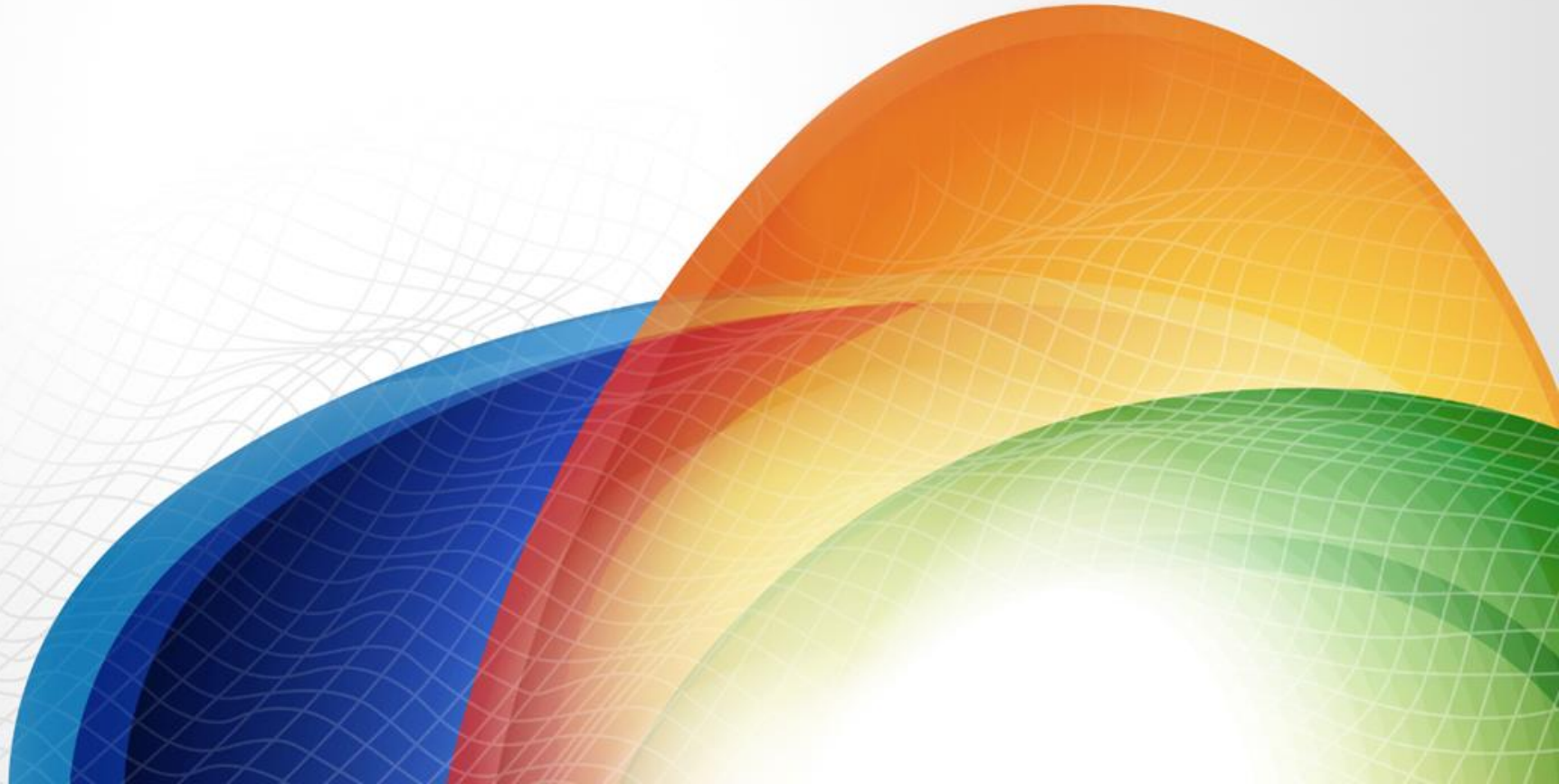
SSH Proxy

Security Sales Manager

r.kim@f5.com

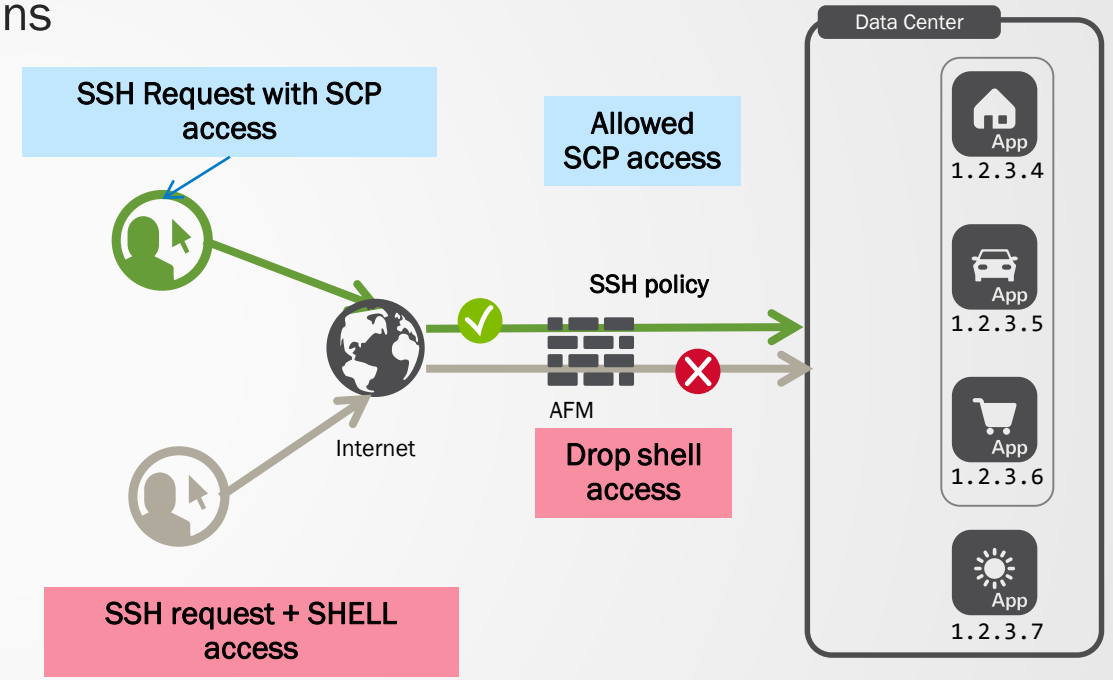
김민영 이사



New Protection for Admin Access to DC Assets: SSH Proxy

Customer Problems

- Customers don't have visibility into SSH connections
- Customers would like to Detect and control the commands that are issued within SSH connections



