How to fix problems after upgrade to Check Point Multi-Domain management R75.30

Vložil/a cm3l1k1 [1], 29 Červen, 2012 - 14:57

- Check Point [2]
- Networks & Protocols [3]

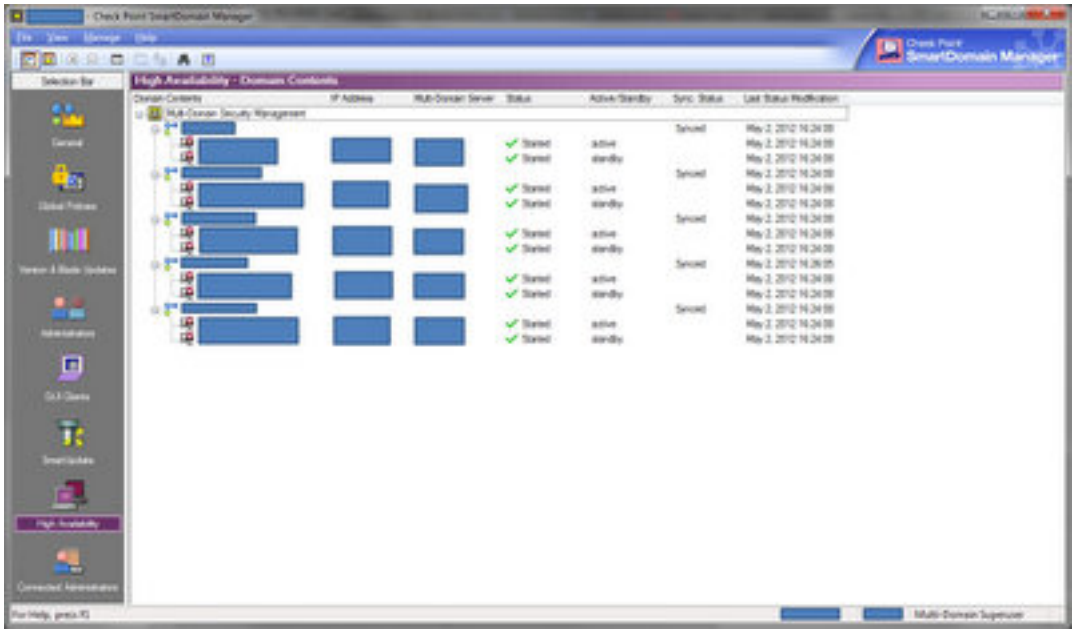
In previous post we focus on installation of MDM/MDS R75.30. As usual upgrade is not straightforward so I will show you what should be checked and how can be fixed common problems. Problems described here:

- After upgrade to R75.30 secondary CMA/CLM still shows R75.20 in SmartDashboard
- Problems with IP Pool NAT
- CP_default_Office_Mode_addresses_pool
- Problem with MDS permission profiles

// After upgrade to R75.30 secondary CMA/CLM still shows R75.20 in SmartDashboard

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_do... [4]

Because of this bug you will have problem with CMA synchronization which would be visible in SmartDomain Manager -> High Availability

