**IT6016 Network Security Practical Tasks**

**Network Plan**

**Nicholas Rowley**

**09/04/2019**

Table of Contents

[**IPv4 Addressing Scheme** 1](#_Toc5650110)

[**Device Network Configuration** 1](#_Toc5650111)

[**Network Topology Diagram** 2](#_Toc5650112)

[Device Authentication and other Details 3](#_Toc5650113)

[Routers, Switches and ASA (General login / ASDM details) (LOCAL only) 3](#_Toc5650114)

[ACS 3](#_Toc5650115)

[PCS 3](#_Toc5650116)

[AAA Logins (TACACS Server on ACSBuzzNick) (For CLI Access and ASDM Access) 3](#_Toc5650117)

[Clientless SSL VPN 3](#_Toc5650118)

[SNMP 3](#_Toc5650119)

[NTP 3](#_Toc5650120)

[Access Lists (R3) 4](#_Toc5650121)

[Access Lists (Switches) 4](#_Toc5650122)

[OSPF Authentication 4](#_Toc5650123)

[ASA Password Encryption 4](#_Toc5650124)

[ASA Access Lists 4](#_Toc5650125)

[ASA Interface Names 4](#_Toc5650126)

[Site to Site VPN Encryption 4](#_Toc5650127)

[Screenshots 5](#_Toc5650128)

[Test 1 - PC’s in subnets can ping servers in other subnets 5](#_Toc5650129)

[PC1 5](#_Toc5650130)

[PC3 6](#_Toc5650131)

[Test 2 - Ping’s from router 2 (r2) and router 1 (r1) cannot reach devices in subnets 7](#_Toc5650132)

[R1 7](#_Toc5650133)

[R2 8](#_Toc5650134)

[Test 3 - Pings from PC1 cannot reach PC2 (in the DMZ zone) 9](#_Toc5650135)

[Test 4 - Syslog and SNMP data from Cisco devices is being recorded on the Syslog/SNMP server 10](#_Toc5650136)

[Syslog 10](#_Toc5650137)

[SNMP 11](#_Toc5650138)

[Test 5 - Connections to manage routers using requires SSH and telnet does not work 12](#_Toc5650139)

[Test 6 - Logging onto a switch and router r3 successfully uses accounts from the ACS TACACS+ server - Buzzadmin1 account 12](#_Toc5650140)

[Router AAA 12](#_Toc5650141)

[Switch AAA 13](#_Toc5650142)

[Test 7 - PC2 in the DMZ zone cannot access the Windows 10 PC 13](#_Toc5650143)

[Test 8 - Traffic from site 1 to site 2 successfully travels across the VPN tunnel and there are VPN sessions 14](#_Toc5650144)

[Test 9 - Windows 10 PC can successfully connect in a secure browser session to the web portal on the ASA using the BuzzVPNuser account 15](#_Toc5650145)

[Test 10 - Router r2 can make a SSH connection to manage the ASA 16](#_Toc5650146)

[GNS3 window with network topology 17](#_Toc5650147)

[ASDM running with a connection to the ASA 18](#_Toc5650148)

[Using the ACS 19](#_Toc5650149)

[Network Devices and AAA Clients page (under Network Resources) 19](#_Toc5650150)

[Users page (under Users and Identity Stores, Internal Identity Stores) 20](#_Toc5650151)

[Authorization page (under Access Polices, Access Services, Default Device Admin) 21](#_Toc5650152)

# **IPv4 Addressing Scheme**

|  |  |
| --- | --- |
| Subnet Name | Network ID with CIDR |
| R1 to R2 | 130.10.1.200 /30 |
| R2 to R3 | 130.10.1.204 /30 |
| Site 1 Outside (VLAN 2) | 204.150.175.0 /29 |
| Site 1 Inside (VLAN 3) | 192.168.1.64 /27 |
| Site 1 Management VLAN (S1BuzzNick) | 192.168.1.0 /27 |
| Site 1 Management VLAN (S2BuzzNick) | 192.168.1.32 /27 |
| Site 1 VLAN 4 | 192.168.1.96 /27 |
| Site 1 VLAN 5 | 192.168.1.128 /27 |
| Site 2 Management VLAN (S3BuzzNick) | 192.168.2.0 /27 |
| Site 2 VLAN 2 | 192.168.2.32 /27 |

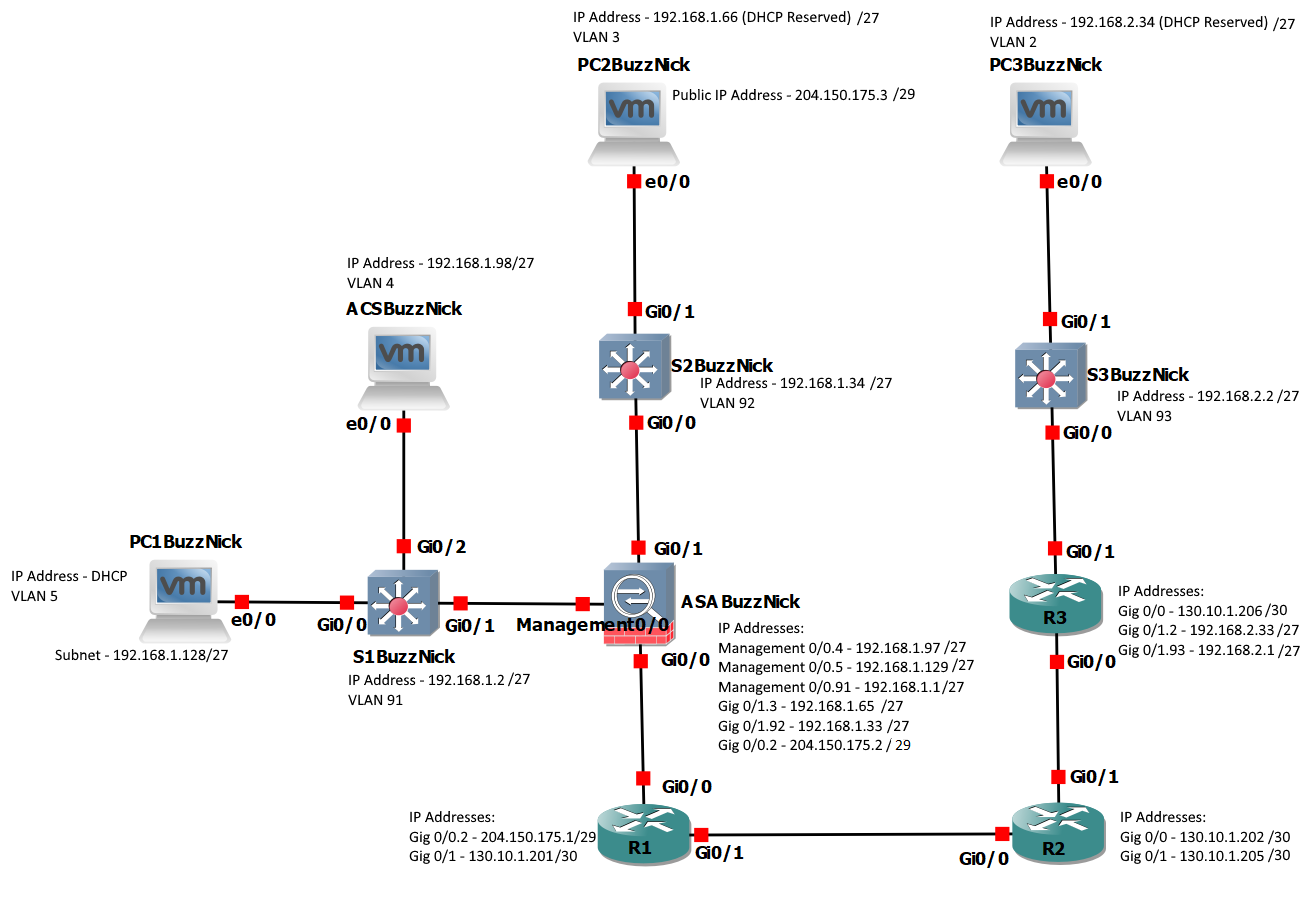
Site to Site VPN uses Interfaces: ASA IP – 204.150.175.2 & R3 IP – 130.10.1.206