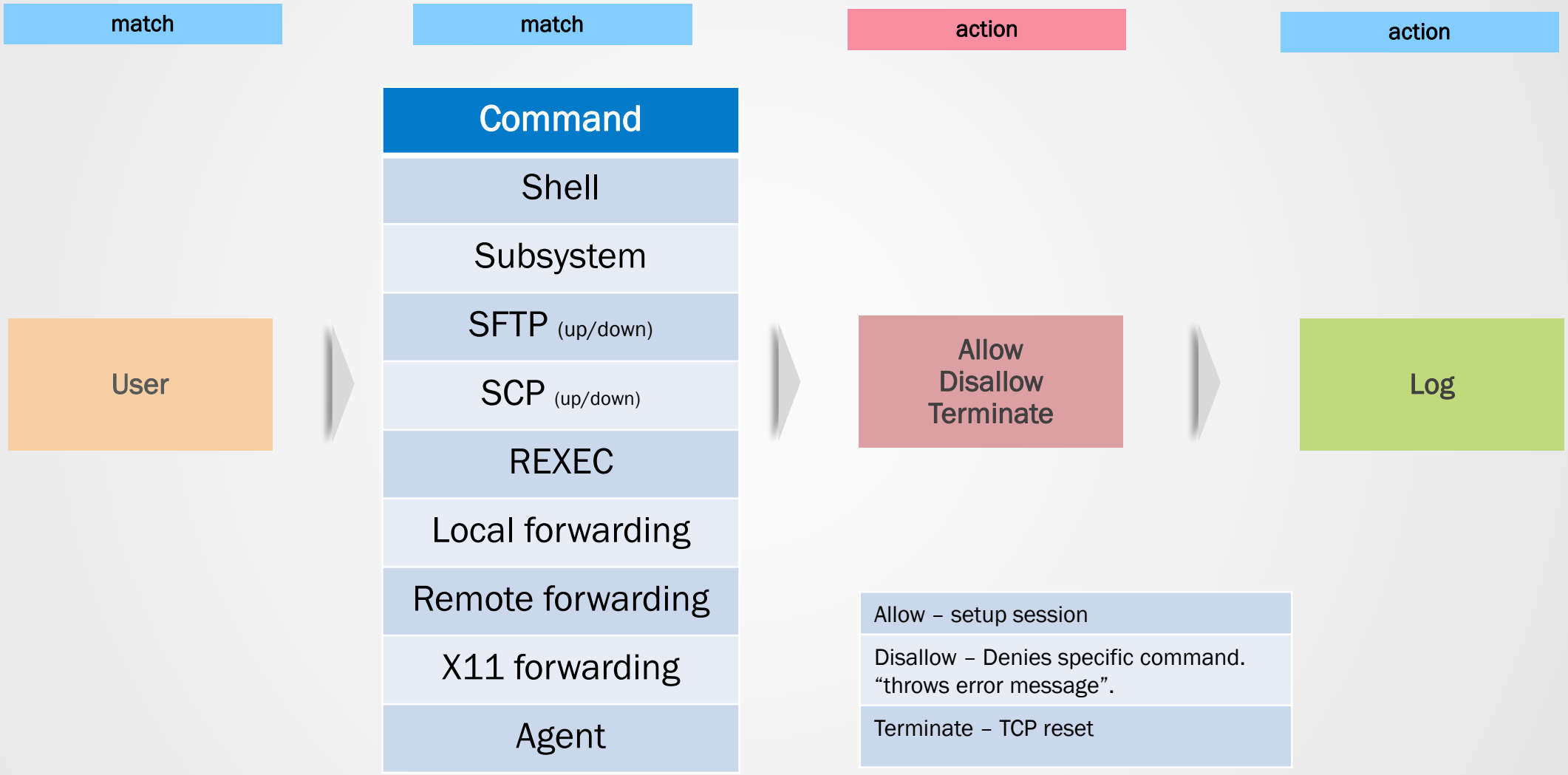
Solution

- Policy-Based SSH Control Capability
- Bring Visibility and control into SSH connection
- Enhanced protection of DC against attackers

