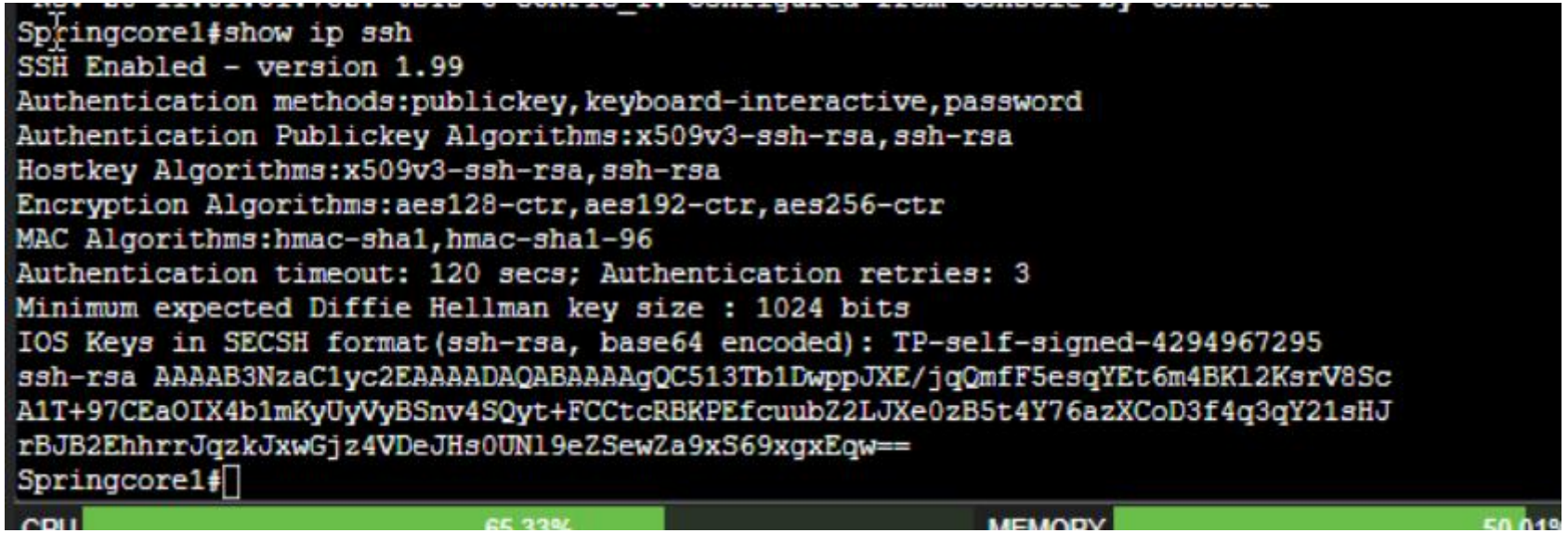
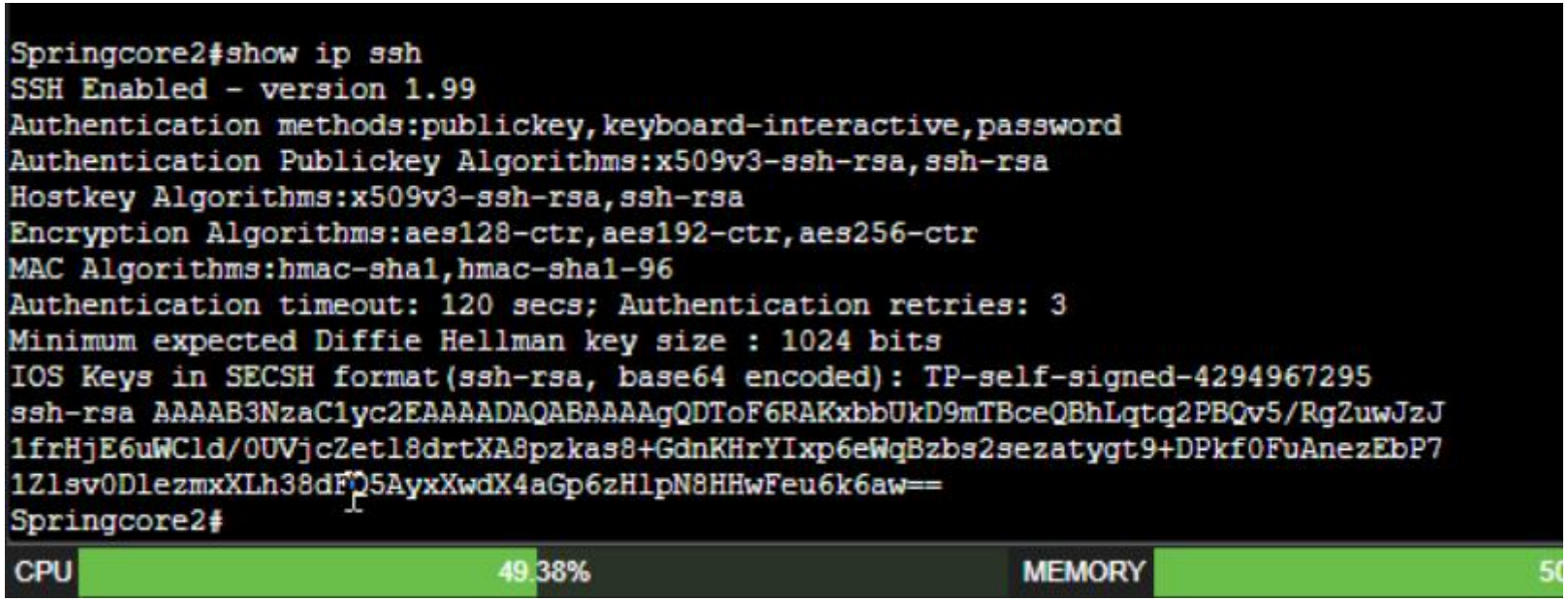
Technical Project Task 3