Site to Site VPN uses local IP subnet addresses from Site 1 and Site 2.

# **Device Network Configuration**

|  |  |  |  |
| --- | --- | --- | --- |
| Device Name | Interface | VLAN | IPv4 Addresses |
| R1 | Gig 0/1  Gig 0/0.2  Loopback 0 | N/A  2 | 130.10.1.201  204.150.175.1  192.168.0.10 |
| R2 | Gig 0/0  Gig 0/1  Loopback 0 | N/A  N/A | 130.10.1.202  130.10.1.205  192.168.0.20 |
| R3 | Gig 0/0.2  Gig 0/0.93  Gig 0/1  Loopback 0 | 2  93  N/A | 192.168.2.33  192.168.2.1  130.10.1.206  192.168.0.30 |
| ASABuzzNick | Gig 0/0.2  Management 0/0.91  Gig 0/1.3  Gig 0/1.92  Management 0/0.4  Management 0/0.5 | 2  91  3  92  4  5 | 204.150.175.2  192.168.1.1  192.168.1.65  192.168.1.33  192.168.1.97  192.168.1.129 |
| S1BuzzNick | VLAN 91 | 91 | 192.168.1.2 |
| S2BuzzNick | VLAN 92 | 92 | 192.168.1.34 |
| S3BuzzNick | VLAN 93 | 93 | 192.168.2.2 |
| ACSBuzzNick | E0/0 | 4 | 192.168.1.98 |
| PC1BuzzNick | E0/0 | 5 | DHCP |
| PC2BuzzNick | E0/0 | 3 | DHCP (Preferred – 192.168.1.66)  (Public IP – 204.150.175.3) |
| PC3BuzzNick | E0/0 | 2 | DHCP (Preferred – 192.168.2.34) |

**Network Topology Diagram**



# Device Authentication and other Details

## Routers, Switches and ASA (General login / ASDM details) (LOCAL only)

Enable Password: BuzzAccess6016!

Local Login: admin

Local Password: BuzzCisco123

## ACS

Local Login (CLI): admin

Password (CLI): BuzzAccess6016!

Web GUI Login: acsadmin

Web GUI Password: Password2

## PCS

Password: Passw0rd!

## AAA Logins (TACACS Server on ACSBuzzNick) (For CLI Access and ASDM Access)

|  |  |  |  |
| --- | --- | --- | --- |
| Login | Password | Enable Password | Group |
| BuzzAdmin1 | BuzzCisco123 | BuzzAccess6016! | Admin |
| BuzzAdmin2 | BuzzCisco123 | BuzzAccess6016! | Admin |

AAA List name (Routers and Switches) – AAALIST

TACACS Server Name (Routers / Switches / ASA) – BuzzTACACS

TACACS key (ACS[ALL DEVICES]) – BuzzTACACS6016

## Clientless SSL VPN

Profile Name: BuzzSSLVPN

Policy Name: Buzz-SSL-VPN-POLICY

Bookmark: Web-Server (<https://192.168.1.66>)

Username: BuzzVPNuser

Password: BuzzSys123

## SNMP

Version: 3

Username: SNMP-Admin

Password: BuzzSNMP6016!

Privacy Password: BuzzSNMPEncrypt6016!

SNMP group: SNMP-Buzz-Group

Host: 192.168.2.34

View Name: SNMP-RO

## NTP

Trusted-Key: 6016

Password: BuzzNTP

## Access Lists (R3)

ALLOWVTYACCESS – Access list for input traffic on vty lines.

VPN-TRAFFIC – Traffic that is allowed from SITE 2 across the site to site VPN

ALLOW-OUTSIDE-VPN-TRAFFIC – Traffic sent from outside of site 2 that is allowed into the LAN

SNMP-ACCESS – Subnets that are allowed to view SNMP for this device

## Access Lists (Switches)

ALLOWVTYACCESS – Access list for input traffic on vty lines.

SNMP-ACCESS – Subnets that are allowed to view SNMP for this device.

## OSPF Authentication

Key – 1

Password – BuzzRouting6016

## ASA Password Encryption

Encryption Password – BuzzEncrypt6016

## ASA Access Lists

OUTSIDE-IN-TRAFFIC – Traffic from the outside interface that is allowed on the LAN.

## ASA Interface Names

|  |  |  |  |
| --- | --- | --- | --- |
| ASA Interface Type & Number | ASA Interface Name | ASA Security Level | Subnet |
| Management 0/0.4 | INSIDE-VLAN-4 | 100 | 192.168.1.96/27 |
| Management 0/0.5 | INSIDE-VLAN-5 | 100 | 192.168.1.128/27 |
| Management 0/0.91 | Inside-Management-1 | 100 | 192.168.1.0/27 |
| Gig 0/0.2 | OUTSIDE | 0 | 204.150.175.0 /29 |
| Gig 0/1.3 | DMZ | 70 | 192.168.1.64/27 |
| Gig 0/1.92 | DMZ-Management-2 | 100 | 192.168.1.32/27 |

* Allow interfaces with the same security levels to send traffic freely between each other.

