

Two-Factor Authentication, Usable or Not?

Richard Hosgood | Principal Systems Engineer



Who am I?

My Credentials

I am a Principal Systems Engineer for One Identity

I hold a Bachelors of Science Degree at Rochester Institute of Technology in New York.

I have been in the security industry for 10+ years.

I have deployed security solutions in top secret government facilities and at the top 10 fortune 500 companies. This allows me to see a plethora security environments in the world's largest companies.

Issues with MFA

Usability

Since a users may need to gain access to multiple devices at once and have to wait 60 Seconds in between the process can take too long and become unusable. If end users pushback enough they will push the business to not use it.

No End user Self Service Portal

User drops their phone or the phone breaks and the end user no longer has access to the their digital MFA tokens.

Limited integration

MFA provider does not work with all of our critical systems so it cannot be implemented corporate wide.

Why One Identity Starling is easy to use

Usability

We have built in MFA caching for users who need to authenticate to multiple systems at any given time. This is time based and connection limited

End user self service portal

By having a end user self service portal they can re-issue tokens to their device in the matter of seconds.

Integration connectors



AmazonS3AWS

Crowd

Crowd



Dropbox



Facebook Workpla
ce

JS

JIRA Server

RSA

RSA Archer



Salesforce

SAP

SAP Cloud Platfor
m

SN

ServiceNow

SF

SuccessFactors

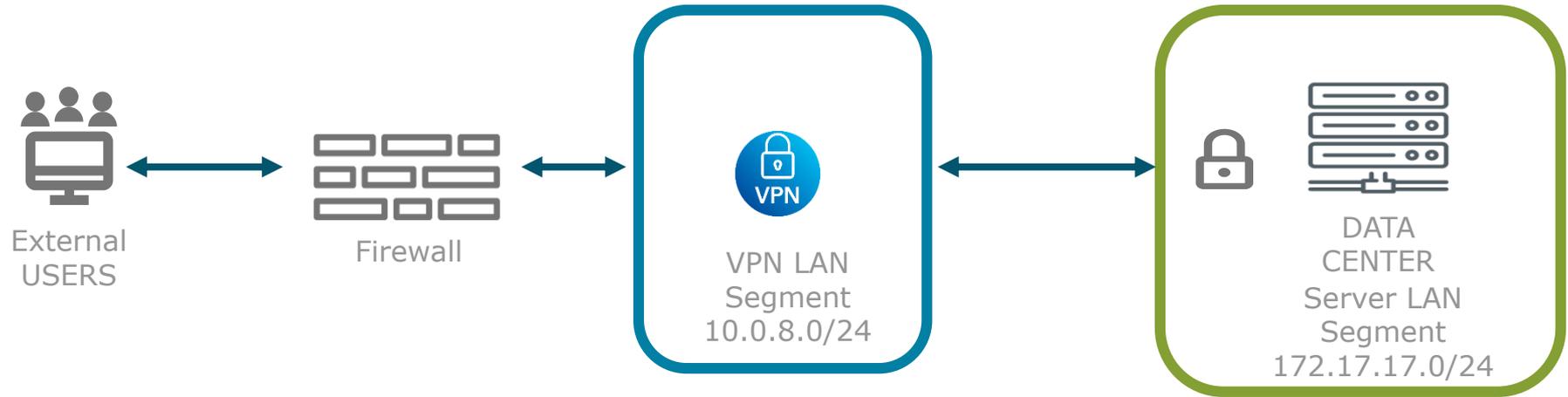
One Identity Starling MFA/ SAAS



Starling MFA Integration points

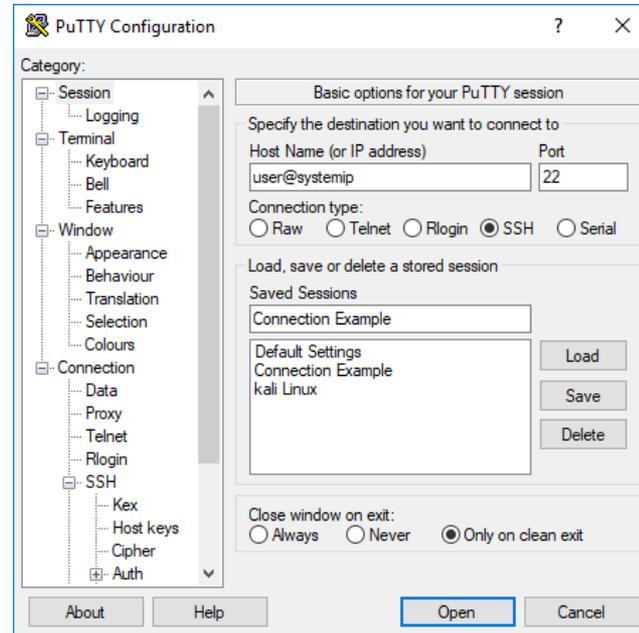
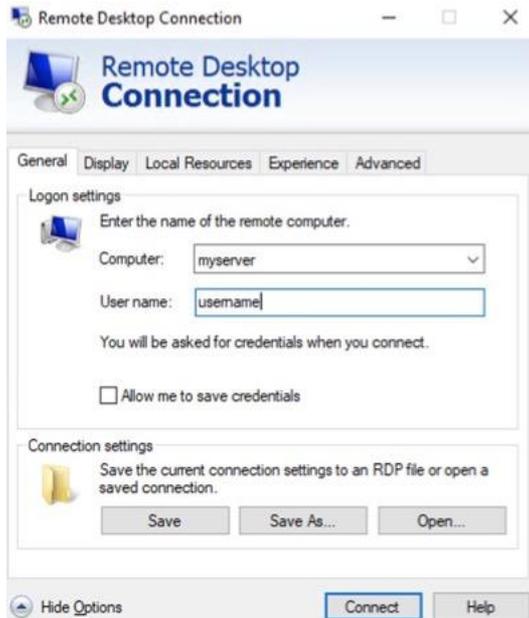
- Remote Desktop Protocol
- SSH
- Salesforce
- Facebook Workplace
- SAP Cloud Platform
- Jira Server
- RSA Archer
- ServiceNow
- Workday
- SAP SuccessFactors
- Amazon AWS
- Amazon S3
- Dropbox
- Atlassian Crowd Users/Groups management