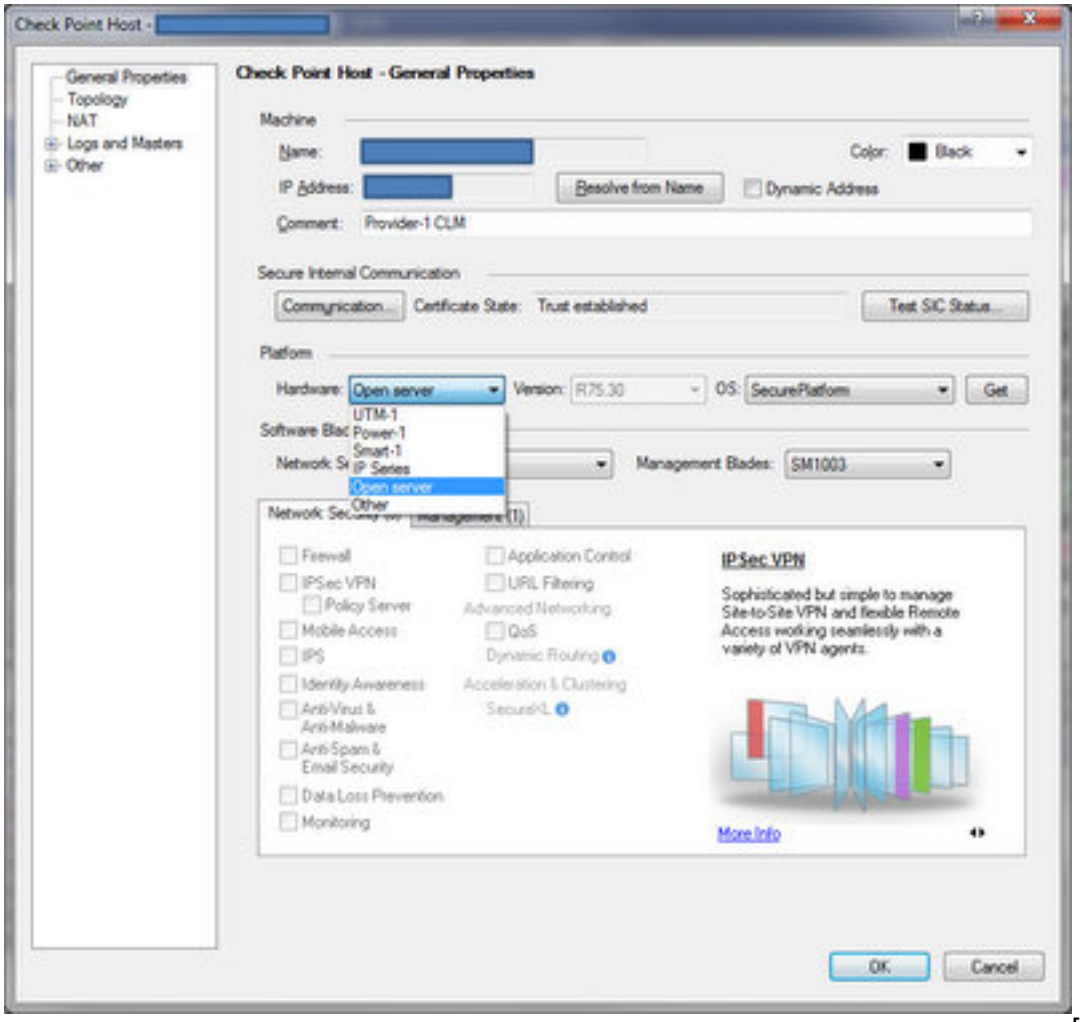


[5]

You're able to fix this easily on CLMs, but not on CMAs. You need to perform same actions through all secondary CLM/CMAs.