## Site to Site VPN Encryption

* Transform set: esp-aes esp-sha-hmac
* Hash: sha
* Group: 2
* Lifetime (seconds): 86400
* Integrity: sha
* Authentication: Pre-share
* Encryption: aes 256
* Isakmp key: BuzzVPNKEY6016
* Interfaces: 204.150.175.2 (ASA) to 130.10.1.206 (R3)

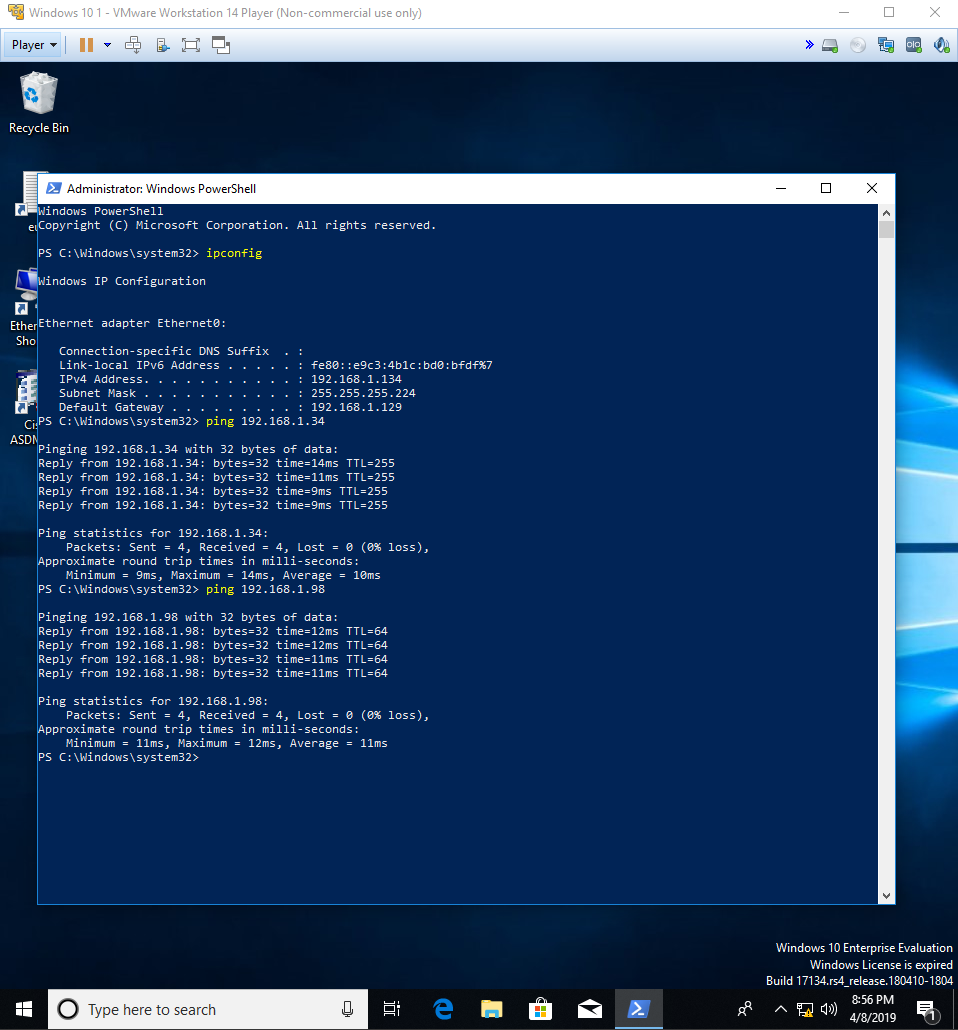
# Network Device Running Configurations

Stored in the ‘IT6016\_91030261\_Running\_Configs’ folder.

