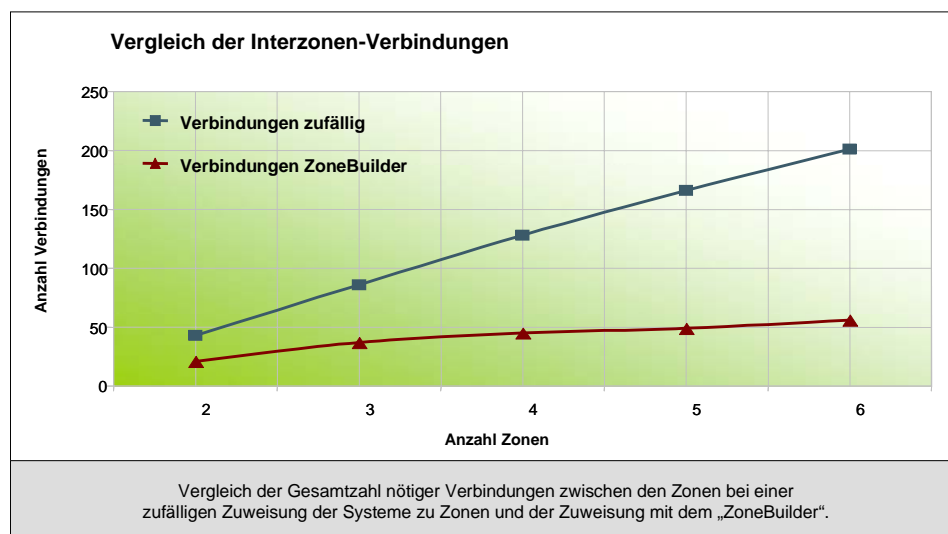
In den letzten Jahren haben sich viele ehemals kleinere Firmennetzwerke zu stark vernetzten und stark beanspruchten grossen Netzwerken entwickelt. Umso schwieriger ist es geworden, dabei den Überblick über alle Anwendungen zu behalten, welche über das Netzwerk laufen.

Spätestens an diesem Punkt lohnt es sich, über eine Restrukturierung des gesamten Firmennetzwerks nachzudenken. Ein sinnvoller und nahe liegender Ansatz besteht darin, das Netzwerk in einzelne Sicherheitszonen einzuteilen, welche gegeneinander geschützt sind. Jede Zone soll Systeme mit demselben Schutzbedarf umfassen. Innerhalb einer Zone erübrigt sich damit die Notwendigkeit, den Verkehr zu filtern. Die Komplexität wird aber nur bei einer sinnvollen, gut durchdachten Zoneneinteilung reduziert. Eine willkürliche Zuweisung von den Endgeräten zu den einzelnen Zonen würde sich eher kontraproduktiv auswirken. Die Betriebbarkeit wäre gefährdet.

Genau hier setzt der „ZoneBuilder“ an. Er analysiert den gesamten Netzwerkverkehr und findet vollautomatisch eine bestmögliche Aufteilung eines Netzwerks in Sicherheitszonen. Dabei berücksichtigt er aber auch den Schutzbedarf jedes Systems. Vertraulichkeit, Integrität und Verfügbarkeit können optional für je des einzelne Endgerät



spezifiziert werden und werden danach vom „ZoneBuilder“ berücksichtigt. Das bedeutet, der „ZoneBuilder“ unterstützt den Entscheid, welches Gerät in welche Zone zu stellen ist und welche Filterregeln auf den Firewalls implementiert werden müssen, so dass alle gewohnten Anwendungen weiterhin problemlos funktionieren und der Betriebsaufwand so klein wie möglich gehalten wird. Eine einzige zentrale Firewall übernimmt dabei die Filterung des Inter-Zonen-Verkehrs. Der Administrationsaufwand wird auf ein Minimum reduziert.



Fazit: Mit dem „ZoneBuilder“ lassen sich verschiedene Szenarien innerhalb kürzester Zeit durchspielen. Das Resultat ist ein sicheres, zentral überwacht Netzwerk mit klar definierten Sicherheitszonen und optimierten Filterregeln.

## Anforderungen

### Systemvoraussetzungen

- JAVA Virtual Machine  $\geq$  1.4.2
- Java Bibliothek ostermillerutils.jar (<http://ostermiller.org/utills/download.html>)
- min. 1GHZ und 256MB RAM empfohlen

### Zusätzlich empfohlene Software

- Microsoft Access (oder andere DB-Software)
- Microsoft Excel (geeignet zur Darstellung von CSV Dateien)
- Ethereal (zur Aufzeichnung des Netzwerkverkehrs)
- Graphviz (open source, [www.graphviz.org](http://www.graphviz.org), zur grafischen Darstellung)
- Perl interpreter (z.B. ActivePerl, [www.activestate.com/Products/ActivePerl](http://www.activestate.com/Products/ActivePerl))
- Das Perlscript "sorthosts.pl" (im Softwarepaket enthalten)

Philippe Bourquin studiert im 8. Semester Informatik an der ETH Zürich. Im Rahmen eines 5-monatigen Praktikums bei at rete entwickelte er in Zusammenarbeit mit dem Security- und dem Networking-Team den „ZoneBuilder“.

