PLATINUM PARTNER

Microsoft DAQUAS

GOLD PARTNER

DEVCON HALL SHOWIT HALL

epam f5

SILVER PARTNER

PROFINIT

NÁSKOK DÍKY ZNALOSTEM

GENERAL PARTNER

ATOM

Modern RDP security

Ing. Ondřej Ševeček | GOPAS a.s. |
MCSM:Directory | MVP:Enterprise Security | CEH | CHFI | CISA |
ondrej@sevecek.com | www.sevecek.com |

moje kurzy v GOPASu

GLAB007 - capture the flag 1 - hackni si podnikovou síť
GLAB008 - capture the flag 2 - hackni si podnikovou síť
GOC175 - implementace bezpečnosti
GOC169 - ISO 27001
GOC172 - Kerberos troubleshooting

GOPAS POCITACOVA.SKOLA.CZ

Tech·Ed DevCon

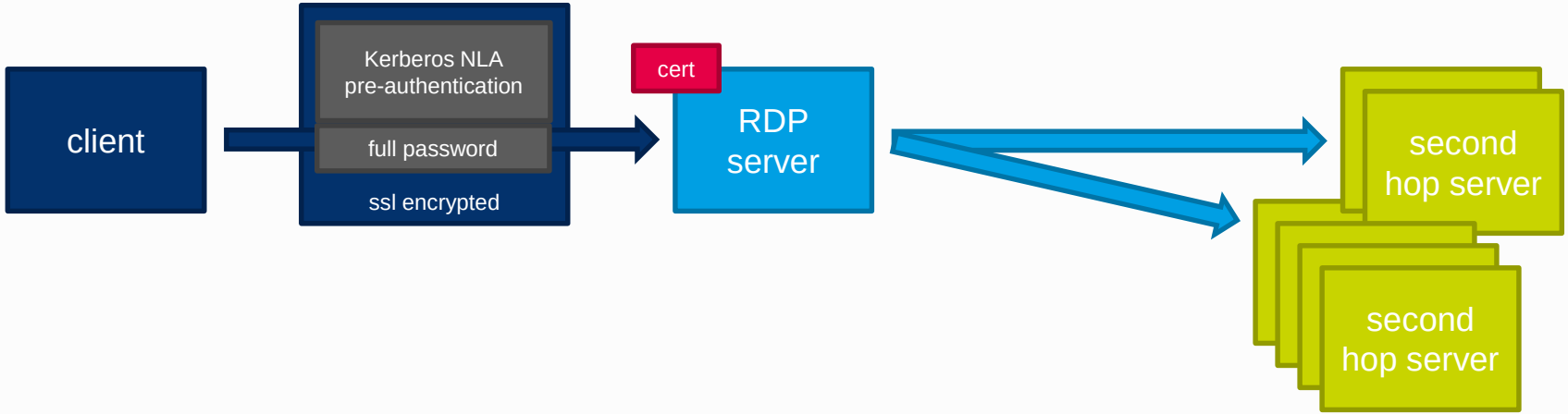
Agenda

- Password transport in full
- SSO principles
- Channel encryption with SSL/Kerberos/NLA
- User access to secure RDP servers
- Admin access to insecure endpoints