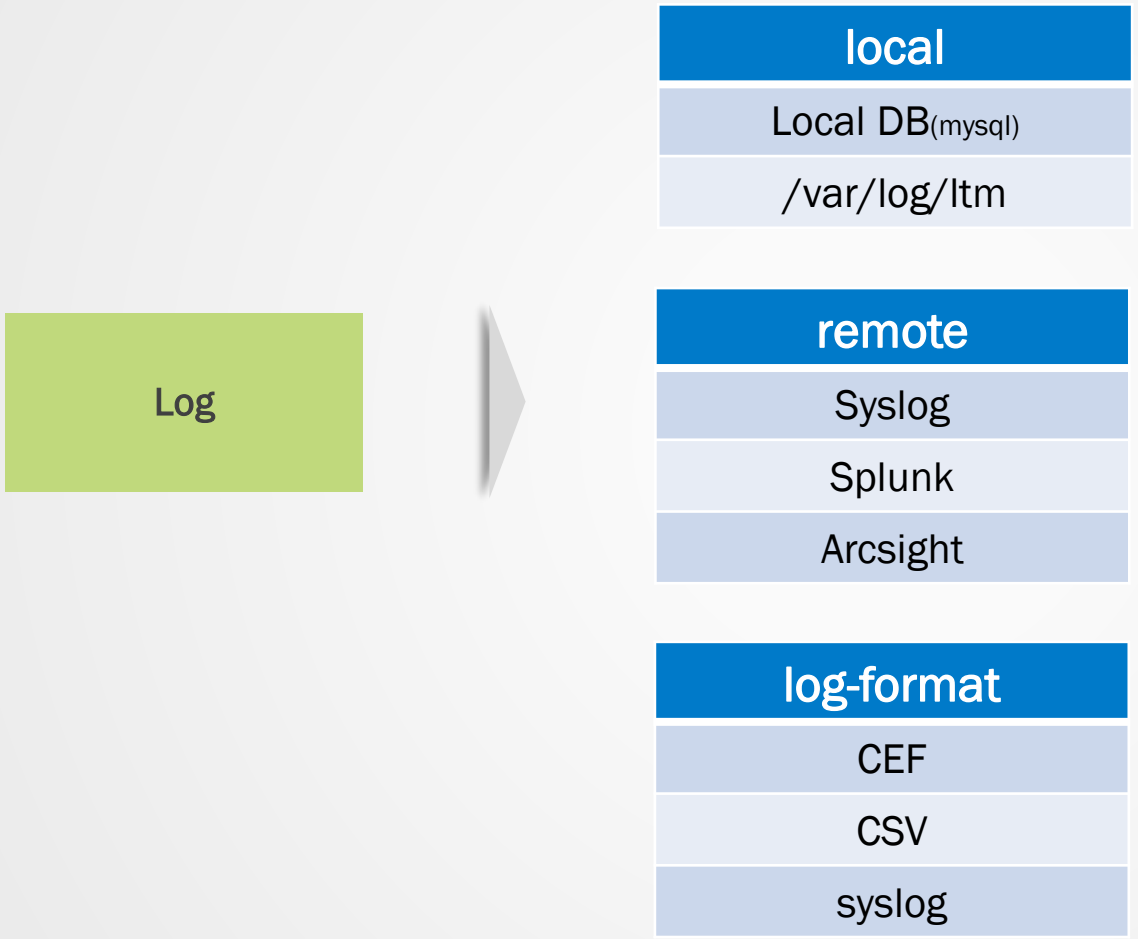
SSH Commands we detect

Command	Direction/comment
Shell	shell access
Subsystem	alias commands
SFTP	upload/download
SCP	upload/download
REXEC	execute remote commands
Local forwarding	forward a local port to a remote server
Remote forwarding	remote server accessing a local port
X11 forwarding	allows forwarding of X11 connections
Agent forwarding	ability to hop from one system to other