Advanced Security and Acl setup

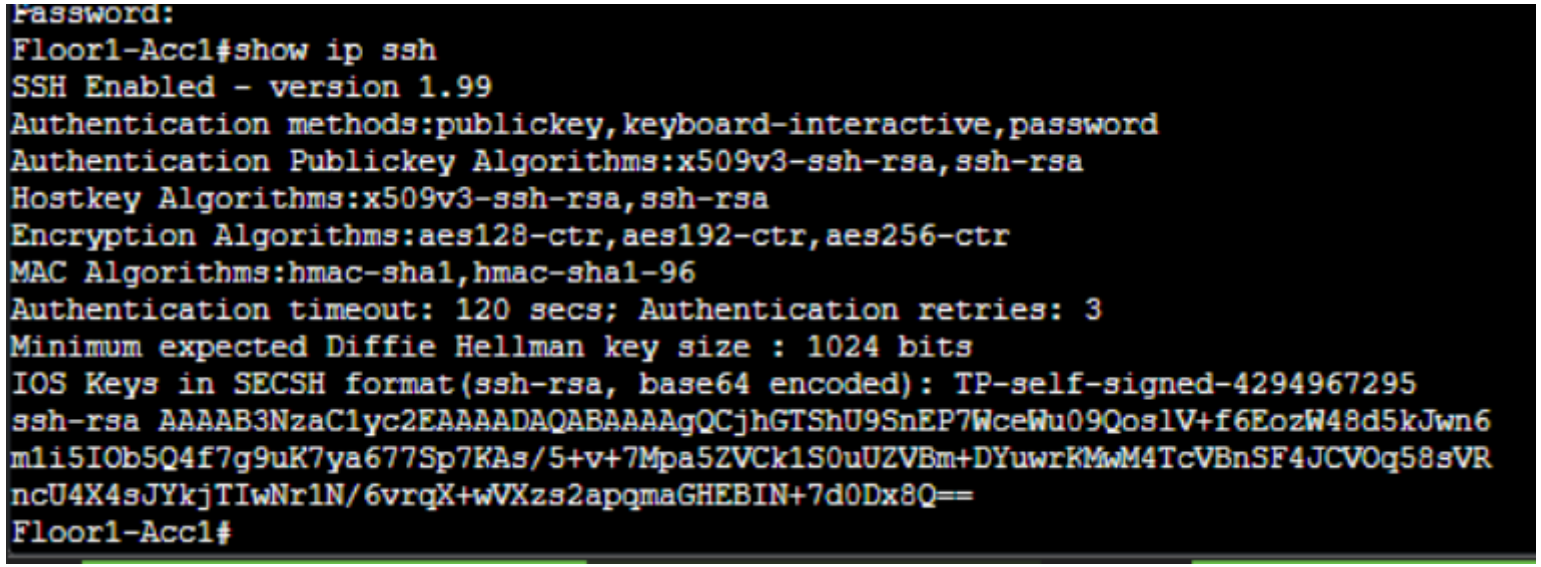
SpringCore1



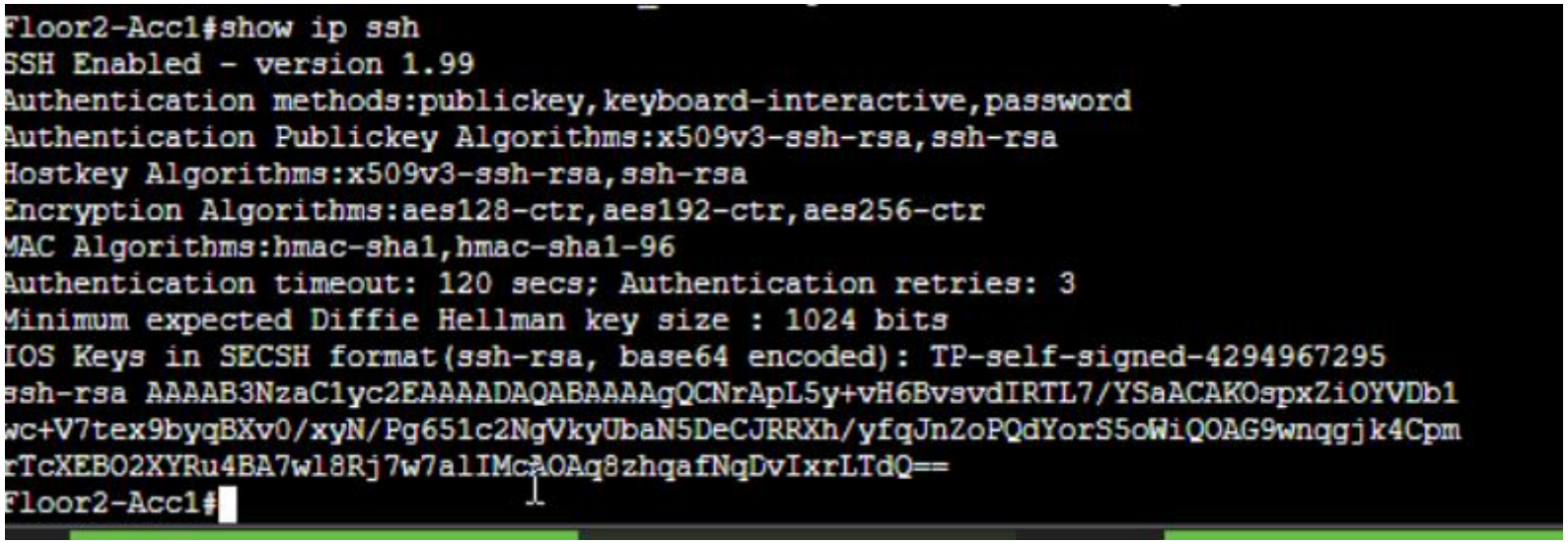
SpringCore2



Floor1-Acc1


Password:
Floor1-Acc1#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-4294967295
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCjhGTShU9SnEP7WceWu09QoslV+f6EozW48d5kJwn6
m1i5IOb5Q4f7g9uK7ya677Sp7KAs/5+v+7Mpa5ZVCk1S0uUZVBm+DYuwrKMwM4TcVBnSF4JCVOq58sVR
ncU4X4sJYkjTIwNr1N/6vrqX+wVXzs2apqmaGHEBIN+7d0Dx8Q==
Floor1-Acc1#