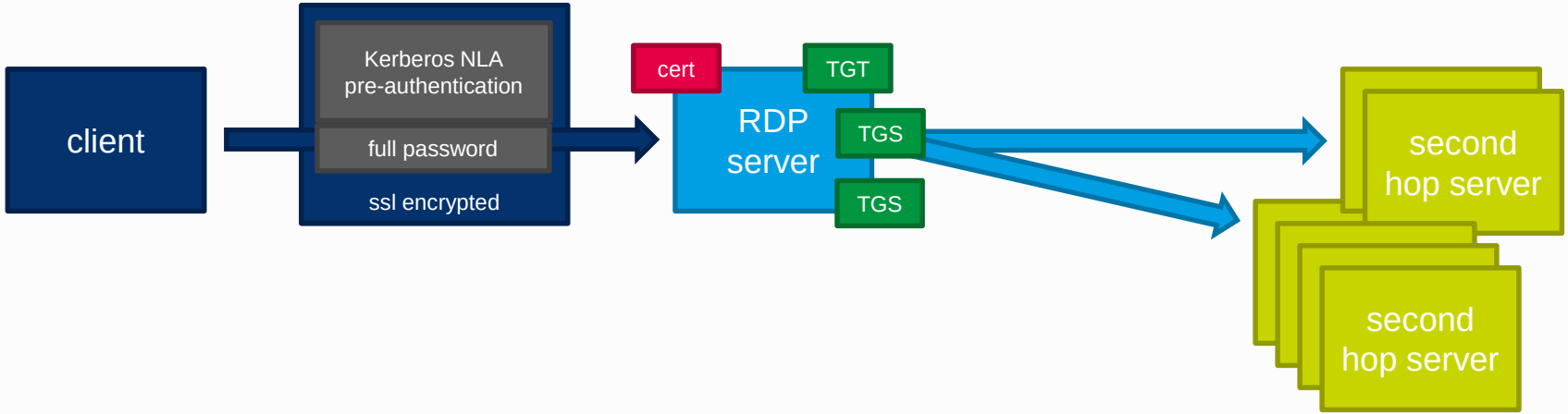
The problem

- clean password transport by default to enable SSO
  - SSL encrypted?!
  - transport on all versions, in-memory permanently until 2012 R2 and Windows 8.1
- compare with Enter-PSSession
  - double-hop authentication
  - Get-WSManCredSSP
  - Enable-WSManCredSSP -Role Client -DelegateComp
  - Enable-WSManCredSSP -Role Server
  - Enter-PSSession -Authentication CredSSP -Credential (Get-Credential)