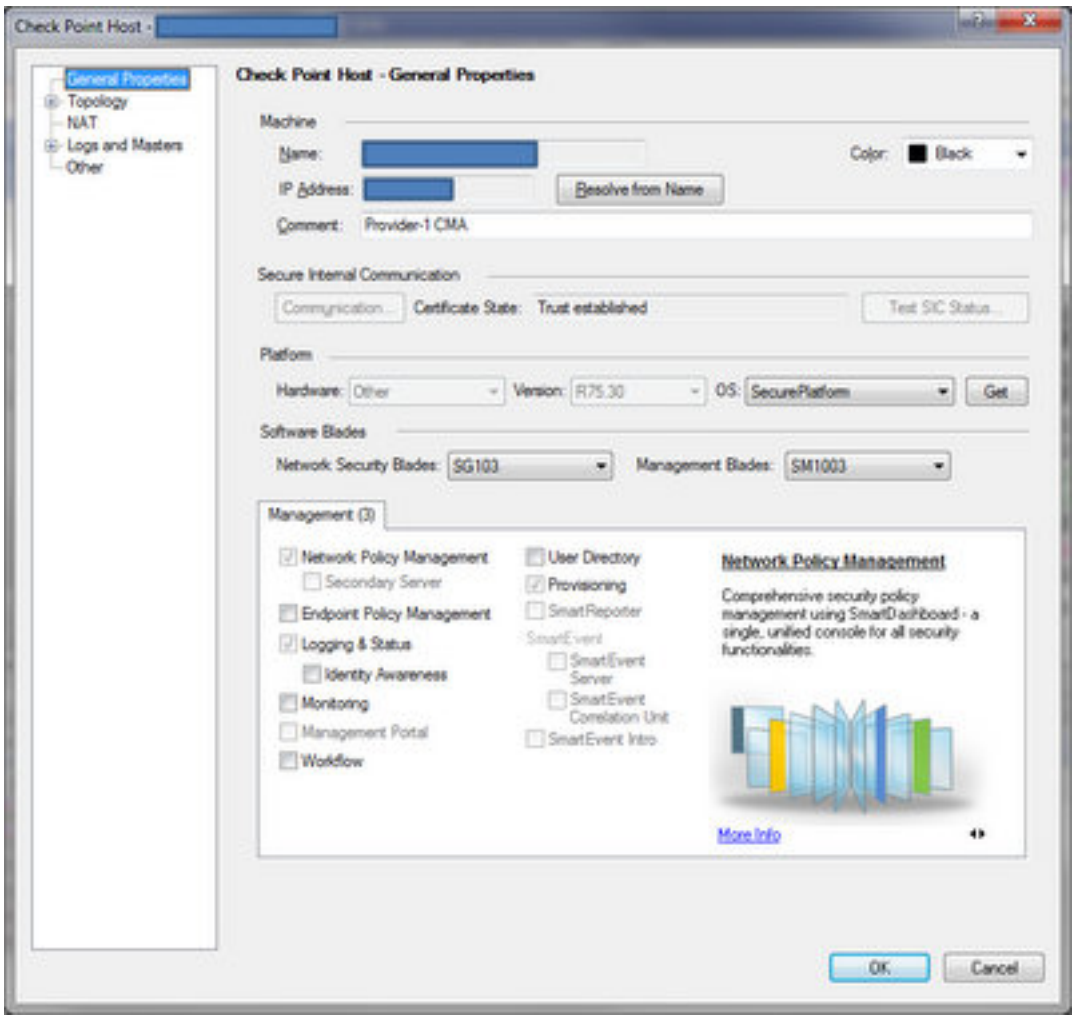
To fix CLM version open SmartDashboard of one CMA and open Check Point CLM object. In general properties you will see wrong version, but you're able to re-select Hardware (for example OpenServer) in Platform section which will make drop down menu “Version” visible and you can

change it to R75.30. Do so and change back correct Hardware type.
Make this as well on others CLMs and “Install Database” to reflect this change. Please don't confuse it with “Install Policy” which will not promote changes to CMA/CLMs but to firewalls.



[6]

To fix that on secondary CMAs you need to use GuiDBedit because you cannot change Hardware type as in previous case.



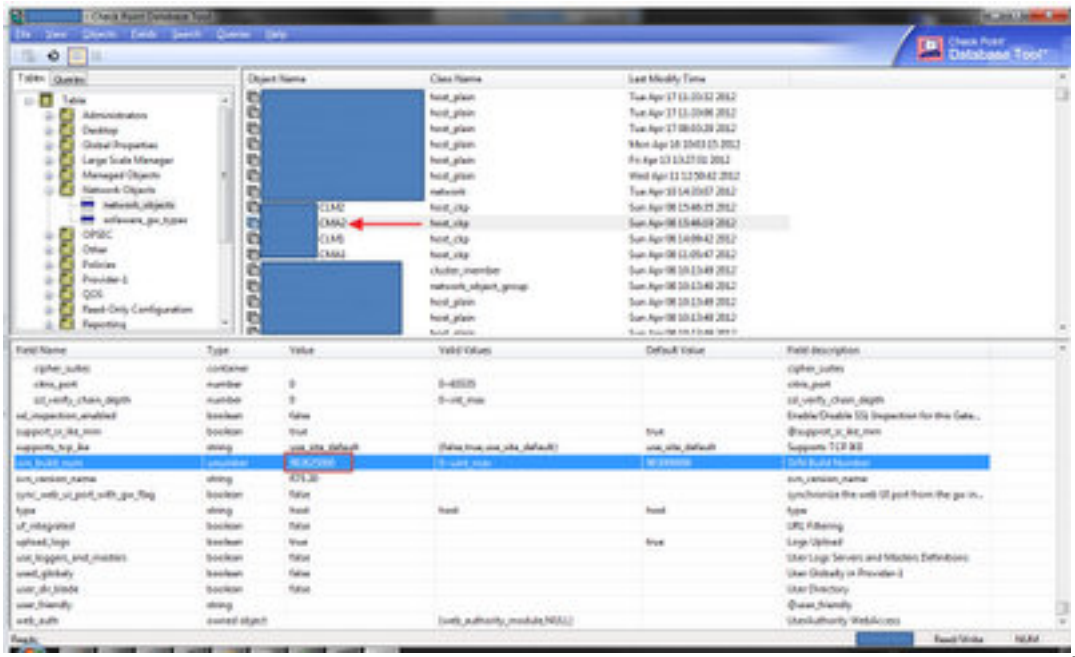
[7]

