Open Infrastructure - Task #7601

Setup an SSH jump host

01/13/2020 11:12 AM - Nico Schottelius

Status:	Rejected	**Start date:**	01/13/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
PM Check date:			

Description

- Authenticated against our ldap
- Allows user to connect to our IPv6 networks

The ways for users to use it:

- via ProxyCommand (some might be able to use that)

I've setup this some time ago and it basically needs a restriction on not having a shell.
Ping me before starting on this - I've a 95% solution already.

History

#1 - 01/13/2020 11:54 AM - Timothée Floure

- Status changed from New to Seen

- I am familiar with LDAP-backed auth with nslcd.
- ProxyCommand is standard for SSH bastions, it is even available on windows with Putty:
  https://fedora-infra-docs.readthedocs.io/en/latest/sysadmin-guide/sops/sshaccess.html#putty-ssh-configuration
  - What do you mean by 'some might be able to use that' ?

#2 - 01/13/2020 11:57 AM - Nico Schottelius

Proxycommand w/ windows exists in putty and usually uses plink - more details soon.

#3 - 07/22/2020 03:20 PM - Timothée Floure

@Nico Schottelius please dump anything you want to say on the subject on this issue. I'll do without next time I go over this issue :-)

#4 - 07/22/2020 04:02 PM - Nico Schottelius

Very easy:

- ssh config ("MatchUser != root") disallowing all commands
- configuring the OS or PAM to authenticate against ldap (subtree of dc=ungleich,dc=ch)
- Basically disallowing shell
- nft rules to allow to jump to 2a0a:e5c0::/29 and 2a09:2940::/29

So from the outside/black box test:

- ssh -w in ~/.ssh/config with our jump host should work
- ssh user@jumphost should not work / close the shell

#5 - 02/10/2021 09:04 AM - Timothée Floure

- Assignee deleted (Timothée Floure)

#6 - 09/10/2022 08:04 PM - Nico Schottelius

- Status changed from Seen to Rejected

Not much requested - dropping it for the moment