The default scenario



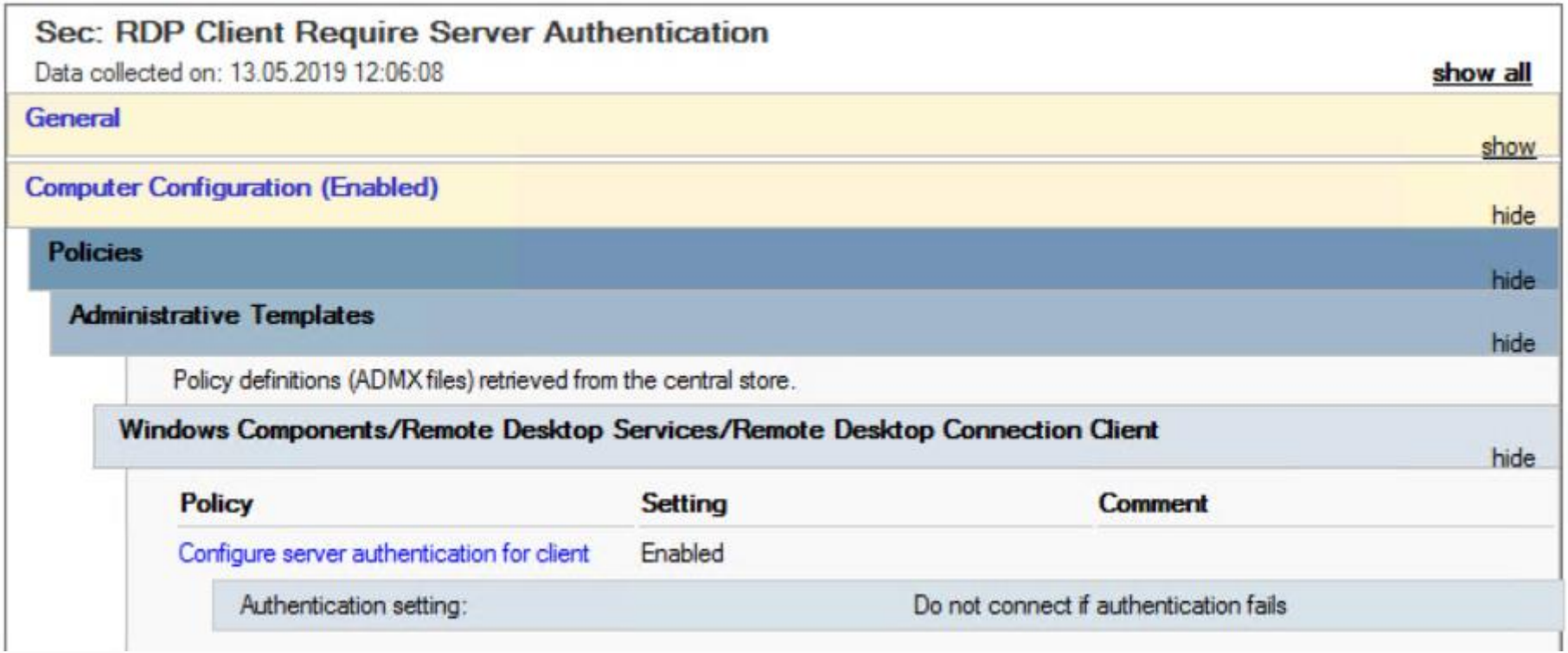
The default scenario



Transport protection

- never ever skip warnings!
- verify lock icon!
  - NLA
  - valid SSL certificate on non-Kerberos scenarios
  - Kerberos authentication
    - or both
  - servicePrincipalName: TERMSRV/rdp.gopas.cz