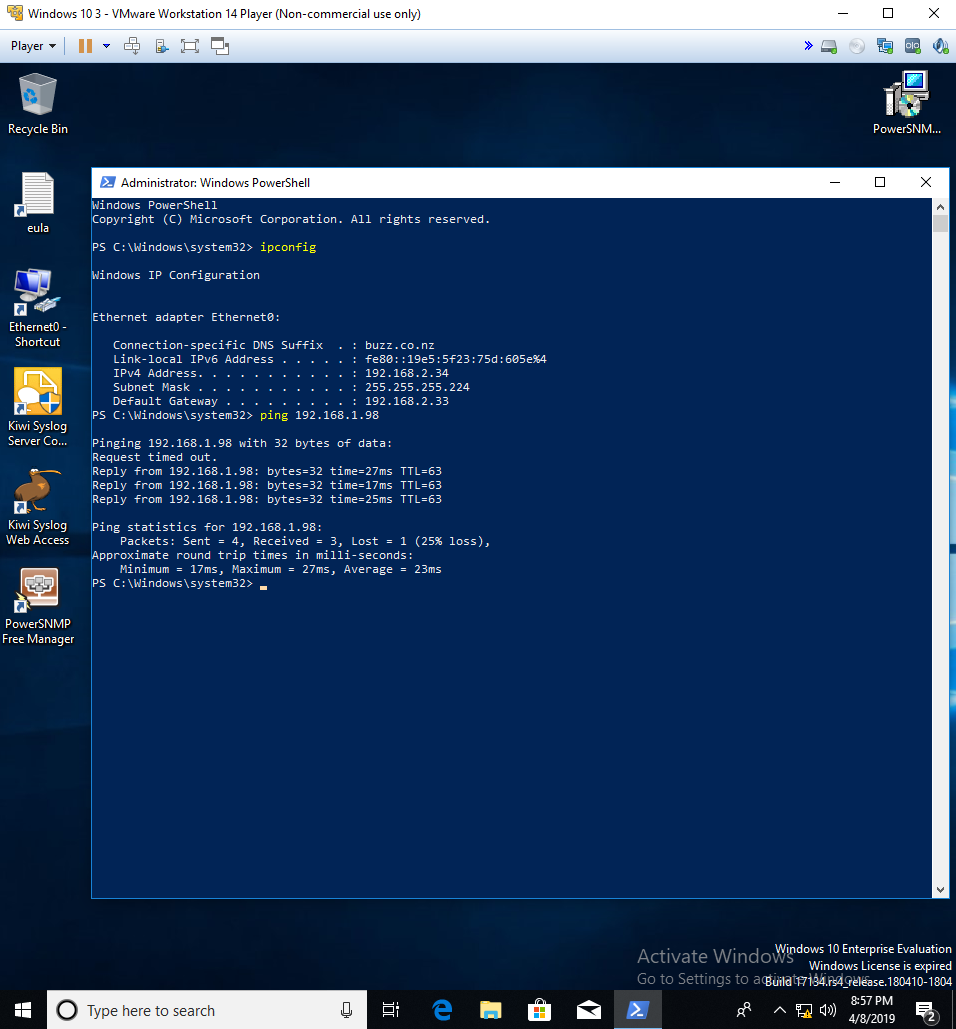
# Screenshots

## Test 1 - PC’s in subnets can ping servers in other subnets

### PC1

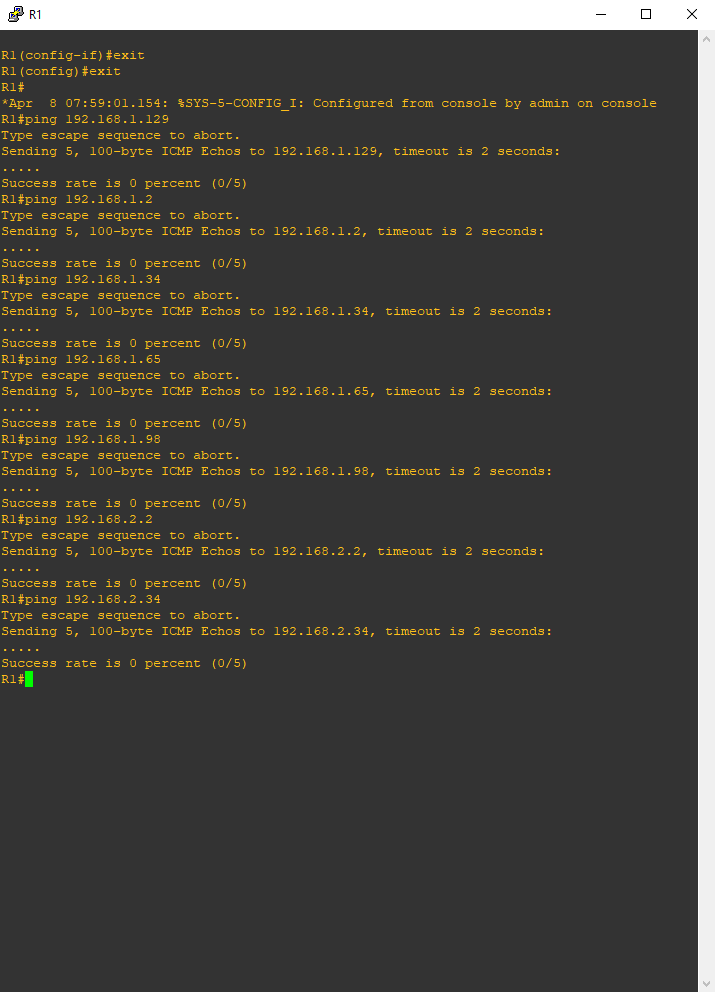


### PC3

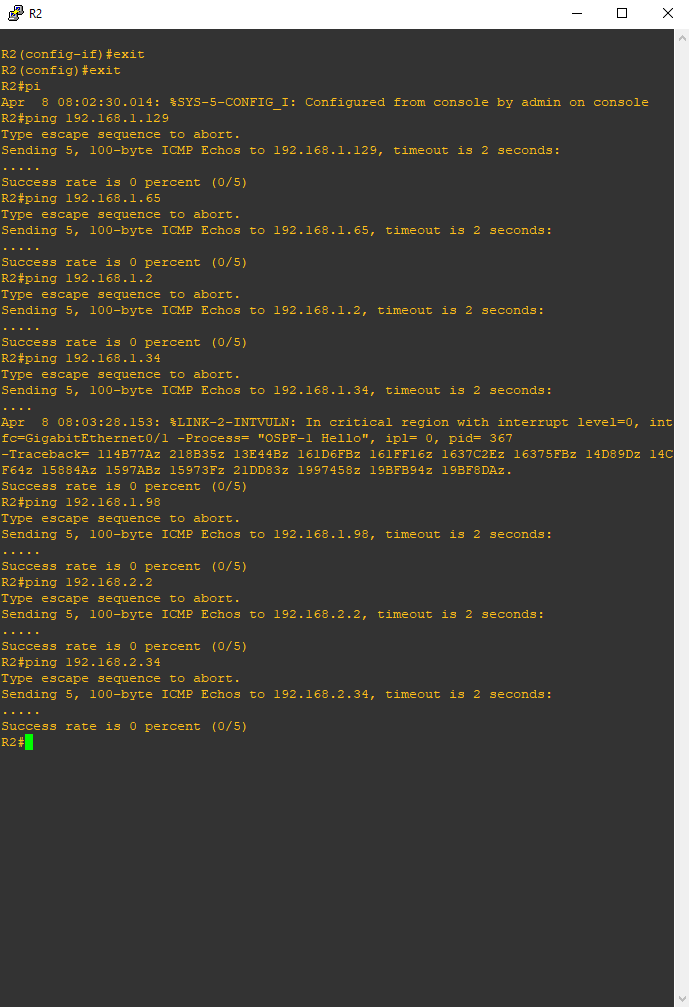


## Test 2 - Ping’s from router 2 (r2) and router 1 (r1) cannot reach devices in subnets

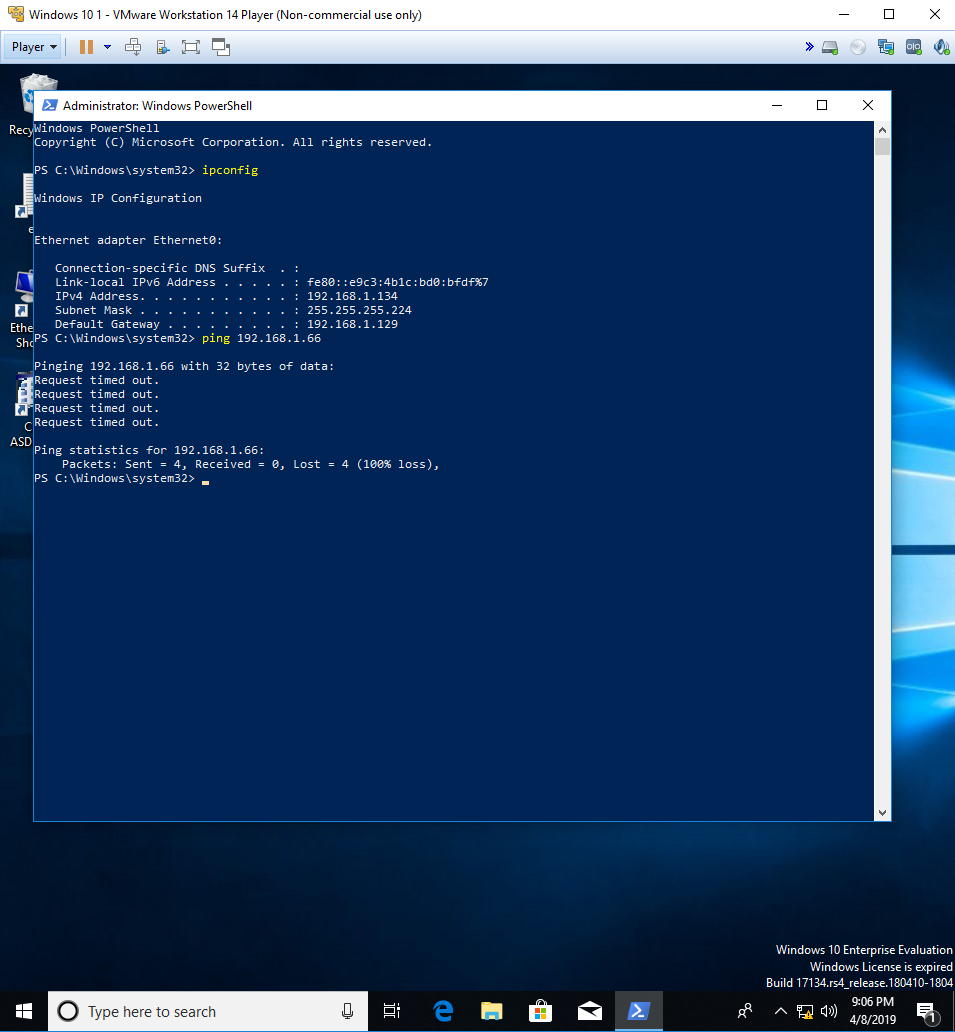