SSH Rule Construction



Log support

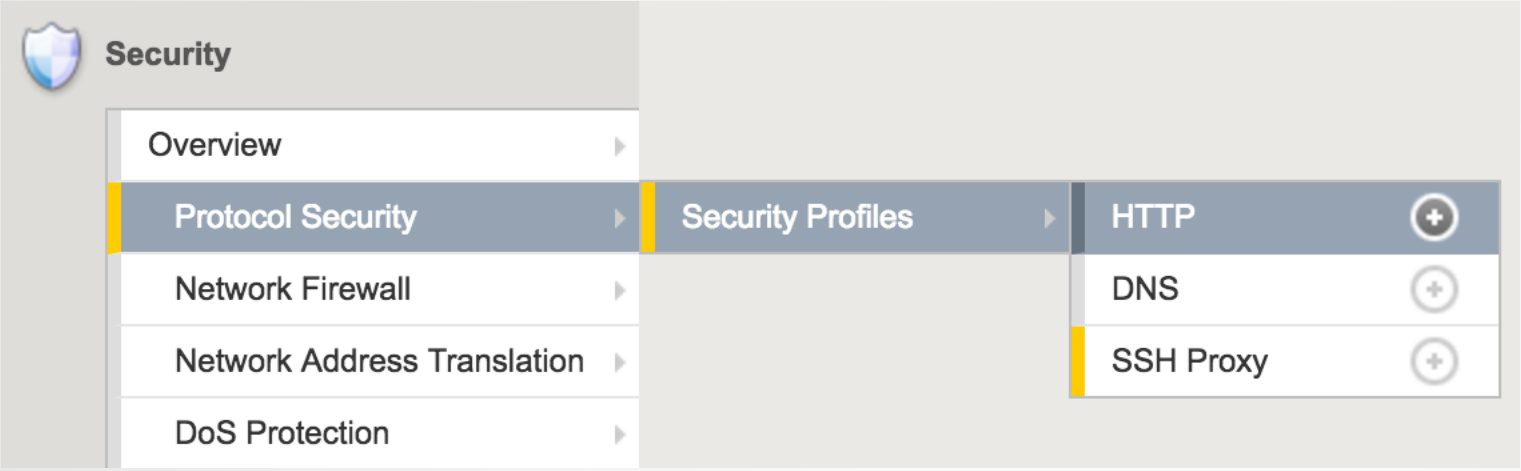


SSH Proxy

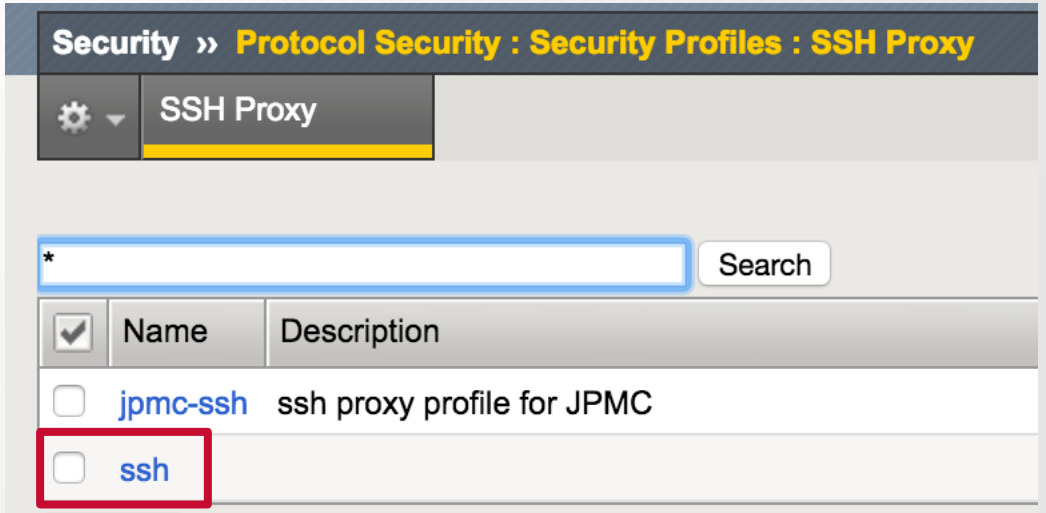
- Available with Cascade release (12.1)
- Available with AFM License
- Support for SSH client/server with Version 2.0 or above only
  - Rekeying is done every one-hour or after 1Gb of transfer
- Presented under Protocol Security in UI
- SSH sessions can be timed out
  - SSH profile supports idle timeout
  - Out-of-box (default) SSH profile is available
  - default rule allows all known SSH commands

SSH Proxy profile

- Security > Protocol Profiles



- Default SSH-Proxy profile (ssh)