Require server authentication on clients



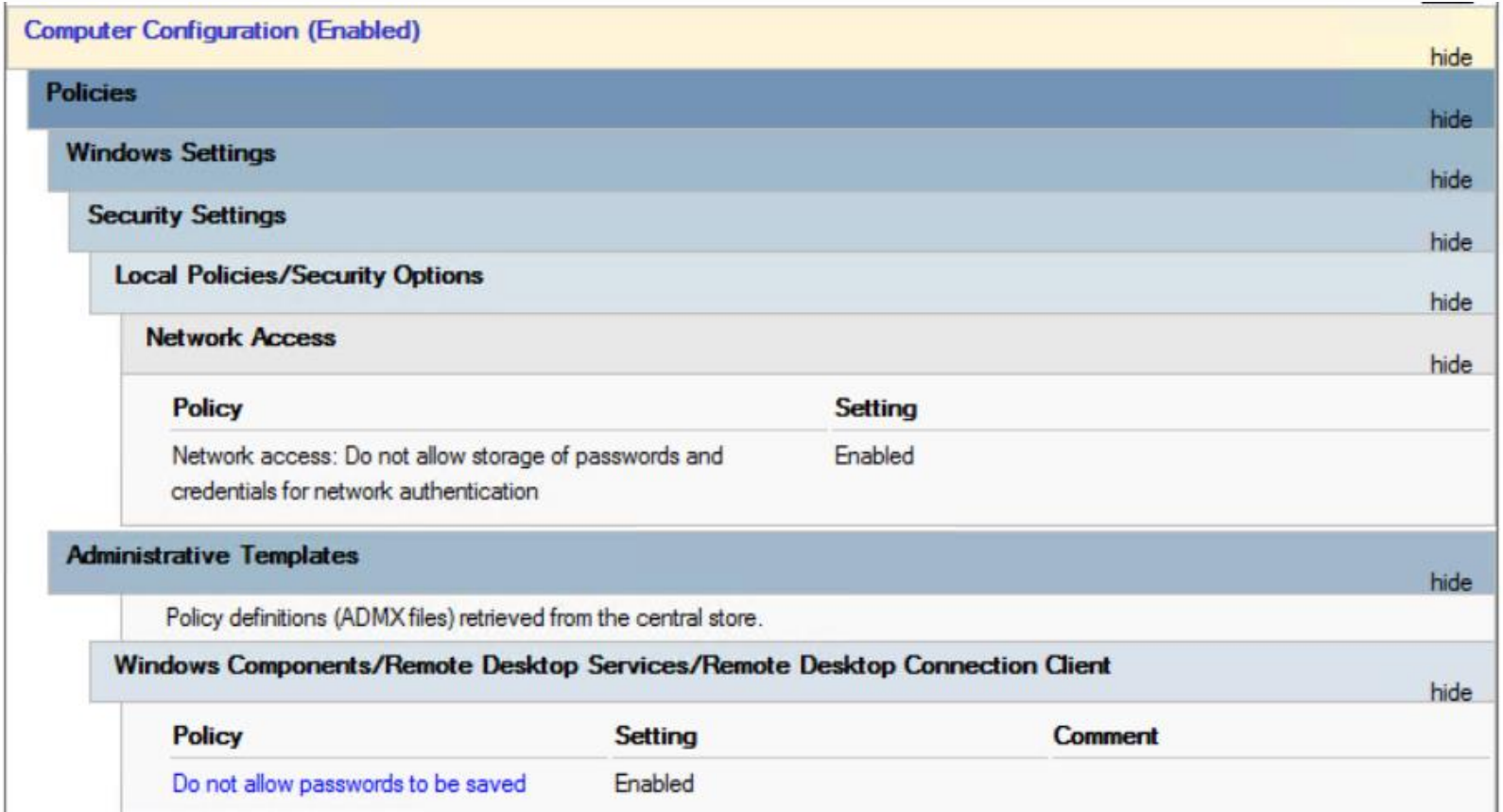
Two scenarios

- user access
  - limited user works on a secure server
- admin access
  - powerful privileged admin connects to insecure machines

User access

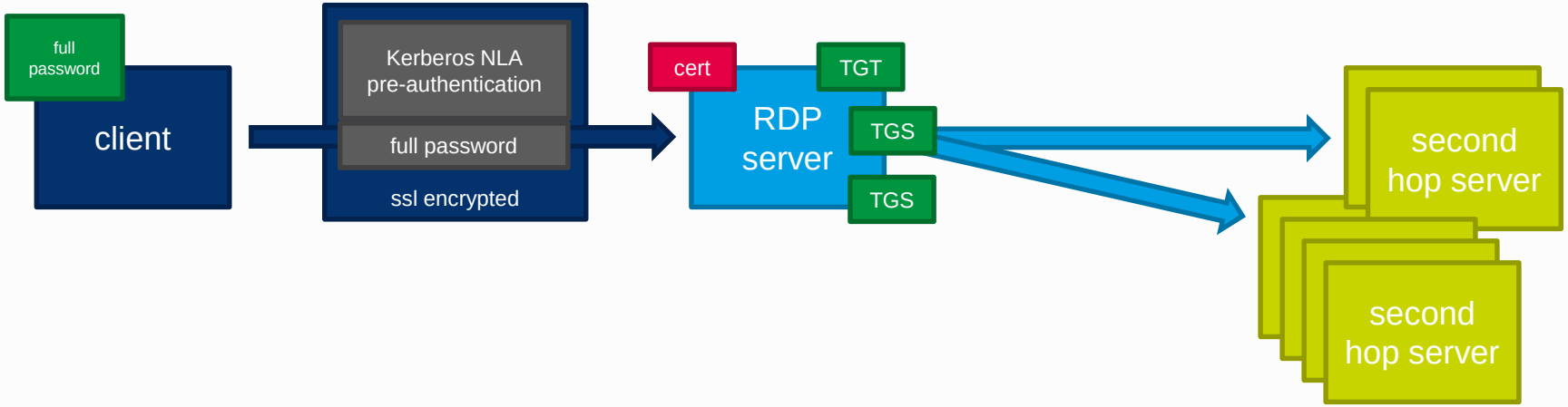
- limit password exposure
  - RDP SSO since Windows Vista/7/2008
  - prevent saving passwords
- never send clean password
  - /remoteGuard since Windows 10/2016
  - does not need Credentials Guard enabled on either side