### R1



### R2

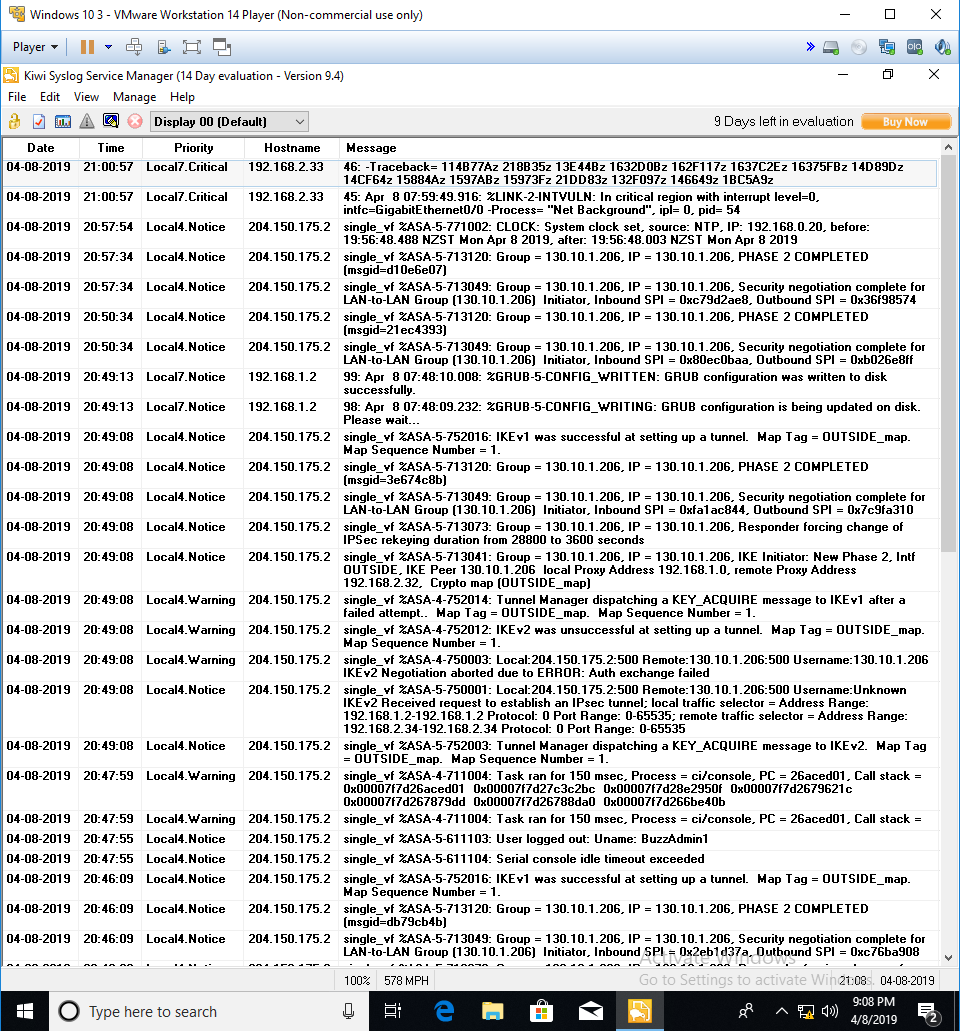


## Test 3 - Pings from PC1 cannot reach PC2 (in the DMZ zone)

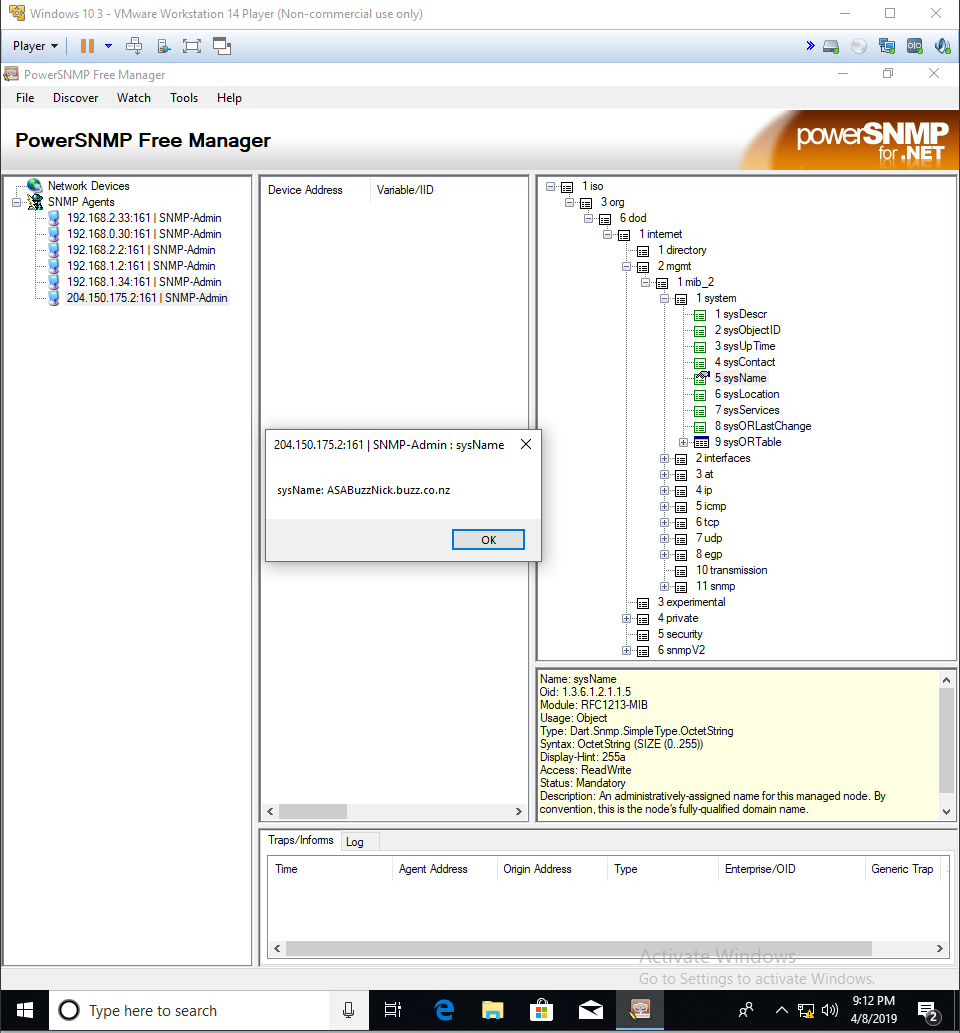


## Test 4 - Syslog and SNMP data from Cisco devices is being recorded on the Syslog/SNMP server

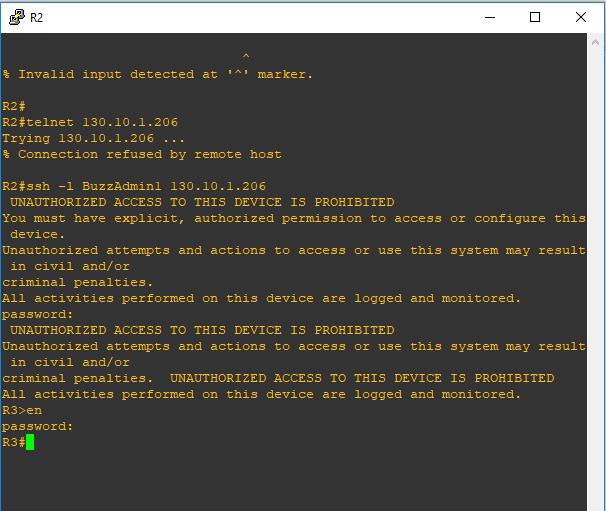