SSH Rule Configuration

Profile Properties

Profile Name	ssh
Description	JPMC SSH profile
Timeout	0 seconds

SSH Proxy Permissions | Key Management

Filter Rules

Add New Rule

Name	Users	Shell	Sub System	SFTP Up	SFTP Down	SCP Up	SCP Down	REXEC	Forward Local	Forward Remote	Forward x11	Agent	Other
Allow-Download	contract-user *user* add new user Add	Disallow Log	Disallow Log	Disallow Log	Allow Log	Disallow Log	Allow Log	Disallow Log	Disallow Log	Disallow Log	Disallow Log	Disallow Log	Allow Log
Allow-upload	DCUser	Disallow Logging	Disallow No Logging	Allow Logging	Disallow No Logging	Allow Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Allow No Logging
DC-Access	k.somu somu	Disallow Logging	Allow No Logging	Allow No Logging	Allow No Logging	Allow Logging	Allow Logging	Allow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Allow Logging
DC-Admins	Jon Sam Adam pinky	Allow Logging	Allow Logging	Allow Logging	Allow Logging	Allow Logging	Allow Logging	Allow Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Allow No Logging
Default Actions		Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging	Disallow No Logging

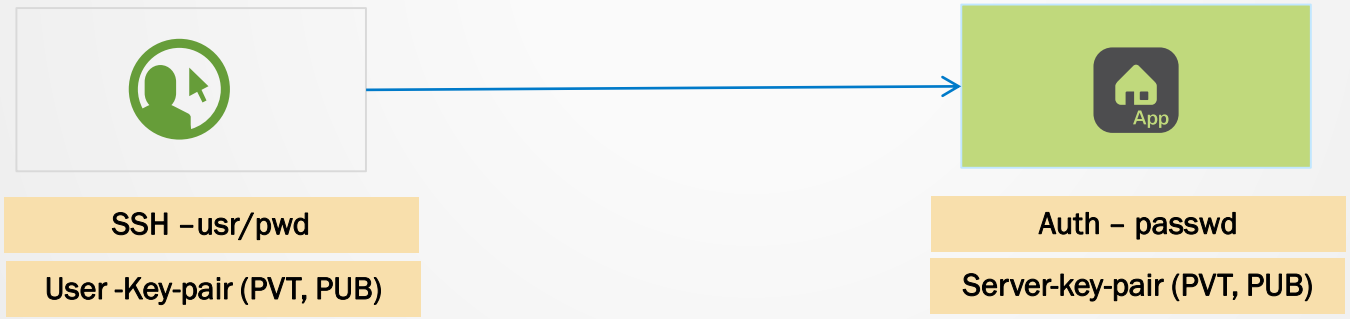