// GuiDBedit

From CP website: "The Check Point Database Tool, also referred to as GuiDBedit, is a graphical user interface (GUI) that enables its users to edit objects and properties in the SmartCenter management database. This Database Tool allows users to change properties that cannot be edited using SmartDashboard."

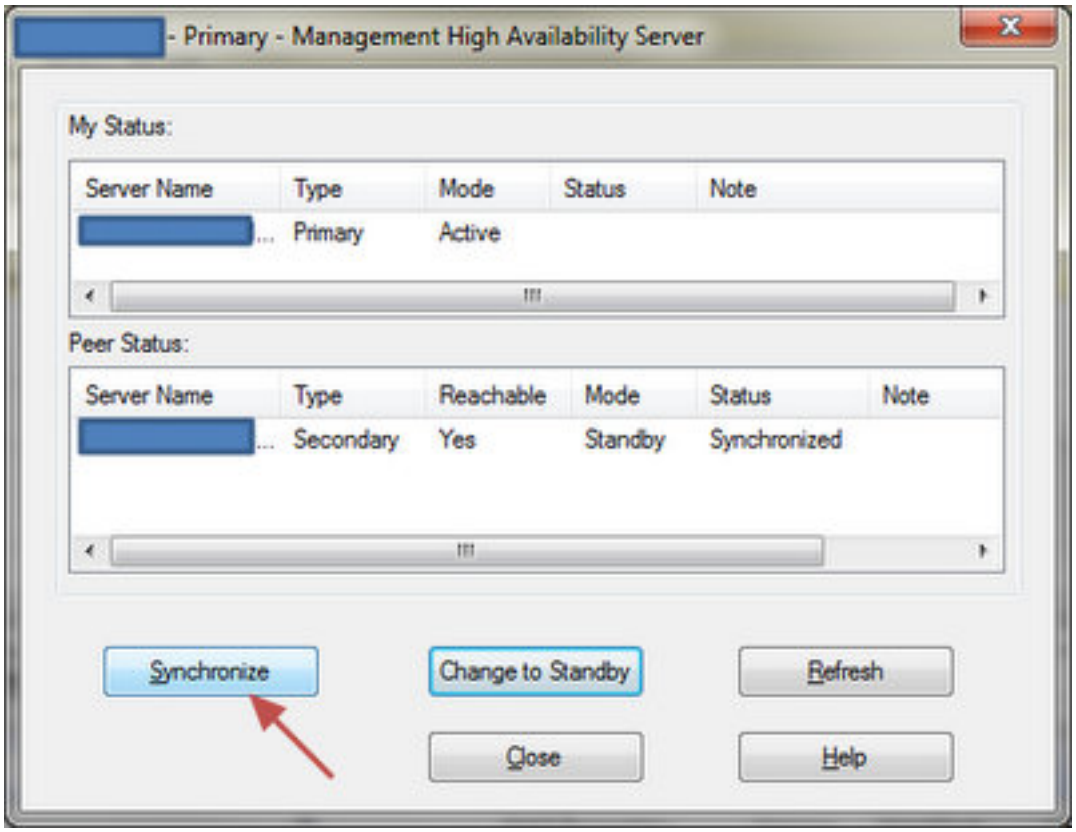
Database Tool - GuiDBedit.exe - is located in the same folder where the SmartConsole is installed. Usually folder C:\Program Files\CheckPoint\SmartConsole\<version>\PROGRAM\

First of all close SmartDashboard windows and open GuiDBedit. Connect to one of CMA (not to Provider-1/MDS) and search in database field "**svn_build_num**". When you find first match also check that you have found this in secondary CMA object name (in our example CMA2) with class name host_ckp (top right box). If it isn't correct field simply use “F3” to find next occurrence. When you find it check that Value is “983000000” (which means R75.20) and change it to “983625000”. When finish save DB, open SmartDashboard and check that version is OK now. If so make this on all others secondary CMAs.