### Syslog



### SNMP

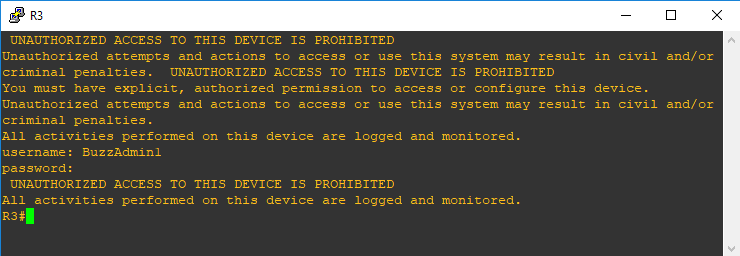


## Test 5 - Connections to manage routers using requires SSH and telnet does not work

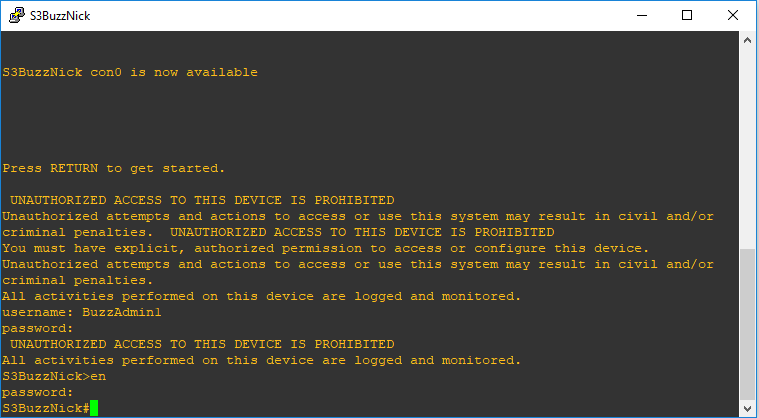


## Test 6 - Logging onto a switch and router r3 successfully uses accounts from the ACS TACACS+ server - Buzzadmin1 account