Deny saving RDP passwords on clients

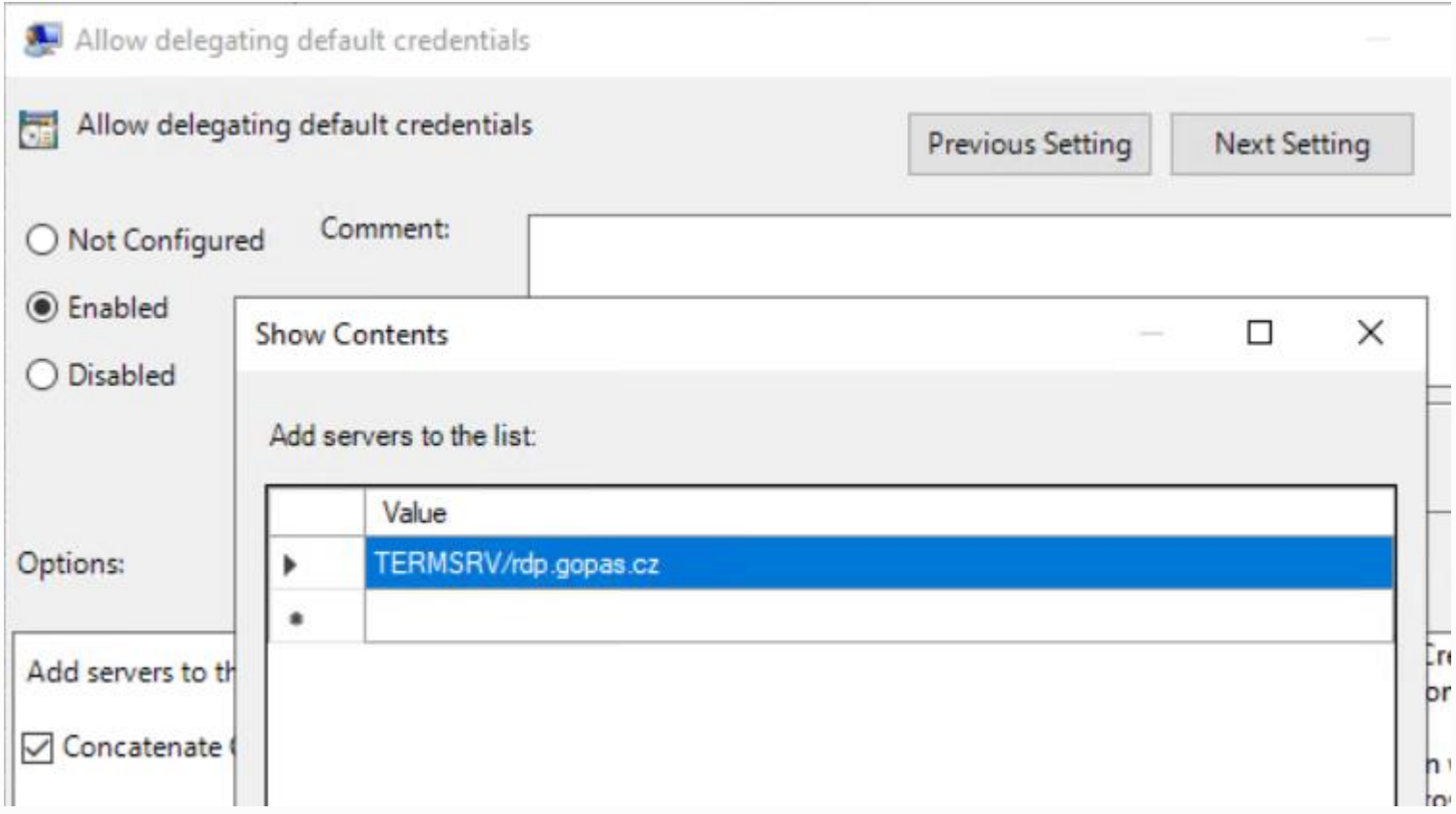


GOPAS
POCITACOVA.SKOLA.CZ

RDP SSO for limited users (2012R2/8.1 and older)