Floor2-Acc1


Floor2-Acc1#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-4294967295
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCNrApL5y+vH6BvsvdIRTL7/YSaACAKOspxZiOYVDb1
wc+V7tex9byqBXv0/xyN/Pg651c2NgVkyUbaN5DeCJRRXh/yfqJnZoPQdYorS5oWiQOAG9wnqgjk4Cpm
rTcXEBO2XYRu4BA7wl8Rj7w7alIMcAOAq8zhqafNqDvIxrLTdQ==
Floor2-Acc1#

Floor3-Acc1

```
Floor3-Acc1#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-4294967295
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCmdf6tTwo5/GQVzOmt2PDOC16m2TL6XvyUHfTGPcjG
70/EiI/7HIZ/qZU3/nI8FIVD2Au+pR0XowuayC7S6laJQPXgchDglq0eRrJkDrrAzT0EdIJRjw37Sc+N
eghUCFQi5ewE+SZtzOGCff0tNklNBguUcYnfE1QhI3IH35N1nQ==
Floor3-Acc1#
```

DataCentre

```
Datacentre#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-4294967295
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQC56ev6EAcEKuB2NAexcI+KBhodub6/vwIuPQs9qKef
bGcNRXIxYLxTd9MV1dyu2DBmVUSC69gs66YEV5rJix3iXL6Eawnymk7uYiOQr8W6P7zIr8xDrem81IN1
nv4RrtBhlC8pEM2Vt/JhRW36LREiqvlFIhneXBD3KkK/+UXXAQ==
Datacentre#
```

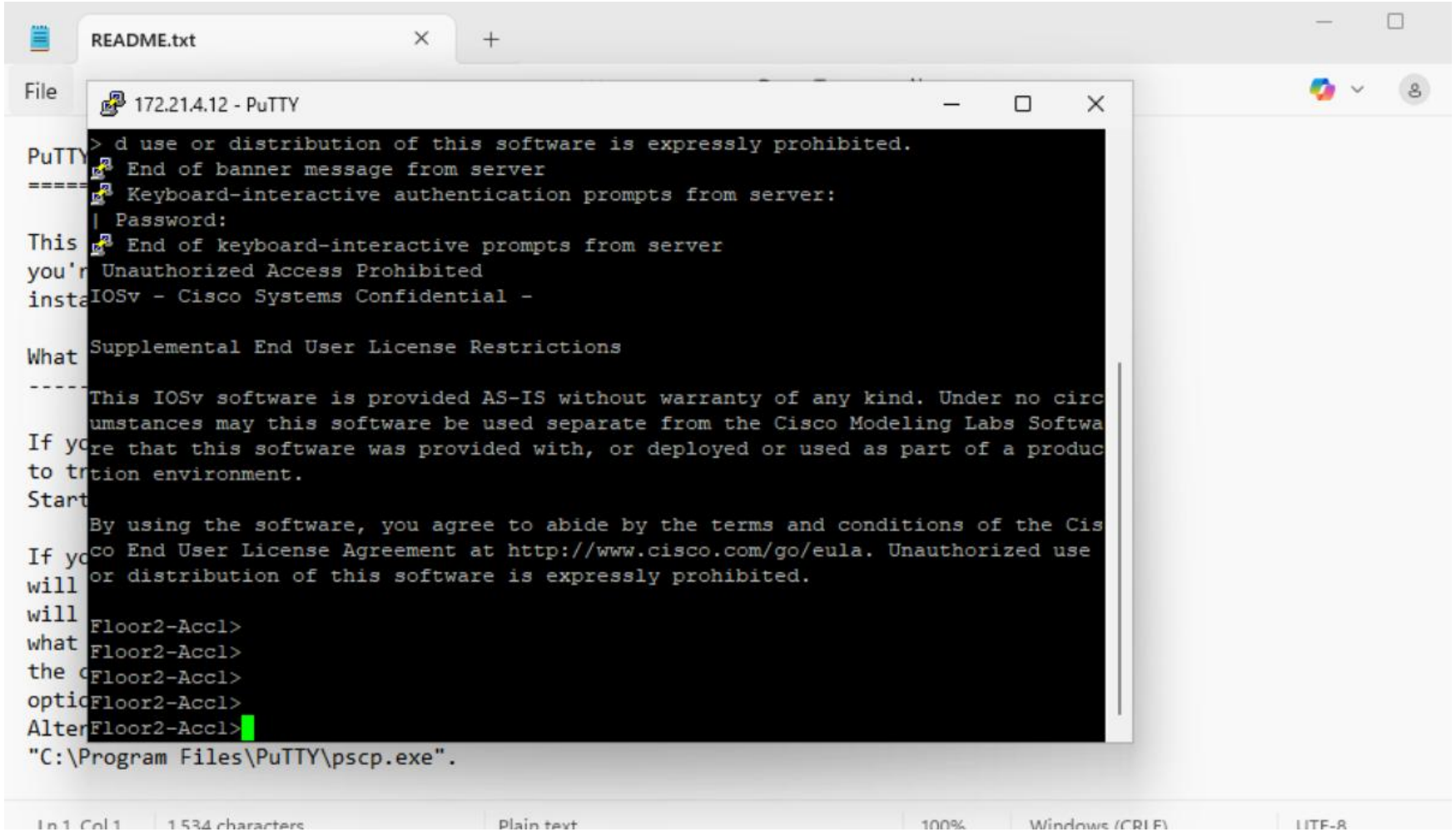
SpringR1

```
SpringR1#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96
KEX Algorithms:diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): SpringR1.shmc.local
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQC7ljpI6Zqg7CJOSz5AY4ZTi5FhJDOmouZeYPALZZPq
ZhAvzM/E3ybQi+f6dJG7RgDsyYZTi0+za/2EWxrU0hMssQozJA8vhj4bnRbVZW0RwVt8mrU+2+Qbvr7r
/R/Z1gyWHQLLXpQRizrIU80eYZqf28PTbpp70HfzsswEQzfbNw==
SpringR1#
```

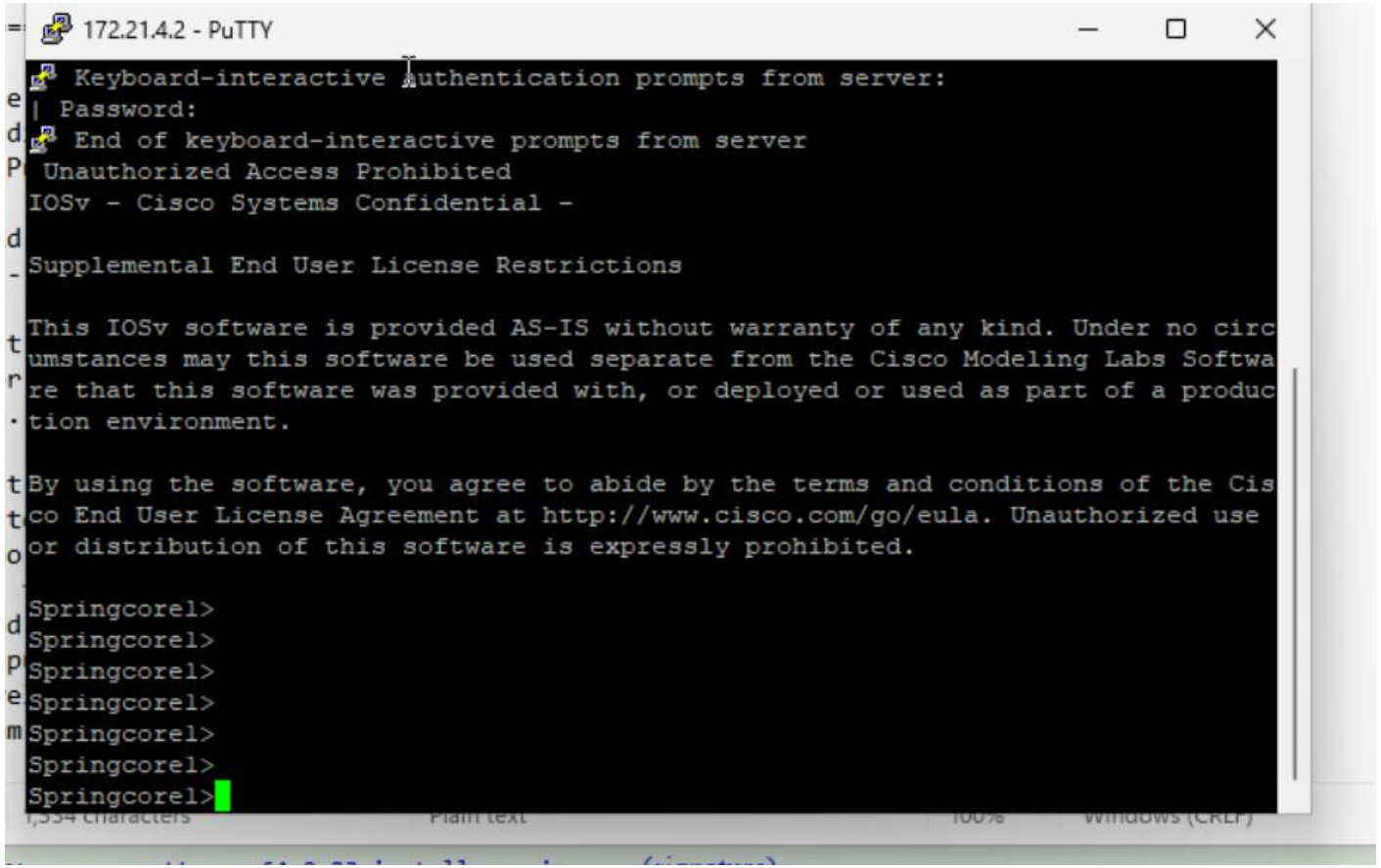
SpringR2

```
SpringR2#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96
KEX Algorithms:diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): SpringR2.shmc.local
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDN/Ow+Tgh45mSefd2Xf8KnjiKgaRLcAlria97mPE81
N/XmGVf56tnBGJuZzCRTqTp32JrRTKdCrAMCLZrl7uhZn0jjhBuMTLBX2rf4qR/CDc7/mXnJX44E3lKA
vRh6bzKNPlO4Ma+SDKtwJRkWshh/qBXxYFRzRaKMl+5WlvnNJQ==
SpringR2#
```

SSH from Client2 > Floor2-Acc1

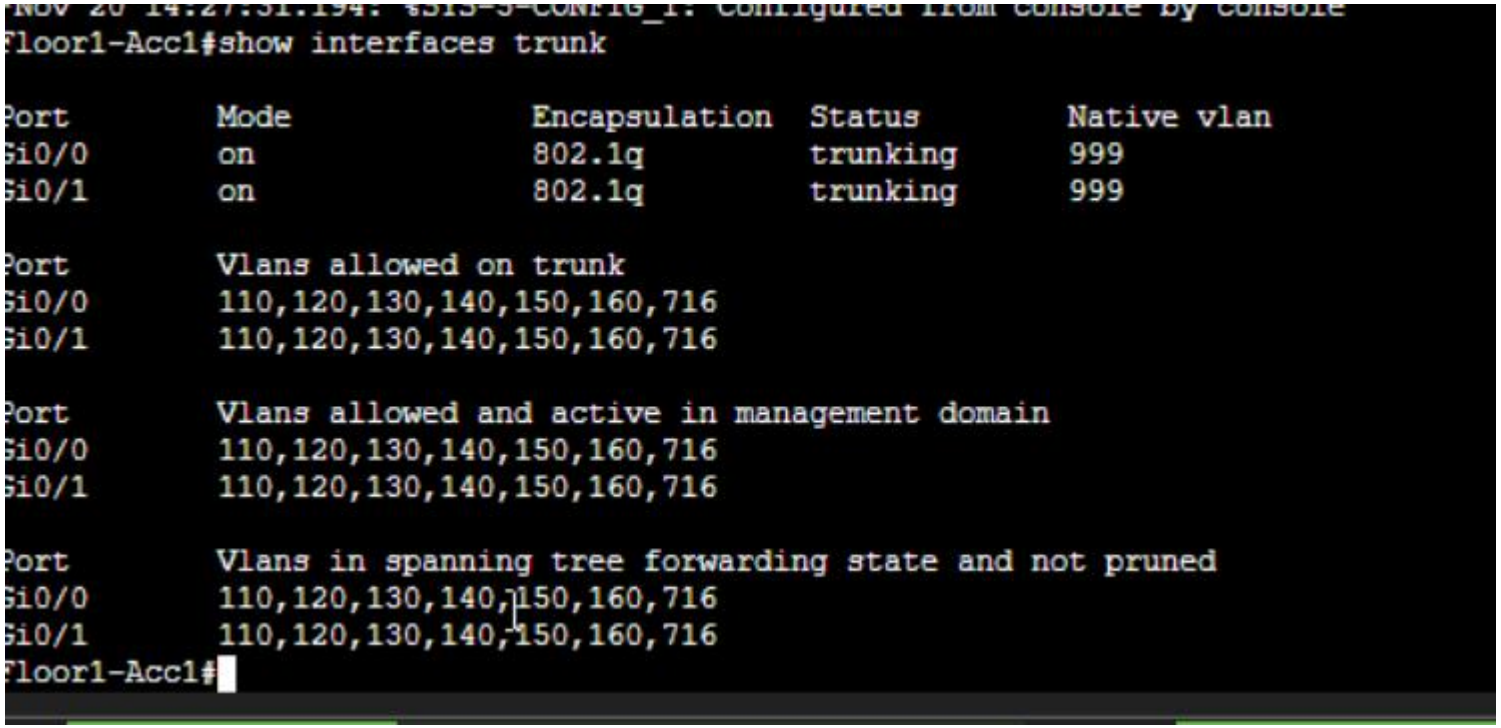


SSH from Client2 > SpringCore 1



Allowed Vlan on Trunk Interfaces of Switches

Floor1-ACC1


Floor1-Acc1#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Gi0/0 on 802.1q trunking 999
Gi0/1 on 802.1q trunking 999
Port Vlans allowed on trunk
Gi0/0 110,120,130,140,150,160,716
Gi0/1 110,120,130,140,150,160,716
Port Vlans allowed and active in management domain
Gi0/0 110,120,130,140,150,160,716
Gi0/1 110,120,130,140,150,160,716
Port Vlans in spanning tree forwarding state and not pruned
Gi0/0 110,120,130,140,150,160,716
Gi0/1 110,120,130,140,150,160,716
Floor1-Acc1#

Floor2-Acc1

```
Floor2-Acc1#show int trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      999
Gi0/1       on               802.1q         trunking      999

Port        Vlans allowed on trunk
Gi0/0       210,220,230,240,250,716
Gi0/1       210,220,230,240,250,716

Port        Vlans allowed and active in management domain
Gi0/0       210,220,230,240,250,716
Gi0/1       210,220,230,240,250,716

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       210,220,230,240,250,716
Gi0/1       210,220,230,240,250,716
Floor2-Acc1#
```

Floor3-Acc1

```
Floor3-Acc1#show int trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      999
Gi0/1       on               802.1q         trunking      999

Port        Vlans allowed on trunk
Gi0/0       310,320,330,340,350,716
Gi0/1       310,320,330,340,350,716

Port        Vlans allowed and active in management domain
Gi0/0       310,320,330,340,350,716
Gi0/1       310,320,330,340,350,716

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       310,320,330,340,350,716
Gi0/1       310,320,330,340,350,716
Floor3-Acc1#
```

DataCentre

```
Datacentre#show int trunk

Port        Mode             Encapsulation  Status        Native vlan
Po1         on               802.1q         trunking      999
Po2         on               802.1q         trunking      999

Port        Vlans allowed on trunk
Po1         716,916,999
Po2         716,916,999

Port        Vlans allowed and active in management domain
Po1         716,916,999
Po2         716,916,999

Port        Vlans in spanning tree forwarding state and not pruned
Po1         716,916,999
Po2         716,916,999
Datacentre#
```

Acl to allow visitors restricting access to sql & tftp servers

Spring Core1

```
Springcore1#show access-list
Standard IP access list SSH_ONLY
    10 permit 172.21.4.0, wildcard bits 0.0.0.255 (2 matches)
    20 deny   any
Extended IP access list CISCO-CWA-URL-REDIRECT-ACL
    100 deny udp any any eq domain
    101 deny tcp any any eq domain
    102 deny udp any eq bootps any
    103 deny udp any any eq bootpc
    104 deny udp any eq bootpc any
    105 permit tcp any any eq www
Extended IP access list VISITOR_DC_PROTECT
    10 permit udp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps
    20 permit udp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps (31 matches)
    30 permit udp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps
    40 permit udp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
    50 permit udp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain (381 matches)
    60 permit udp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
    70 permit tcp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
    80 permit tcp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
    90 permit tcp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
    100 deny ip 172.21.5.0 0.0.0.255 host 172.21.0.30
    110 deny ip 172.21.6.0 0.0.0.255 host 172.21.0.30 (4 matches)
    120 deny ip 172.21.7.0 0.0.0.255 host 172.21.0.30
    130 deny ip 172.21.5.0 0.0.0.255 host 172.21.0.40
    140 deny ip 172.21.6.0 0.0.0.255 host 172.21.0.40 (4 matches)
    150 deny ip 172.21.7.0 0.0.0.255 host 172.21.0.40
    160 permit ip any any (6779 matches)
```

SpringCore2

```
Springcore2#show access-list
Standard IP access list SSH_ONLY
    10 permit 172.21.4.0, wildcard bits 0.0.0.255
    20 deny   any
Extended IP access list CISCO-CWA-URL-REDIRECT-ACL
    100 deny udp any any eq domain
    101 deny tcp any any eq domain
    102 deny udp any eq bootps any
    103 deny udp any any eq bootpc
    104 deny udp any eq bootpc any
    105 permit tcp any any eq www
Extended IP access list VISITOR_DC_PROTECT
    10 permit udp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps
    20 permit udp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps
    30 permit udp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps
    40 permit udp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
    50 permit udp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
    60 permit udp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
    70 permit tcp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
    80 permit tcp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
    90 permit tcp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
    100 deny ip 172.21.5.0 0.0.0.255 host 172.21.0.30
    110 deny ip 172.21.6.0 0.0.0.255 host 172.21.0.30
    120 deny ip 172.21.7.0 0.0.0.255 host 172.21.0.30
    130 deny ip 172.21.5.0 0.0.0.255 host 172.21.0.40
    140 deny ip 172.21.6.0 0.0.0.255 host 172.21.0.40
    150 deny ip 172.21.7.0 0.0.0.255 host 172.21.0.40
    160 permit ip any any (4412 matches)
```

ACL to only allow HTTP/HTTPS from the MN visitor networksto the ISP public internet

SpringCore1

```
Extended IP access list VISITOR_WEB_ONLY
    10 permit tcp 172.21.5.0 0.0.0.255 any eq www
    20 permit tcp 172.21.5.0 0.0.0.255 any eq 443
    30 permit tcp 172.21.6.0 0.0.0.255 any eq www (217890 matches)
    40 permit tcp 172.21.6.0 0.0.0.255 any eq 443 (76424 matches)
    50 permit tcp 172.21.7.0 0.0.0.255 any eq www
    60 permit tcp 172.21.7.0 0.0.0.255 any eq 443
    70 deny ip 172.21.5.0 0.0.0.255 any (351 matches)
    80 deny ip 172.21.6.0 0.0.0.255 any (77387 matches)
    90 deny ip 172.21.7.0 0.0.0.255 any (349 matches)
    100 permit ip any any (553660 matches)
    110 permit udp any any eq domain
    120 permit tcp any any eq domain
```

SpringCore 2