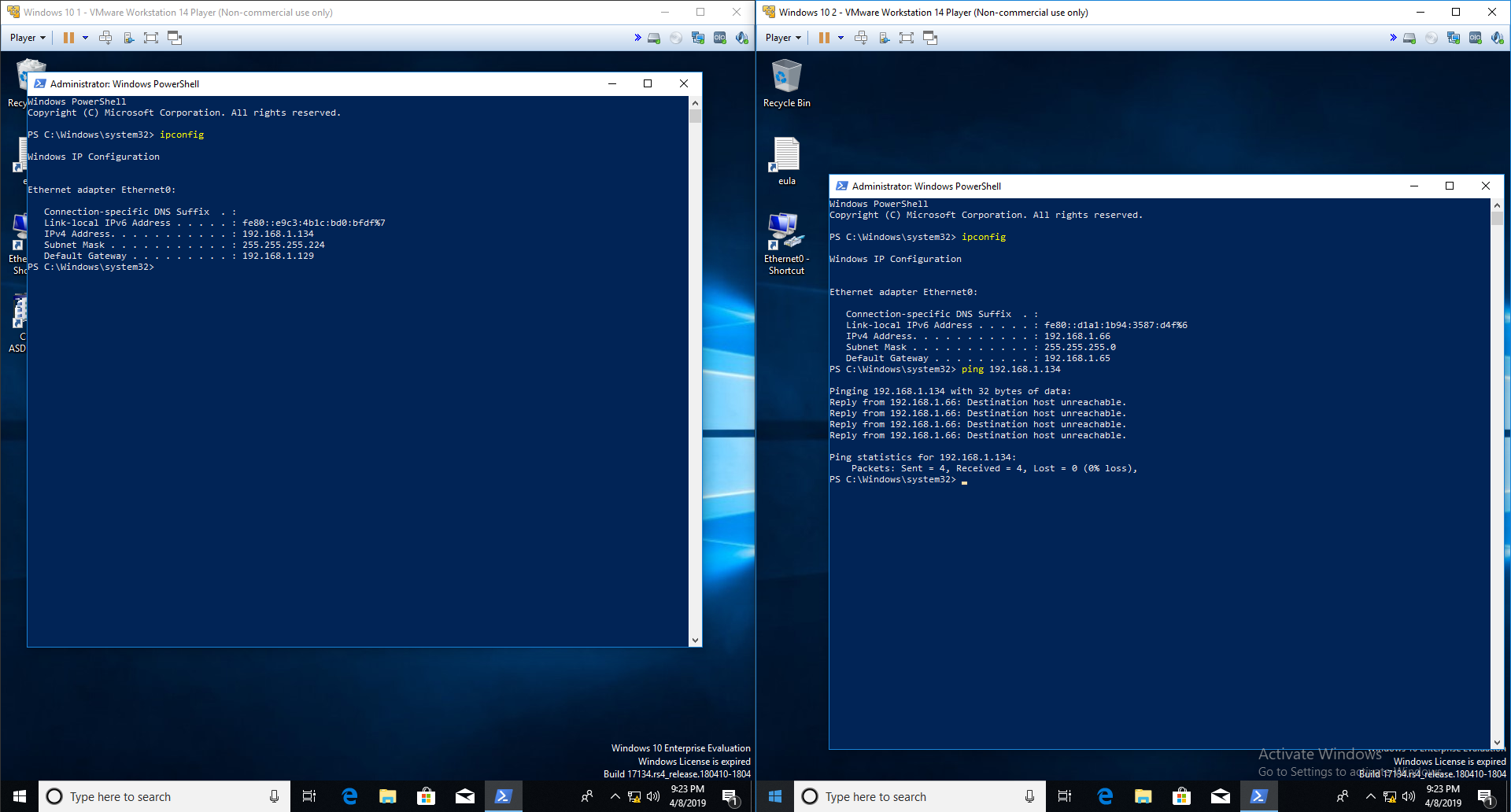
### Router AAA



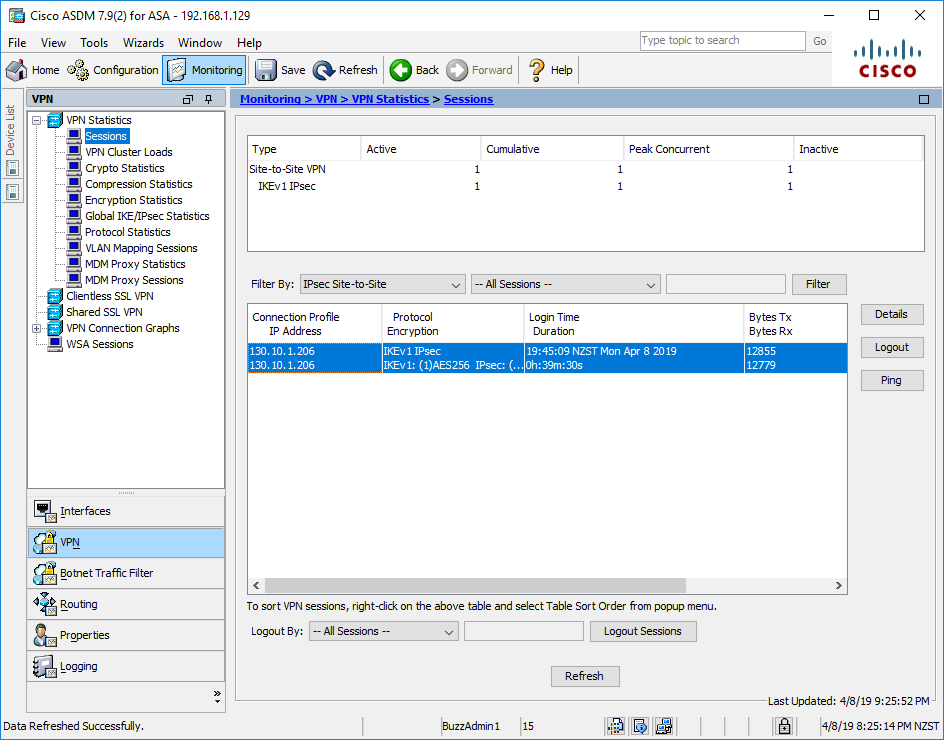
### Switch AAA



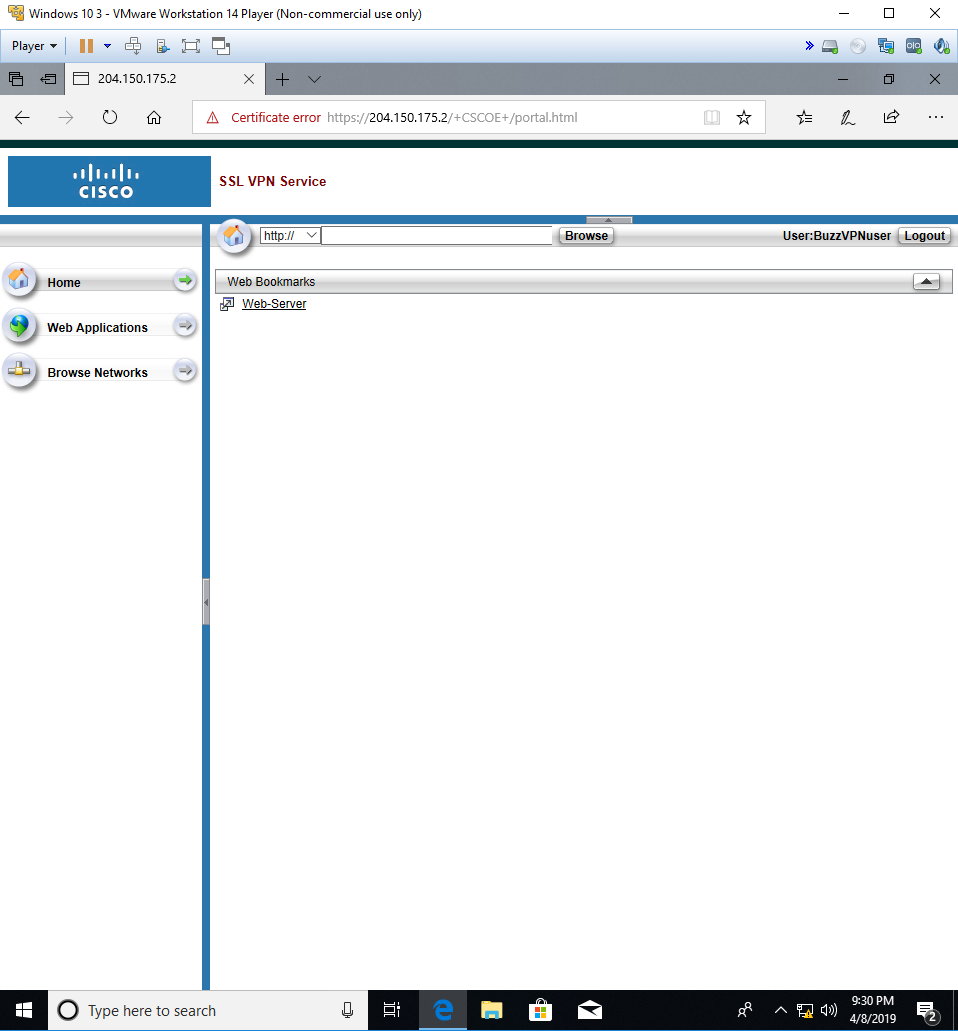
## Test 7 - PC2 in the DMZ zone cannot access the Windows 10 PC