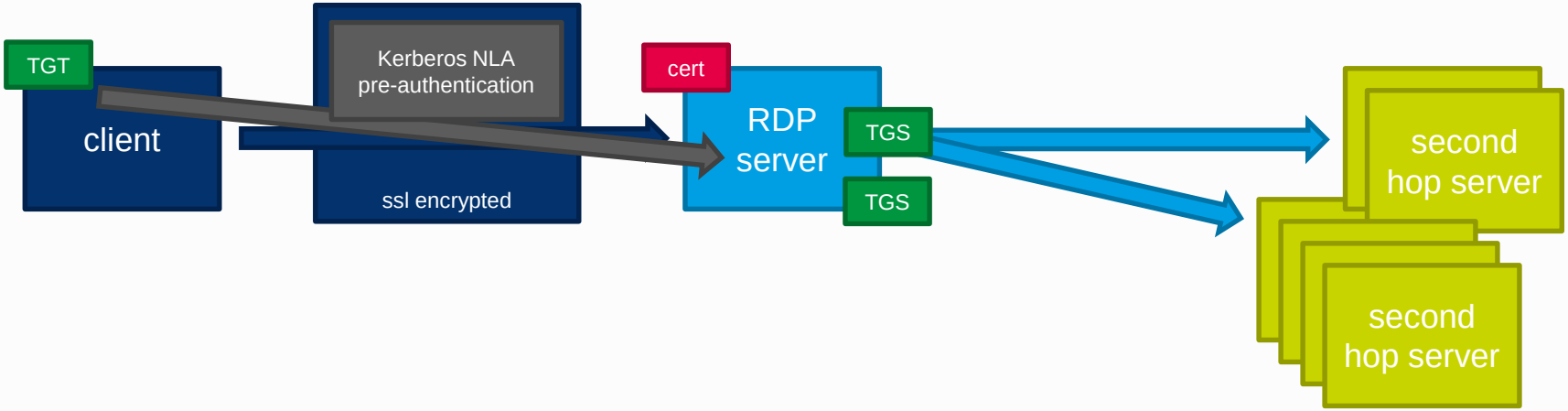


Client RDP SSO settings for standard users (2008/Vista/7+)



GOPAS
POCITACOVA.SKOLA.CZ

Remote Guard for limited users (2016/10 and newer)