[8]

Now you can synchronize active and standby CMAs in SmartDashboard -> Policy -> High Availability



[9]

// Problems with IP Pool NAT

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_do... [10]

IP Pool NAT enables N hosts to be NATed using M IP addresses (N:M, where N > M), unlike Static NAT which translates N:N IP addresses (from subnet to subnet), or Hide NAT which translates N:1 and does not support incoming connections. This allows also back-connections because it provides a

unique IP per NATed host.

This mapping/setup has been historically configured in file $FWDIR/lib/user.def which has been replaced by several files during upgrades (I don't know why). So when you upgrade to R75.30 be sure that it is different file. Here you have file location which is also in relation to SPLAT version running on firewalls (why not bring some chaos into)

R75:

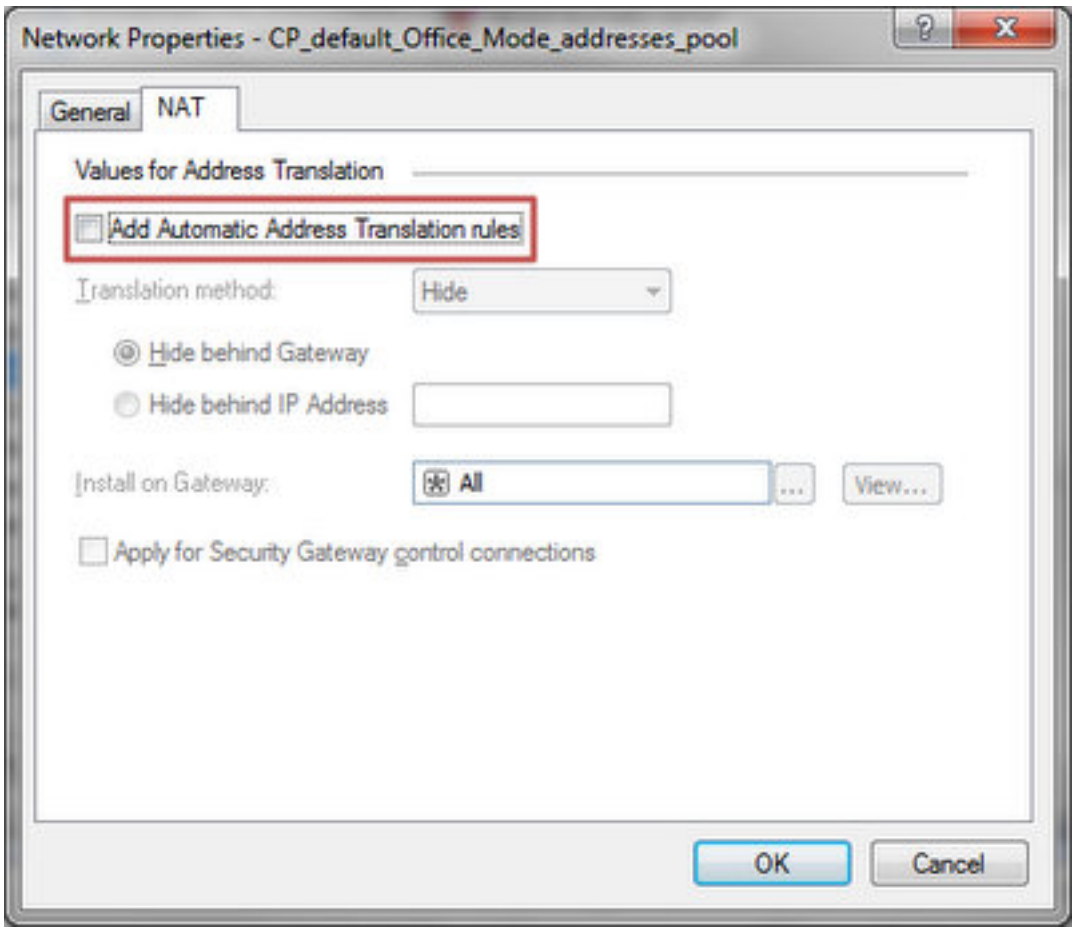
- **R75** Management Managing **R70/R71** Gateways: $FWDIR/conf/user.def.FLICMP
- **R75** Management Managing **R75** Gateways: $FWDIR/conf/user.def.NGX_R75
- **R75.20** Management Managing **R75/R75.10** Gateways: user.def.R75CMP
- **R75.20** Management Managing **R75.20** Gateways: user.def.NGX_R75.20
- **R75.40** Management Managing **R65** Gateways: user.def.NGXCMP
- **R75.40** Management Managing **R70/R71** Gateways: user.def.FLICMP
- **R75.40** Management Managing **R75/R75.10** Gateways: user.def.R75CMP
- **R75.40** Management Managing **R75.20/R75.30** Gateways: user.def.R7520CMP
- **R75.40** Management Managing **R75.40** Gateways: user.def.Fiber