Common external access for contractors into corporate infrastructure

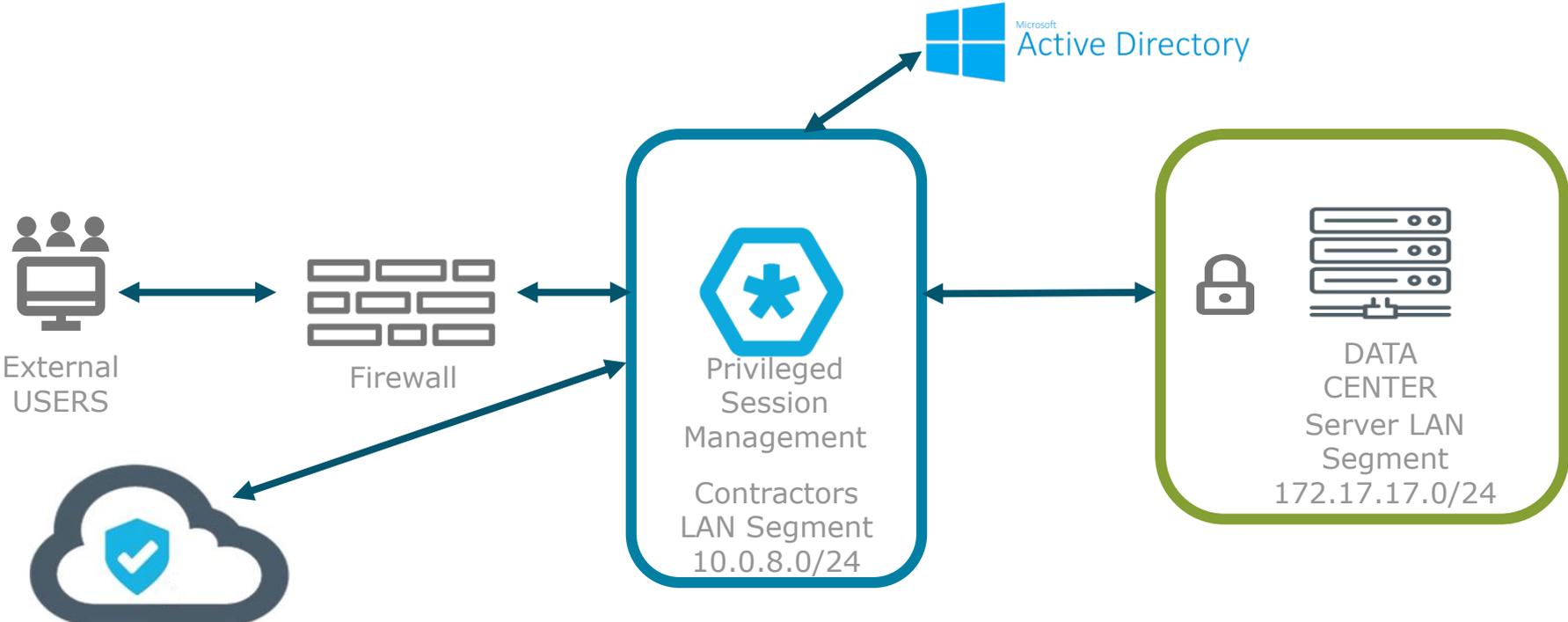


MFA combined with SSH and RDP connections

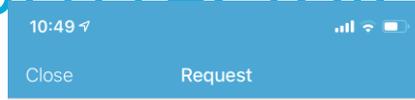
MFA is not compatible with remote connections to critical infrastructure via RDP and SSH.



Privileged access management direct access with multifactor.



IMPLEMENTING MULTIFACTOR FOR RDP SSH



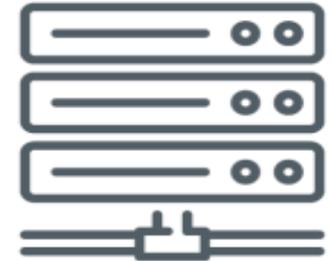
ONE IDENTITY

PSM Gateway Authentication

Protocol: RDP
Gateway: scb.bblab
Client IP: 172.20.20.157
Date: October 07, 2018 at 10:49
Server User: richard.hosgood



RDP/SSH CONNECTION



DATA CENTER





To find out more go to: <https://www.oneidentity.com/PAM>