Done Editing Cancel

Contractors were given access to download but not upload

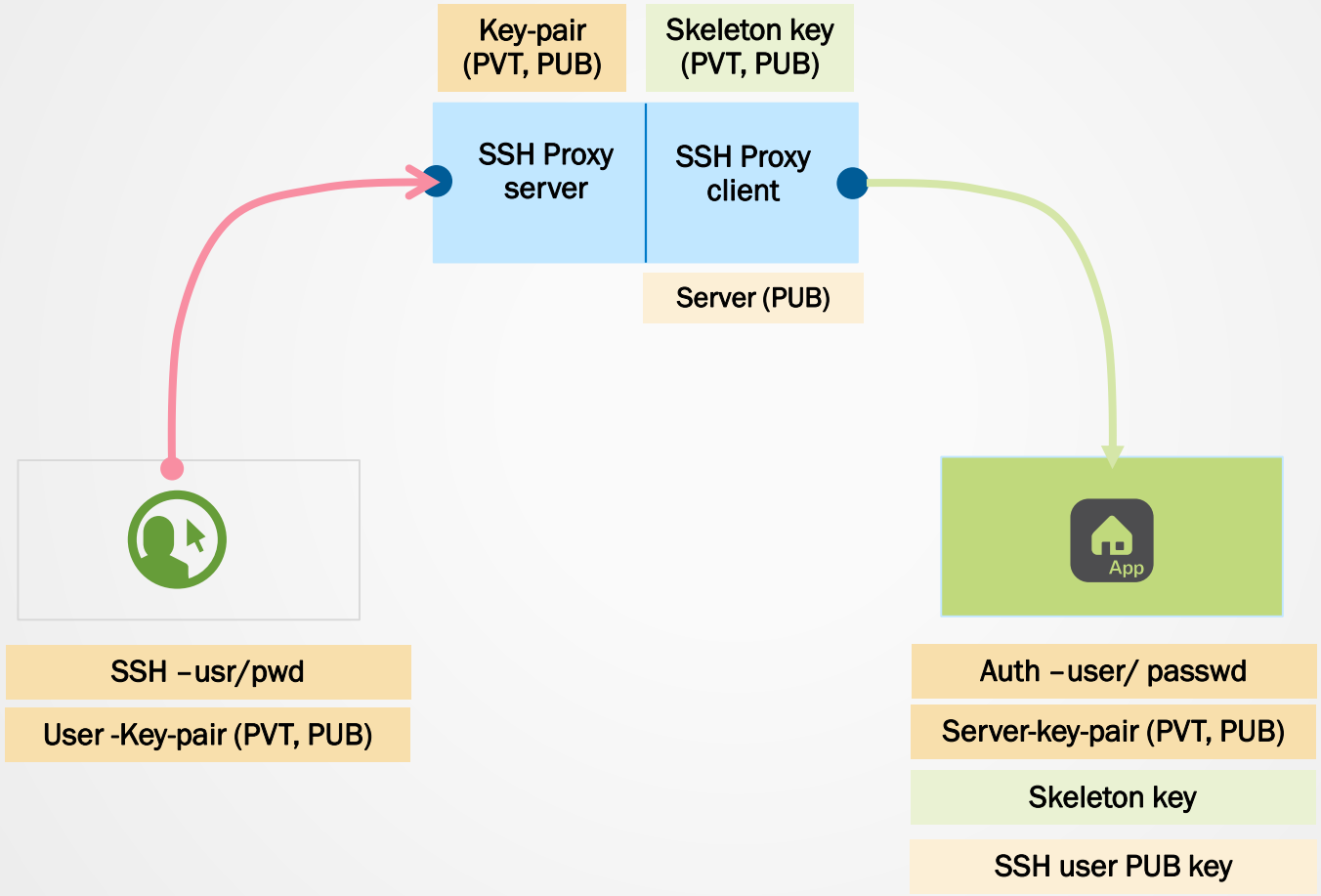
Authentication methods supported

1. SSH Key (public key)
2. password
3. Keyboard-interactive

User SSH Access



SSH access with AFM inline



SSH-Proxy key management

Profile Properties

Profile Name	jpmc-ssh
Description	ssh proxy profile for JPMC
Timeout	0 seconds

SSH Proxy Permissions | Key Management

Add New Auth Info

Name: jpmc-rsa Delete

Proxy Client Auth

Public Key

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEA4mjTbW2EAorBjvxZ3AJvMnZX+r0qduMFECeIgTm9cgGIyeXfxq52RLnw54naOnE+sCO8vgP
SfvF7zw1LJOMIYOfyQj7HKpmEl
```

Private Key

```
$M$PE$IiGRJzPa05dAS6BLhU1jqA1ErxB91VGJ1W34OxC3dUMProbd/gOXGf07i4V9tGfOWFaqFrsFlD7hIXLoVm2FsEoOasIzU
k/p1OYAgEOdAXd07K24DMmd7Q5S+CYYj2cNQKTRZR+9KcXHI//U8LYq8Chfd7dd1lSxxXFbhr/bDmXFEbiPq5EdrXgWSBfdqYDi
Cy53+41rUU6LwahEnl8GW7y63SVLzDcDjK3LDyKQy7MwDLbFOZBtVEHIia3M73E2njlwv2KXonlSa62bM43WFQsnDrZ+uz5WxNj
```

Proxy Server Auth

Public Key

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEA4mjTbW2EAorBjvxZ3AJvMnZX+r0qduMFECeIgTm9cgGIyeXfxq52RLnw54naOnE+sCO8vgP
SfvF7zw1LJOMIYOfyQj7HKpmEl
```

