bank-verlag Das Service-Unternehmen der privaten Banken

How to control IP connections

Wolfgang Breidbach

Bank-Verlag

- Founded in 1961 as the publishing house of the magazine „Die Bank“.
- Running on IBM Systems /1 and /370 the first Authorisation Center in Germany for ATM-transactions was founded at the Bank-Verlag in 1986.
- In 1988 authorisation was migrated to Tandem creating the first active-active application.
- In the following years we took our way through Cyclone, CLX, CLX2000, K10000, K20000, S7000, S70000, S72000 to at last S86000
- 2005 we moved to Integrity NonStop
- 2010 the secondary datacentre was moved to a new location
- 2012 we migrated our production systems to NonStop blades
- Today wer are **the** IT-service provider for the Private Banks in Germany

Our problems

- The are more and more network connections with different partners
- The time of the „Green-Screens“ is finally over
- You usually do not know security details about your partners
- We have got Safeguard but that is no magic wand
- In addition to invalid logons there are some other problems that might cause the system to become inaccessible

The logon problem

- Safeguard logs all logons into its logfile
- You find all the local data like hometerminal, processname and so on
- But: No external information like the address or the name of the client is available
- Doing a research afterwards turns out to be very difficult or even impossible
- If we have an invalid logon we want to know the source

Some additional thoughts concerning logon

- Telnet is only one of the connections supporting a logon to the system
- Advantage: Telnet has an SPI-Interface the information is avaliable
- FTP in opposite does not provide that information
- We must not forget IP/V6, some things are changing with V6!
- We have to look at all produucts requiring a logon
- There are some other products like ODBC(/MX) requiring a logon!

Additional problems

- A process listens illegally to a port
- There are too many open sessions for a port (might be FTP or Telnet)
- We do not listen to a needed port
- There are too many or too few connections established to a remote port

A sample

- Somebody opens TELNET-sessions to our NonStop, starts a TACL-Prozess and enters „PAUSE“, no valid Logon is necessary
- The session is ended and because of “PAUSE” TACL does not notice that the session has gone
- TACL runs as lowpin-process, so the lowpin-PCBs can be eaten up really fast
- Do you notice?
- And if yes, what can be done against that?

A real-life sample

- Bank-Verlag operating was working 2 shifts with shared PCs, during the takeover from one shift to the other one operator logged off and the other logged on on the PC
- TACL-sessions were put into „PAUSE“ to avoid the autologoff after 30 minutes.
- After logging off from the PC those sessions were lost but the TACLs kept running.
- And very slowly the lowpin PCB were eaten up.
- Fortunately our $CMON is checking the number of lowpin PCBs and created a message early enough

Some precautions

- Change the telnet-configuration, instead of TACL the program $SYSTEM.SYSTEM.LOGON is started
- LOGON doesn‘t allow „PAUSE“ als ends properly at end of session
- LOGON is running highpin
- Disadvantage: 1 additional process
- It does not help against logged on TACLs put in PAUSE
- Nice to have: A logon timeout.

What would we like to have?

- The logon-timeout: If you do not complete the logon within a couple of minutes the session is aborted.
- A limit for the number of sessions like TACL in total or per user, there is no need to have 20 TACL for one system
- More interaction between the subsystems, Safeguard should fetch or get the external data from programs like telnet, ftp or ODBC/MX
- A configurable GUI for the safeguardlogs, SafeArt is not really “state of the art”

Security problem?

- We are using MXCS also known as ODBC/MX
- SQL-queries can cause very much system load and may last a while
- Users are not patient, the PC application creating the query is aborted (something is wrong) and restarted creating a second query increasing the system load because the first query is not stopped!
- We had a similar case with an application program started by a GUI. The program contained a loop with a tiny bit of I/O and finally the users managed to start more than 10 of those looping processses, fortunately not on a production system.

Security problem?

- The system was running with 100% CPU load and a CPU-queue of 180
- Because of that tiny bit of I/O the priority was not changed by the system
- Users did not get any response from that system
- Using a high-priority-TACL we could stop those processes

The request from the security administration

- Security administration gets a daily list of failed logons
- No problem with personalised logons
- Problem are „technical users“ like super.super and unknown users
- One day one of the administrators asked „Yesterday at 10:05 somebody tried a logon with the user Administrator. Can you tell me where that came from?“
- There is no chance in finding that information because using the standard configurations the IP-address is not logged.

We have been working on that

- We are reading the safeguardlog
- Telnet-logons are completed with TCP/IP-information
- ODBC/MX is a problem but usually we are able to find out the name of the workstation
- We are able to check TCP/IP-Ports and compare the actual state with the configured state and produce a message if there is a difference
- Orphaned processes like interactive TACL on a no longer existent terminal or an inactive FTPSERV are automatically stopped

Our advantages

- We are maintaining a SQL table containing all invalid logons including the source-address
- We intend to check this table realtime
- We can find out if there are too many sessions of the same type (like ftp or telnet) from one IP-address
- This is a part of our monitoring toolbox

Another real life case concerning a security problem

- Our NonStop is accessing another server though a firewall
- There have to be 2 established connections on port 4711
- A rule within the firewall was erroneously changed
- The NonStop could no longer establish a new connection to the server
- The already established connections were not affected
- The real problem we had weeks later when one of the connections had to be reestablished
- The monitoring tool found the missing connection immediately

A new challenge with the new systems

- A disk goes down and is replaced by the HP technician
- The technician takes the disk back to HP
- We have a contract with HP and the auditors are satisfied
- With the new systems the disk is no longer taken back to HP
- We have to take care of the disk ourselves!
- Our auditors want to see a proof that this dedicated disk has been physically destroyed
- We are automatically keeping track of those disk changes

And finally: Too much security?

- Our production systems NS16000 were replaces by NB54000
- The old system were renamed and stayed at Bank-Verlag
- Usually we are using SECOM
- We needed access to SUPER.SUPER but because of the rename SECOM no longer worked
- The password was in our safe, 2 parts 32 bytes each
- I do not want to use such a password in a crisis situation
- Afterwards the password was shortened to 2 times 16 bytes

Any questions???

Wolfgang Breidbach
Bank-Verlag GmbH
IT-Services
Wendelinstr. 1
50933 Köln

E-Mail: Wolfgang.Breidbach@Bank-Verlag.de
www.Bank-Verlag.de