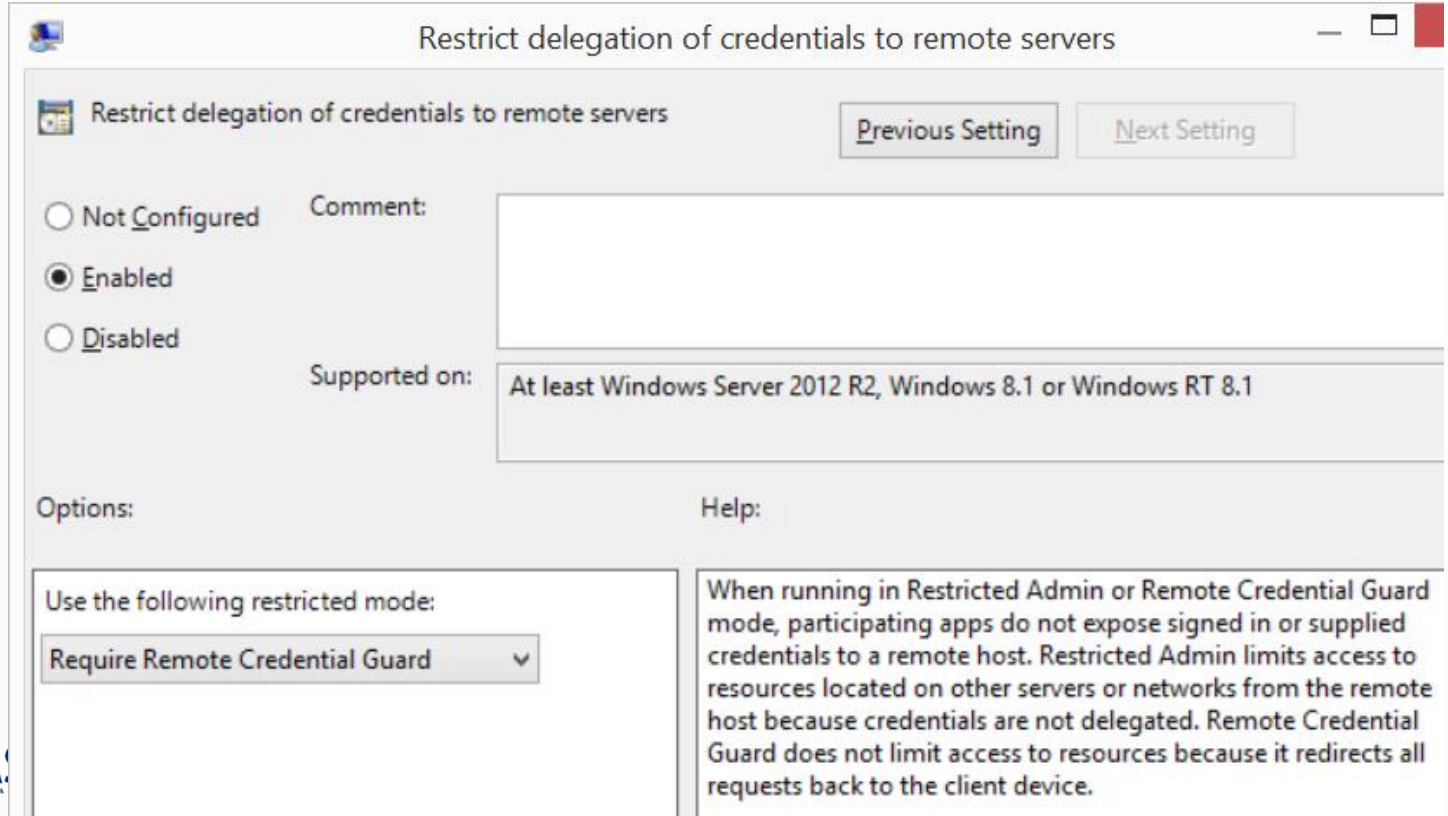
RemoteGuard requirements

- Kerberos server authentication + Kerberos user NLA authentication
- Windows 10.1607+, Windows 2016+

- HKLM\System\CurrentControlSet\Control\LSA
  - DisableRestrictedAdmin = DWORD = 0
  - must be enabled on the remote RDP server

- /remoteGuard cmd switch requires Administrators membership
  - user get "The requested session access is denied" for non-Administrators
- use GPO client enforcement for non-Administrators

Enforce RemoteGuard on clients with GPO for non-Administrators

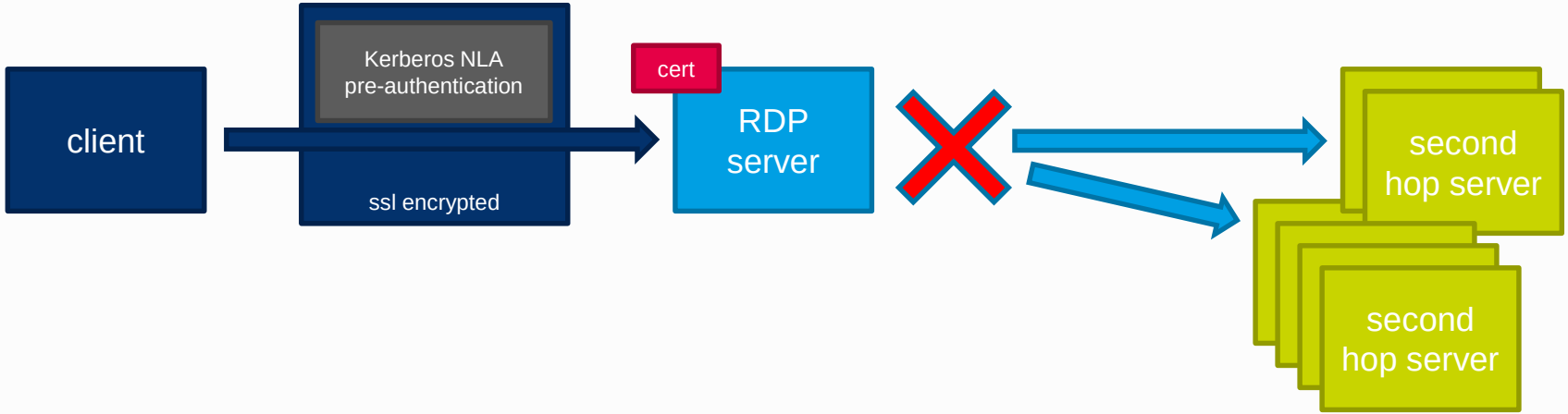


Admin access

- /restrictedAdmin
  - since 2012 R2/8.1
  - since 7/2008 R2 with update

- HKLM\System\CurrentControlSet\Control\LSA
  - DisableRestrictedAdmin = DWORD = 0

Restricted Admin mode (Windows 2012 R2/8.1 and update for 2008 R2/7 and newer)



Enforce restricted admin

- GPO forcing admin clients to use /restrictedAdmin
- Authentication policies
  - client with NLA
  - server even without NLA
  - Windows 2008R2/7 blocked by default

Děkuji za pozornost

moje kurzy v GOPASu

GLAB007 - capture the flag 1 - hackni si podnikovou síť
GLAB008 - capture the flag 2 - hackni si podnikovou síť
GOC175 - implementace bezpečnosti
GOC169 - ISO 27001
GOC172 - Kerberos troubleshooting

www.**gopas.cz**