Private Key

```
mYZo7ZcpAo/3lKwZhZFO7hgBQSIq+ggwhS77BDQOqkCIG23LLz43/SINSDLIUf3XeADm3IkWOgQdXCHKMJoeufaHEFEex+HSAj2
89VdWASAtYkT5pMKdYSxCRUG9/bAuX24LDm14fgj8dutpIC5hnSvecer+8hpivUeMKD9+tKNYjIagV9hqNfUQufaYLIL6V4oZQq
7cy+WLJ+o9dvD8rlkA6omy7dt6jRzVsuP6rRlvMeiGpMnyYVfCBC5bZP8ce8bOmOYwVQsBLGid8aByw90orB5nB4pXeG/67g6gK
```

Real Server Auth

Public Key

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC22argU16evd1ZZmTTJ3gPuiBmDPmia/XONSlZXgUieIQdhzGKVdc5+9nGIsqvZyJcKPu
3lAxjz5W6ly4f0vuYX0KZhN6xrP++Xd5ou6b01HANtY/HdCQEiLNeSXTAuHz2tZ2KIkWZ0CllJwzCMghQPX3Biv3zSQ/wL4vLN6
```

SSH Proxy Configuration

1. Create a SSH profile
    1. Create user based rule to control SSH commands
        - Actions – Allow/Disallow/terminate
        - Log – optional
    2. Setup Authentication information
        - Proxy-Server Auth Keys (pub, pvt)
        - Proxy-Client Auth Keys (pub, pvt)
        - Real Server Auth (pub)
2. Apply the SSH profile in a VS
3. Create a log Profile
    - Associate a log publisher

Log Profile

```
security log profile ssh-log {
    ssh-proxy {
        ssh-log {
            allowed-channel-action enabled
            disallowed-channel-action enabled
            log-publisher syslog-publisher
            successful-client-side-auth enabled
            successful-server-side-auth enabled
            unsuccessful-client-side-auth enabled
            unsuccessful-server-side-auth enabled
        }
    }
}
```

```
sys log-config publisher syslog-publisher {
    destinations {
        local-syslog { }
    }
}
```

Log Messages (/var/log/ltm)

SCP download example – policy with action - Allow

```
root@ubuntu-desktop:~# scp user@10.10.10.2:/home/user/test .
test                                          100% 8980     8.8KB/s   00:00

Mar 28 16:24:10 SSHProxy info tmm[18280]: 23003164 "Mar 28 2016 16:24:10","ssh_clientside_auth_success","10.10.10.1","10.10.10.2","23
993","5632","2560","TCP","user","Public key authentication success"
Mar 28 16:24:10 SSHProxy info tmm[18280]: 23003165 "Mar 28 2016 16:24:10","ssh_channel_action_allowed","10.10.10.1","10.10.10.2","239
93","5632","2560","TCP","user","SCP download"
```

Log Messages (/var/log/ltm)

SCP upload example – policy with action Terminate

```
root@ubuntu-desktop:~# scp test-2-server user@10.10.10.2:/home/user
Connection to 10.10.10.2 closed by remote host.
lost connection
```

SCP upload example – policy with action Disallow

```
root@ubuntu-desktop:~# scp test-2-server user@10.10.10.2:/home/user
Received disconnect from 10.10.10.2: 11: This user is not authorized to do SCP uploads.
lost connection

Mar 28 16:31:13 SSHProxy info tmm[18276]: 23003164 "Mar 28 2016 16:31:13","ssh_clientside_auth_success","10.10.10.1","10.10.10.2","24
249","5632","2560","TCP","user","Public key authentication success"
Mar 28 16:31:13 SSHProxy info tmm[18276]: 23003165 "Mar 28 2016 16:31:13" "ssh_channel_action_disallowed","10.10.10.1","10.10.10.2","
24249","5632","2560","TCP","user","SCP upload"
```

Solutions for an application world.