Using SERVAUTH NETACCESS to restrict inbound IP traffic – why and how

Aron Eisenpress
z/OS Systems Programmer
City University of New York

Quick review of SERVAUTH NETACCESS

- The SERVAUTH class controls access to TCP/IP functions.
- NETACCESS controls network access and works with definitions in the TCPIP.PROFILE that define IP addresses as resources.
- Many other SERVAUTH profiles protect other TCP/IP resources.

NETACCESS is usually thought of as controlling access by userid to connect to an IP address – that is, outbound transfers.

But NETACCESS can also be used to control <u>inbound</u> connections and transfers.

How is this different from an external firewall?

- The controls are by the target RACF userid, not by port number. This gives different granularity.
- Logging is by the RACF resource name assigned to the group of IP addresses. It does not include the IP address itself.

How is this different from an external firewall?

- These controls are in the z/OS TCP/IP configuration and the RACF profiles/permits, and likely under the control of a different group than the network firewall rules.

Why?

- In our case, a historically open system (this is changing).
- Omegamon kept running out of storage. Turned out to be a bug induced by port scanners connecting to its monitoring port number. (There was no intrusion.)

Why?

- Restricting “outside” access to system servers by userid resolved this issue. (That Omegamon service can be turned off, but I also wanted to protect other system services.)
- NETSTAT CONN will give you a list of system servers with open ports that you might want to protect.

Definitions: In the TCPIP.PROFILE dataset

```
NETACCESS INBOUND   OUTBOUND
   172.16.nn.0/24     OPEN
   172.16.0.0/16      INSIDE
   172.16.0.0/12      ZONE1
   127.0.0.1/8        LOOPBACK
   0.0.0.0/32         ADDRANY
   yy.yy.0.0/16       BLOCKED
   zz.zz.0.0/16       BLOCKED
   DEFAULT            WORLD
ENDNETACCESS
```

Definitions: RACF profiles and permits

```
RDEF SERVAUTH EZB.NETACCESS.*.TCPIP.INSIDE
  OWNER(SYS1) UACC (NONE)
RDEF SERVAUTH EZB.NETACCESS.*.TCPIP.ZONE1
  OWNER (SYS1) UACC (READ)
RDEF SERVAUTH EZB.NETACCESS.*.TCPIP.BLOCKED
  OWNER(SYS1) UACC (NONE)
RDEF SERVAUTH EZB.NETACCESS.*.TCPIP.WORLD
  OWNER (SYS1) UACC (READ)

PE  EZB.NETACCESS.*.TCPIP.WORLD  ID
 (OMEGAMVS) ACCESS (NONE) CLASS (SERVAUTH)

SETR REFRESH RACLIST(SERVAUTH)
```

Some other considerations:

- You will need to know your network topology, since if you want to define “everything else” you first have to define your “everything”.
- Documentation is in the *Comm Server IP Configuration Reference* and the *IP Configuration Guide* (not the RACF books).