von Thomas Barlen

In vielen Firmen wird der Einsatz einer Firewall als ausreichend betrachtet, um sich gegen Angriffe aus dem Internet zu schützen. Dabei wird oft übersehen, dass die meisten Schäden durch Angriffe, sei es absichtlich oder aus Versehen, aus dem Intranet heraus initiiert werden. Diese Tatsache bedeutet, dass Ihr iSeries Server allen Angriffsversuchen aus dem Intranet voll ausgesetzt ist. Wäre es nicht schön, einen Service zu haben, der es Ihnen erlaubt, unerwünschten Netzwerkverkehr direkt an der Kommunikationsschnittstelle in das System abzuweisen? Es gibt tatsächlich einen Service, der es erlaubt, IP Datenverkehr in und aus dem System auf physischer Schnittstellenebene zu kontrollieren.

Über den Autor

Thomas Barlen ist ein Consulting IT Specialist für iSeries und AS/400 im IBM eServer iSeries Technical Sales Support bei IBM Deutschland. Sie können Herrn Barlen unter barlen@de.ibm.com erreichen.

IP Paketregeln

Unter OS/400 ist dieser Service als „IP Paketregeln“ bekannt und er ermöglicht Ihnen, als primären Schutz Intranetverkehr zu filtern und eine zweite Verteidigungslinie gegenüber dem Internet aufzubauen. IP Paketregeln wurden erstmals mit V4R3 im OS/400 zur Verfügung gestellt und mit V5R2 erheblich erweitert. Das Filtern von IP Verkehr findet auf der IP Ebene (Netzwerkebene) statt. Die Entscheidung, ob ein Paket die IP Schnittstelle passieren kann, wird beim Filtern anhand von Informationen im IP Header getroffen. Die meisten Paketfilter erlauben das Filtern anhand folgender Kriterien:

1. Quellen- und Zieladresse
2. Quellen- und Zielport
3. Protokoll (TCP, UDP, ESP, etc.)
4. Datenrichtung (INBOUND oder OUTBOUND)

V5R2 erlaubt das Filtern auf allen physischen und virtuellen (LPAR und Windows Integration) LAN Schnittstellen, Point-to-Point und Layer 2 Tunneling Protocol (L2TP) Schnittstellen. Für PPP und L2TP Schnittstellen können unterschiedliche Filterregelgruppen für verschiedene Benutzer aktiviert werden. Ein gutes Basiswissen des IP Protokolls sollte vorhanden sein, um IP Paketregeln erfolgreich einzusetzen. Eine typische Implementierung von IP Paketregeln setzt sich aus der Planungs-, Konfigurations- und Aktivierungsphase zusammen.

Planung

Paketregeln können Datenverkehr erlauben oder blockieren sowie Daten einer VPN Verbindung

verarbeiten. Im Falle eines VPNs muss die sogenannte IPSec-Regel vor dem Aktivieren der VPN Verbindung eingerichtet sein. Ist der VPN Tunnel aktiv und ein Paket entspricht einer IPSec-Regel, so wird dieses Paket entsprechend der zugehörigen Konfiguration verschlüsselt. Da VPN nicht das Hauptthema dieses Artikels ist, widme ich mich wieder der reinen Filterfunktion. Sobald Filterregeln für eine Schnittstelle aktiviert sind, wird jeglicher IP Datenverkehr, der nicht ausdrücklich erlaubt ist, automatisch durch eine implizite „Deny"-Regel abgewiesen. Deswegen ist es außerordentlich wichtig, vor der Konfiguration eine sorgfältige Planung durchzuführen. Dies erfordert die Sammlung von Informationen, z.B. welche Anwendungen (Ports und Protokoll) aktiv und in Gebrauch sind sowie die fernen Adressen, welche auf diese Anwendungen zugreifen sollen. Während dieser Planungsphase werden Sie wahrscheinlich feststellen, dass einige Anwendungen aktiv sind aber nicht benötigt werden oder Sie sehen Benutzer, die auf Anwendungen zugreifen, für die sie eigentlich nicht autorisiert sind. Obwohl die Planung die meiste Zeit in Anspruch nimmt, so ist diese Phase aber auch die wichtigste Phase in der gesamten Implementierung. Grundsätzlich stehen zwei unterschiedliche Wege zur Verfügung, um festzustellen, welche Pakete erlaubt oder explizit abgewiesen werden sollen. Die erste Methode nutzt die NETSTAT Funktion, welche über die 5250 Befehlszeile (NETSTAT *CNN) oder über den iSeries Navigator (Netzwerk->TCP/IP Konfiguration->IPv4-> Verbindungen) genutzt werden kann. NETSTAT gibt Auskunft über alle aktiven Verbindungen, alle Anwendungen, die gestartet sind und über IP Adresse, Protokoll und Port, die der Anwendung zugeordnet sind. Die über NETSTAT erlangten Informationen verschaffen Ihnen einen guten Überblick über die genutzten Anwendungen und Zugriffe, stellen aber nur eine Momentaufnahme zum Zeitpunkt der Ausführung dar. Um eine detailliertere Aufstellung zu erhalten, können Sie eine einzelne IP Paketregel konfigurieren. Diese Regel erlaubt jeglichen Verkehr, sei es ein- oder ausgehend, nutzt aber die Journaloption. Dabei schreibt OS/400 für jedes eingehende und ausgehende Paket einen Journaleintrag. Diese Methode stellt Ihnen eine komplette Aufstellung zur Verfügung, hat aber auch einen negativen Einfluss auf die Systemperformance und den Plattenbereich. Die Filterjournaloption sollte nur während der Planungsphase oder für spezielle Einsätze (z.B. Problemeingrenzung) aktiviert werden. Das Ergebnis der Datensammlung sollte sich mit den Sicherheitsrichtlinien Ihres Unternehmens decken.

Konfiguration

Während der Konfigurationsphase werden alle Regeln konfiguriert, die IP Datenverkehr explizit erlauben oder abweisen. Die Konfiguration erfolgt auf der Basis der Informationen aus der Planungsphase. In diesem Beispiel werden die mit V5R2 zur Verfügung gestellten Konfigurationsassistenten genutzt. IP Paketregeln können nur über den iSeries Navigator konfiguriert werden. Dies geschieht über den Regeleditor, der über folgende Schritte geöffnet werden kann:

1. iSeries Navigator starten
2. Den Navigationspfad auf Netzwerk-> IP Richtlinien->Paketregeln erweitern
3. Mit der rechten Maustaste auf Paketregeln klicken und Regeleditor auswählen

Die Konfiguration basiert auf dem in Bild 1 dargestellten Beispielszenario.