If you're using this feature please update new file by simply copying configuration lines via text editor. As you see not all possible scenarios are described there, so if unsure copy config to many of them... yes, it is little bit confusing.

// CP_default_Office_Mode_addresses_pool

I'm not sure why, because we never use it, but after upgrade this object take its position in object database and what is worse enable automatic NAT. It means that when you're using range dedicated for Office Mode (172.16.10.0/24) in your network it can overwrite your NAT rules!
If deleted, it must be specified for each gateway individually (in the VPN Clients page Advanced section).
Solution: Disable automatic NAT on CP_default_Office_Mode_addresses_pool object.

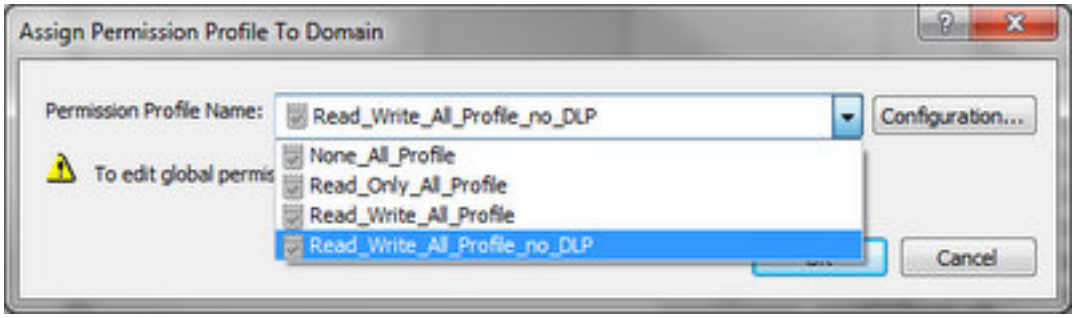
CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn



[11]

// Problem with MDS permission profiles

This problem seems to be related to users who don't have Multi-Domain Superuser permissions. In our case we have accounts with read-only permissions to selected CMAs (for policy review, etc.) and those accounts were unable login into MDS.
Permission profiles has been changed and you need to reselect current roles.



[12]

I don't remember other main problems. Simply check that High Availability is OK (if not synchronize CMA) and also check that SmartView Monitor see all firewalls.

That's all for now, be cool and ready for R75.40 Gaia OS [13]! :]

URL článku:
https://security-portal.cz/clanky/how-fix-problems-after-upgrade-check-point-multi-domain-management-r7530

Odkazy:

[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/check-point
[3] https://security-portal.cz/category/tagy/networks-protocols
[4] https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk68563
[5] https://security-portal.cz/sites/default/files/SmartDomain-Manager-High-Availability.png
[6] https://security-portal.cz/sites/default/files/SmartDashboard-CLM-General.png
[7] https://security-portal.cz/sites/default/files/SmartDashboard-CMA-General.png
[8] https://security-portal.cz/sites/default/files/GuiDBedit-svn_build_num.png
[9] https://security-portal.cz/sites/default/files/SmartDashboard-Policy-High-Availability.png
[10] https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk62590
[11] https://security-portal.cz/sites/default/files/SmartDashboard-Office-mode-NAT.png
[12] https://security-portal.cz/sites/default/files/SmartDomain-Manager-Administrators-Assign-Permissions.png
[13] http://www.checkpoint.com/gaia/

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn