

# Configuring a Remote Access VPN (3e)

Access Control and Identity Management, Third Edition - Lab 06

Student:

Jacob Jeffers

Email:

jjeffers6151@ucumberlands.edu

Time on Task:

3 hours, 21 minutes

Progress:

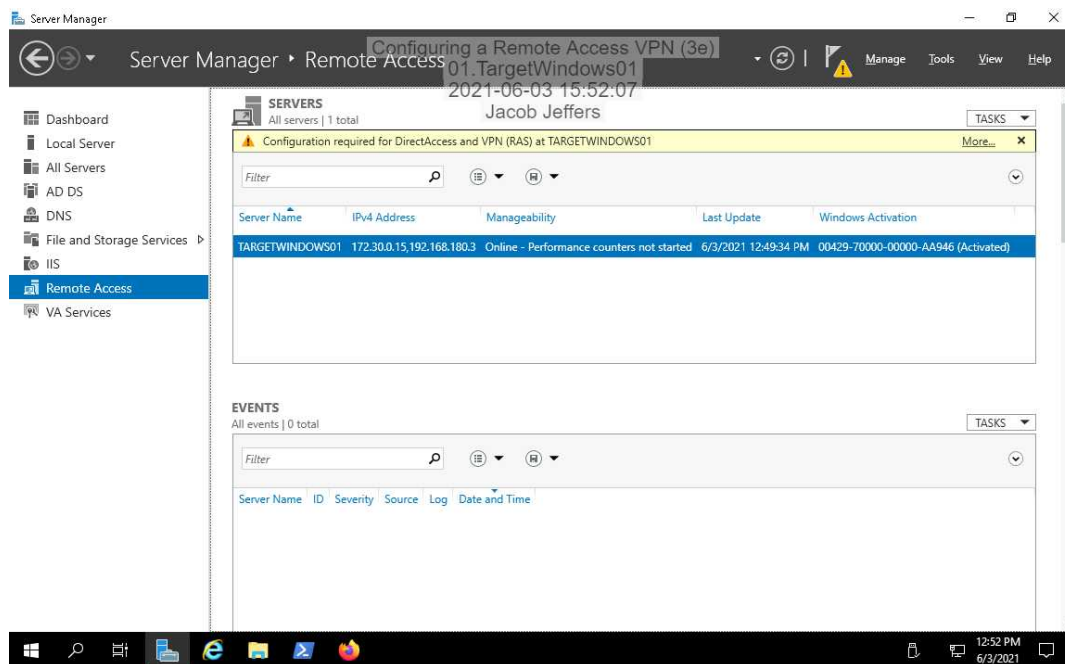
100%

Report Generated: Thursday, June 3, 2021 at 5:13 PM

## Section 1: Hands-On Demonstration

### Part 1: Configure a Windows Server VPN

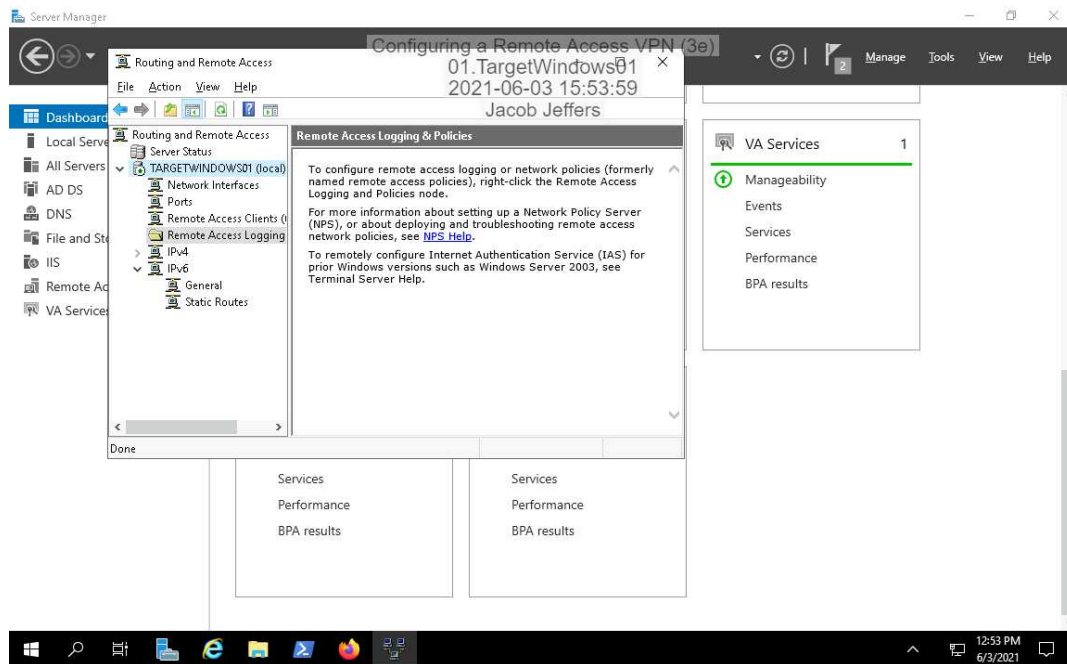
15. **Make a screen capture** showing the **Results** page in the **Add Roles and Features Wizard** confirming successful VPN installation.



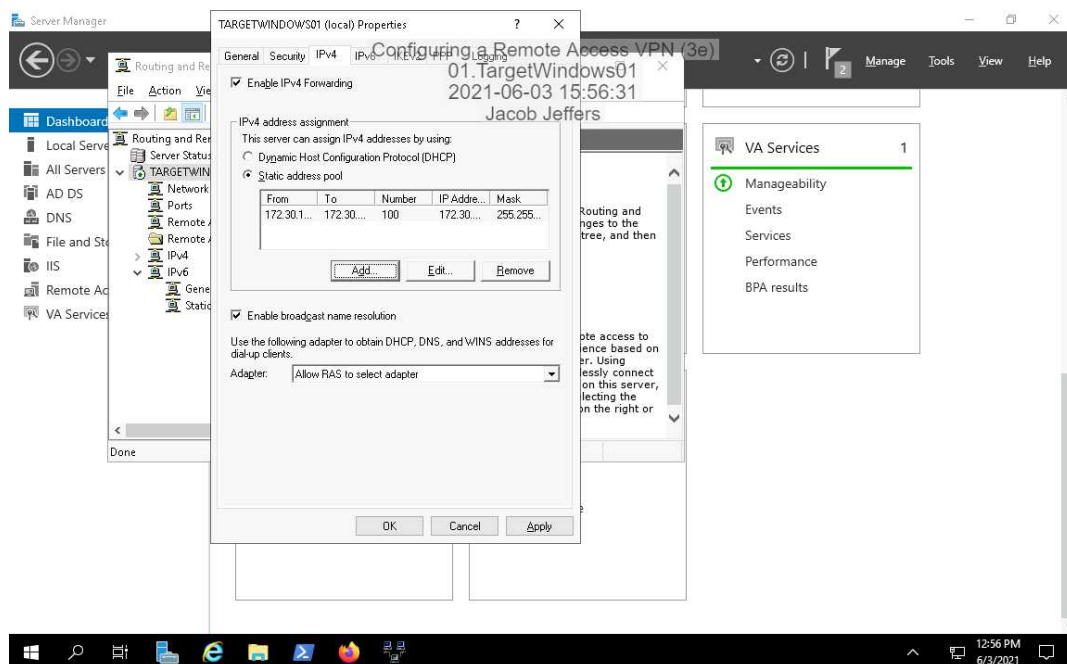
## Configuring a Remote Access VPN (3e)

Access Control and Identity Management, Third Edition - Lab 06

25. Make a screen capture showing the **Routing and Remote Access** console with the active service on **TargetWindows01**.



33. Make a screen capture showing the **TARGETWINDOWS01 Properties** dialog box with the configured static address pool.

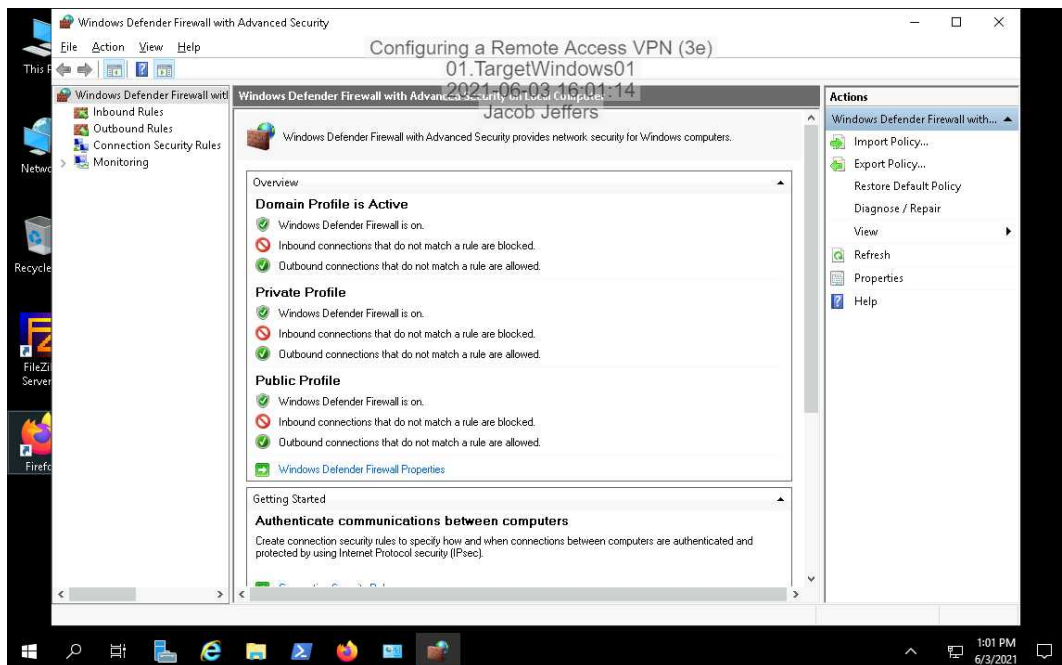


## Part 2: Configure VPN Access Controls

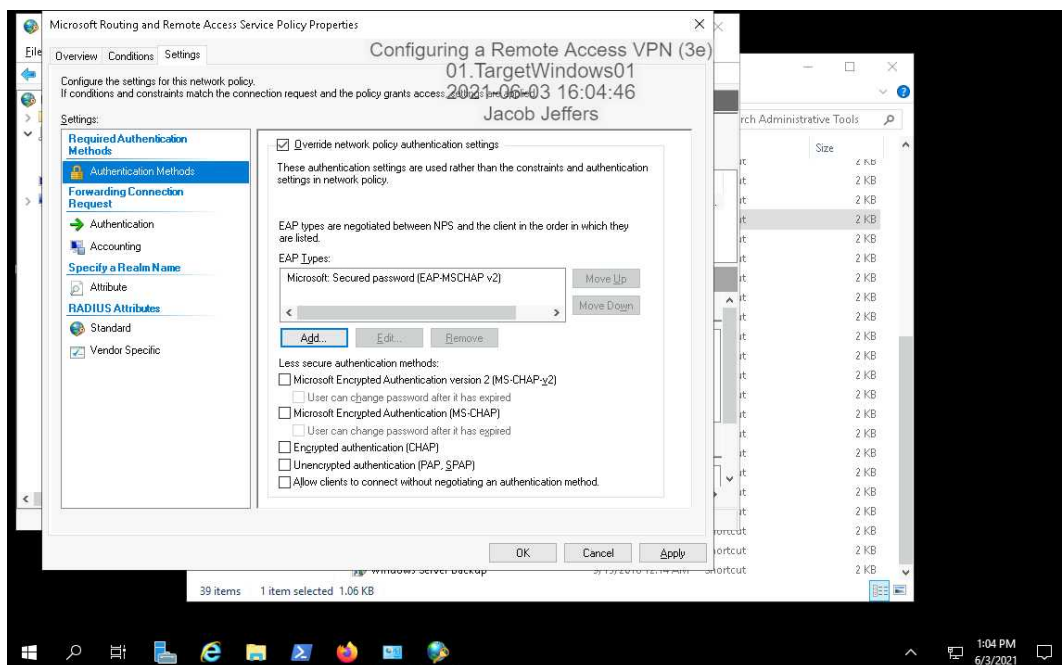
# Configuring a Remote Access VPN (3e)

Access Control and Identity Management, Third Edition - Lab 06

## 8. Make a screen capture showing the activated Windows Defender Firewall.



## 23. Make a screen capture showing the successfully configured Routing and Remote Access Policy properties.

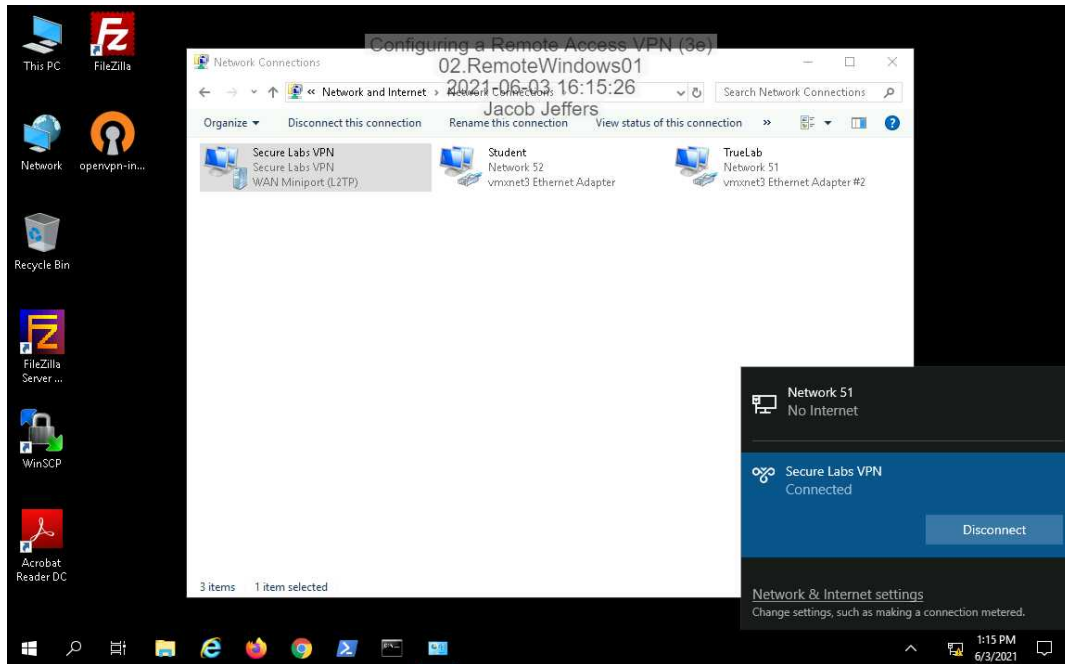


## Part 3: Connect to the VPN

## Configuring a Remote Access VPN (3e)

Access Control and Identity Management, Third Edition - Lab 06

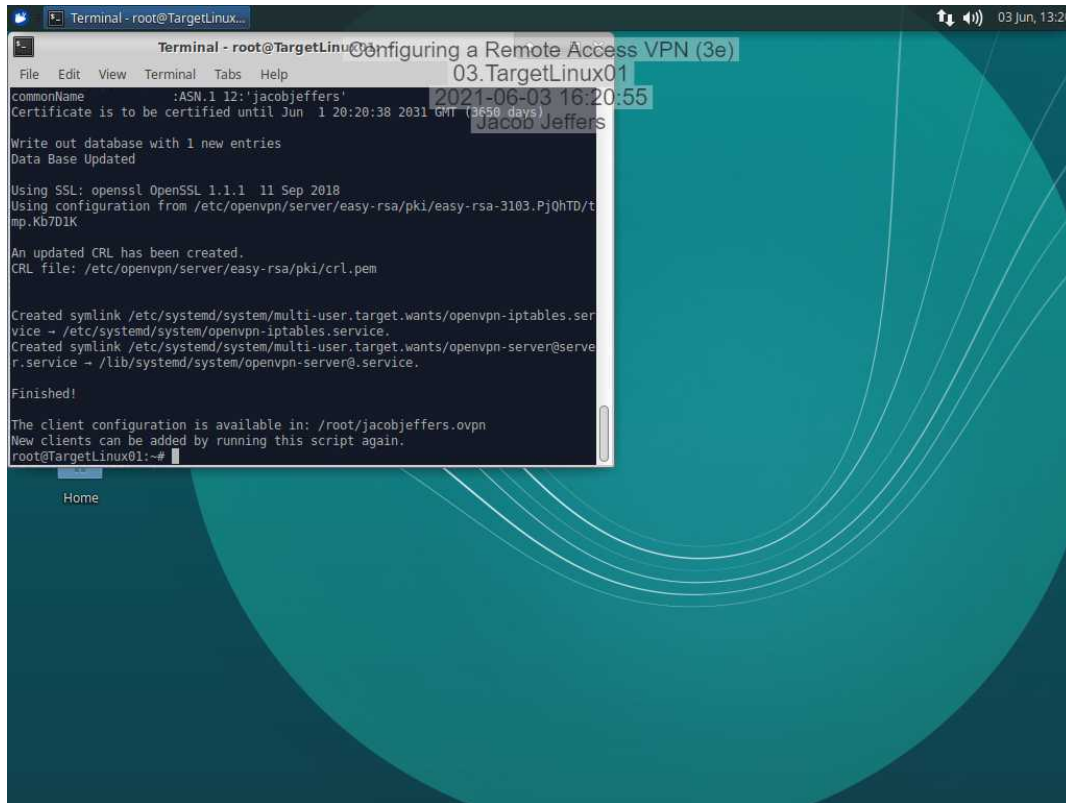
24. Make a screen capture showing the **successful VPN connection status**.



## Section 2: Applied Learning

### Part 1: Configure OpenVPN

13. Make a screen capture showing the **successful OpenVPN server installation**.

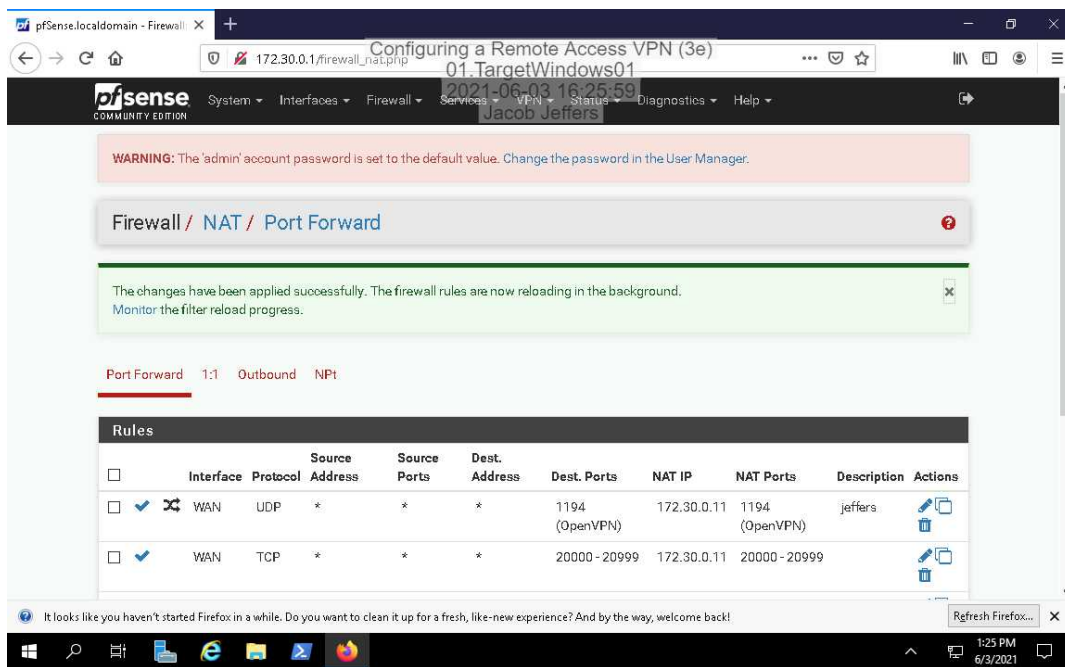


### Part 2: Configure the Network Firewall

# Configuring a Remote Access VPN (3e)

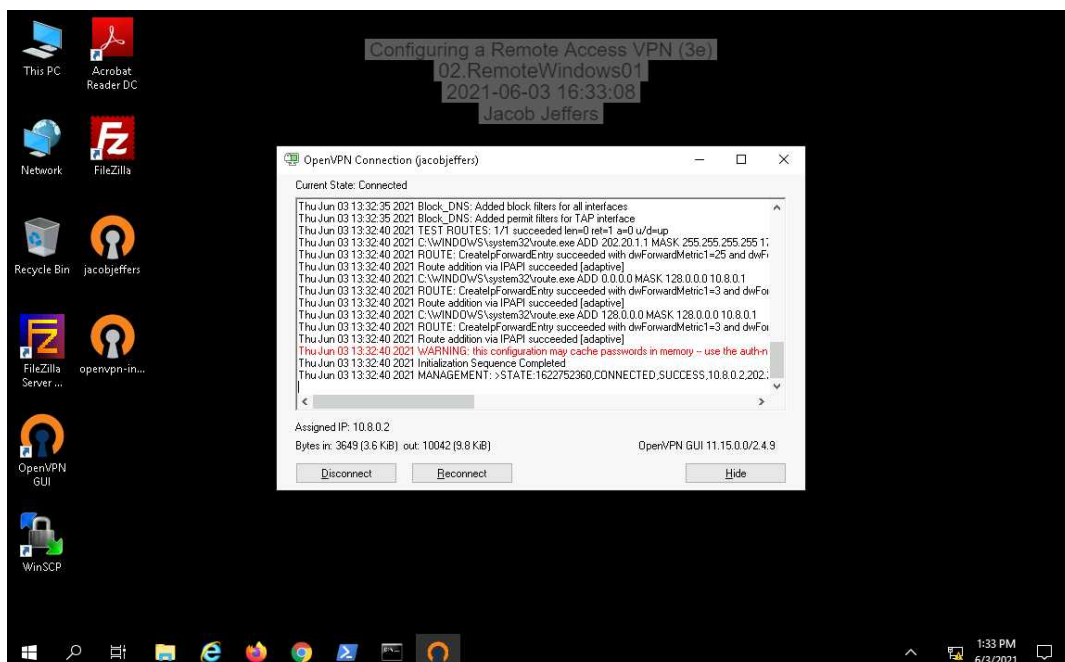
## Access Control and Identity Management, Third Edition - Lab 06

10. Make a screen capture showing the **successfully applied pfSense firewall rule allowing VPN access.**



### Part 3: Connect to the VPN

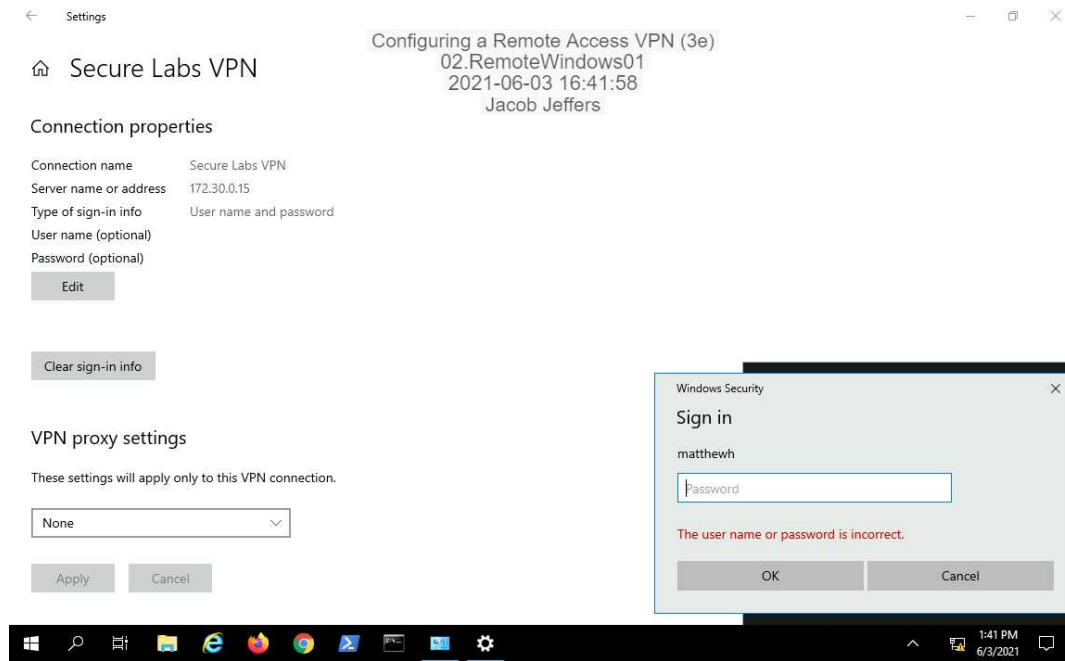
17. Make a screen capture showing the **OpenVPN status window and the successful connection status.**



### Section 3: Challenge and Analysis

#### Part 1: Generate Login Attempts

Make a screen capture showing the **failed logon attempt to the Windows VPN**.



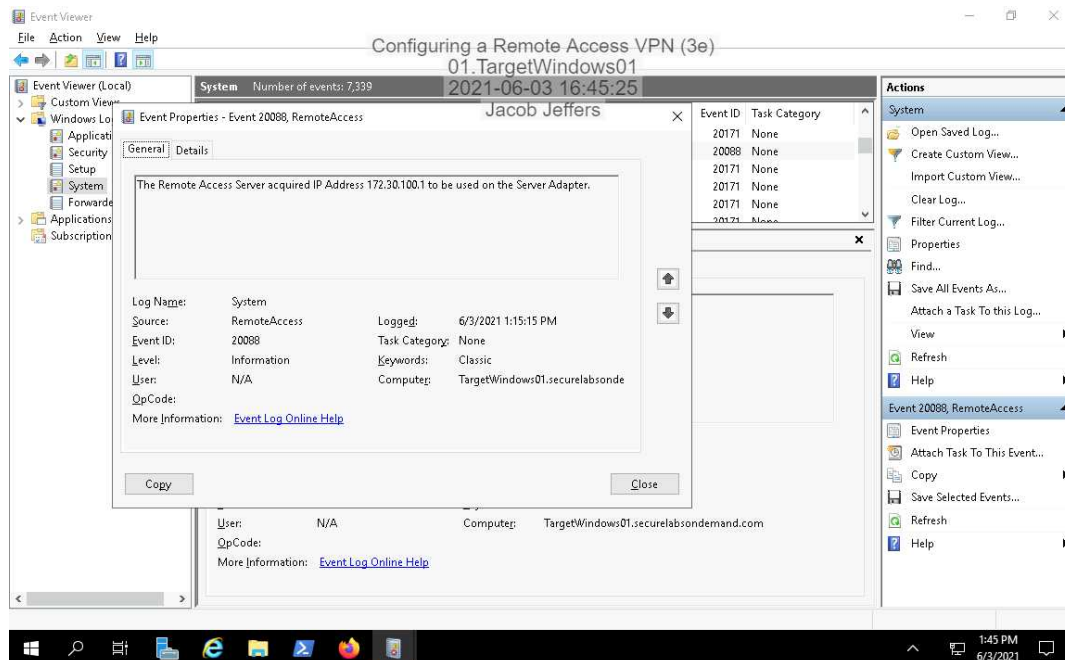
#### Part 2: Review Windows Logs



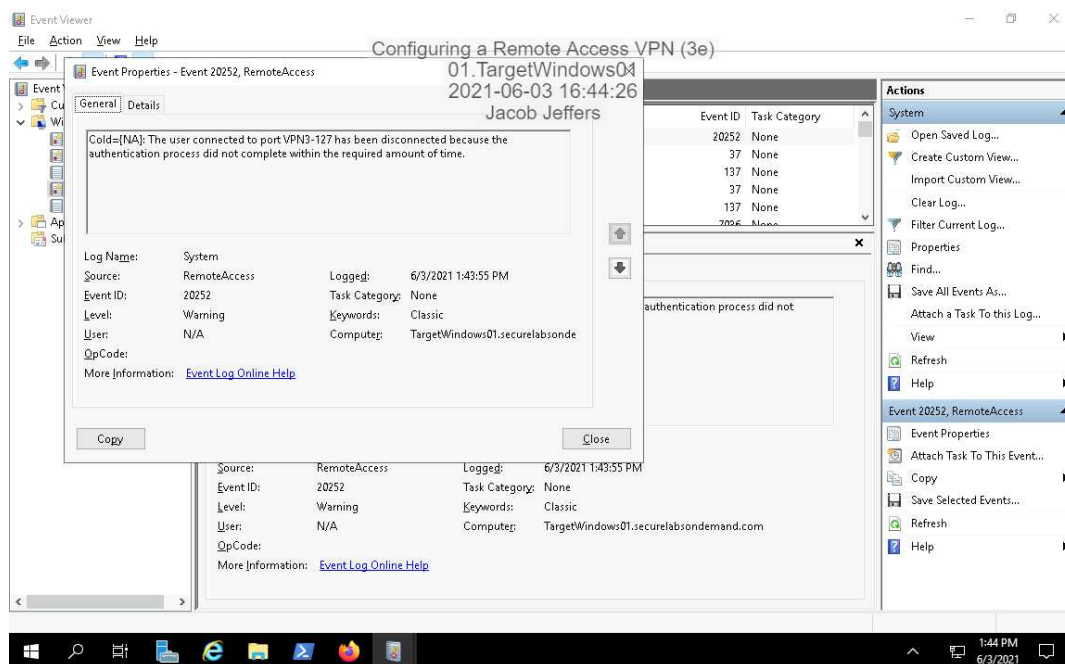
# Configuring a Remote Access VPN (3e)

## Access Control and Identity Management, Third Edition - Lab 06

**Make a screen capture showing the log entry for the successful login attempt.**



**Make a screen capture showing the log entry for the unsuccessful login attempt.**



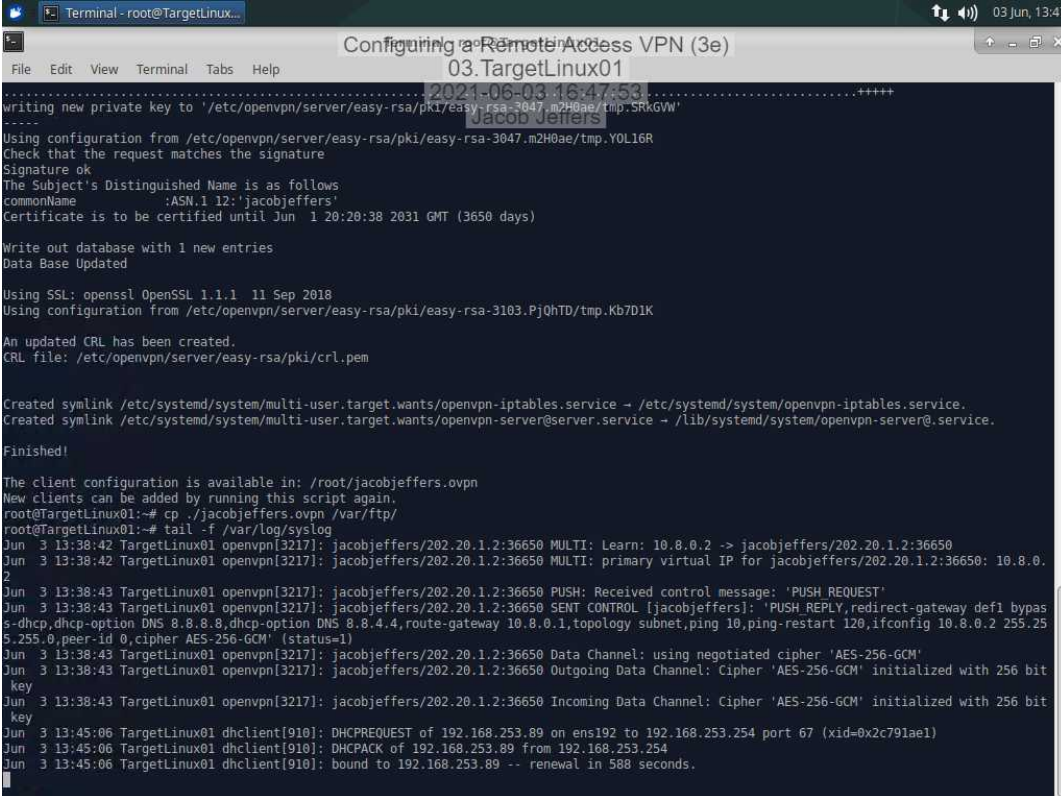
## Part 3: Review Linux Logs



# Configuring a Remote Access VPN (3e)

## Access Control and Identity Management, Third Edition - Lab 06

Make a screen capture showing the **command** that you used to retrieve the log entry and the **resulting log entry**.

A terminal window titled 'Terminal - root@TargetLinux...' with a window title bar that says 'Configuring a Remote Access VPN (3e) 03.TargetLinux01'. The terminal shows the output of a script for configuring an OpenVPN server. It includes steps for generating keys, creating certificates for 'jacobjeffers', setting up the database, and creating symlinks for systemd services. The script finishes by showing the client configuration file location. Following this, the user runs 'tail -f /var/log/syslog' to view log entries. The logs show a client connecting, receiving a 'PUSH REQUEST' control message, and establishing data channels using AES-256-GCM encryption. The final log entry shows a DHCP request and response for the client's IP address.

```
.....+++++
writing new private key to '/etc/openvpn/server/easy-rsa/pki/easy-rsa-3047.m2H0ae/tmp.SRkGW'
-----
Using configuration from /etc/openvpn/server/easy-rsa/pki/easy-rsa-3047.m2H0ae/tmp.YOL16R
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'jacobjeffers'
Certificate is to be certified until Jun  1 20:20:38 2031 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

Using SSL: openssl OpenSSL 1.1.1 11 Sep 2018
Using configuration from /etc/openvpn/server/easy-rsa/pki/easy-rsa-3103.Pj0hTD/tmp.Kb7D1K

An updated CRL has been created.
CRL file: /etc/openvpn/server/easy-rsa/pki/crl.pem

Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-iptables.service -> /etc/systemd/system/openvpn-iptables.service.
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-server@server.service -> /lib/systemd/system/openvpn-server@.service.

Finished!

The client configuration is available in: /root/jacobjeffers.ovpn
New clients can be added by running this script again.
root@TargetLinux01:~# cp ./jacobjeffers.ovpn /var/ftp/
root@TargetLinux01:~# tail -f /var/log/syslog
Jun  3 13:38:42 TargetLinux01 openvpn[3217]: jacobjeffers/202.20.1.2:36650 MULTI: Learn: 10.8.0.2 -> jacobjeffers/202.20.1.2:36650
Jun  3 13:38:42 TargetLinux01 openvpn[3217]: jacobjeffers/202.20.1.2:36650 MULTI: primary virtual IP for jacobjeffers/202.20.1.2:36650: 10.8.0.2
Jun  3 13:38:43 TargetLinux01 openvpn[3217]: jacobjeffers/202.20.1.2:36650 PUSH: Received control message: 'PUSH REQUEST'
Jun  3 13:38:43 TargetLinux01 openvpn[3217]: jacobjeffers/202.20.1.2:36650 SENT CONTROL [jacobjeffers]: 'PUSH REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 8.8.8.8,dhcp-option DNS 8.8.4.4,route-gateway 10.8.0.1,topology subnet,ping 10,ping-restart 120,ifconfig 10.8.0.2 255.255.0,peer-id 0,cipher AES-256-GCM' (status=1)
Jun  3 13:38:43 TargetLinux01 openvpn[3217]: jacobjeffers/202.20.1.2:36650 Data Channel: using negotiated cipher 'AES-256-GCM'
Jun  3 13:38:43 TargetLinux01 openvpn[3217]: jacobjeffers/202.20.1.2:36650 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Jun  3 13:38:43 TargetLinux01 openvpn[3217]: jacobjeffers/202.20.1.2:36650 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Jun  3 13:45:06 TargetLinux01 dhclient[910]: DHCPREQUEST of 192.168.253.89 on ens192 to 192.168.253.254 port 67 (xid=0x2c791ae1)
Jun  3 13:45:06 TargetLinux01 dhclient[910]: DHCPACK of 192.168.253.89 from 192.168.253.254
Jun  3 13:45:06 TargetLinux01 dhclient[910]: bound to 192.168.253.89 -- renewal in 588 seconds.
```