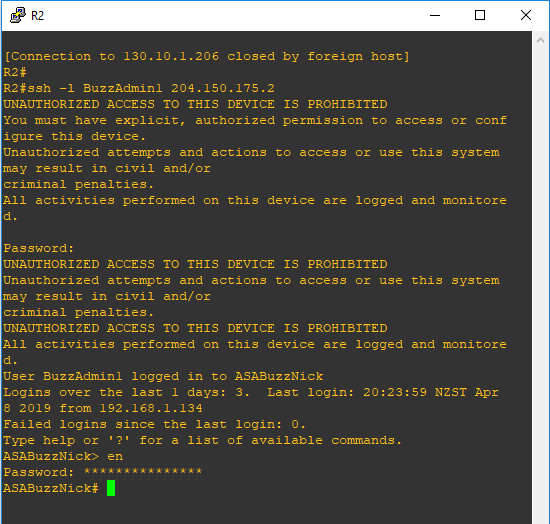
## Test 8 - Traffic from site 1 to site 2 successfully travels across the VPN tunnel and there are VPN sessions



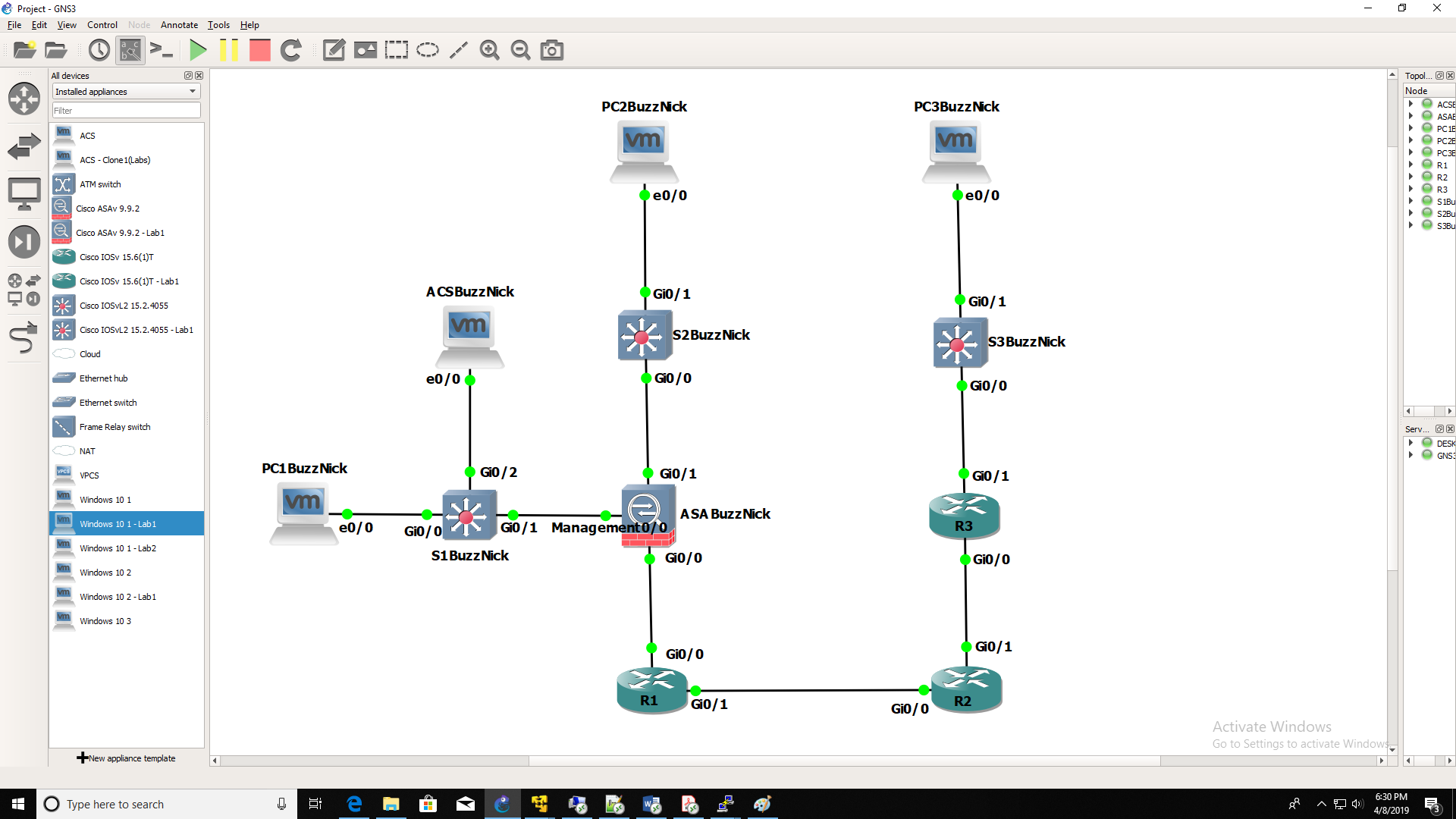
## Test 9 - Windows 10 PC can successfully connect in a secure browser session to the web portal on the ASA using the BuzzVPNuser account



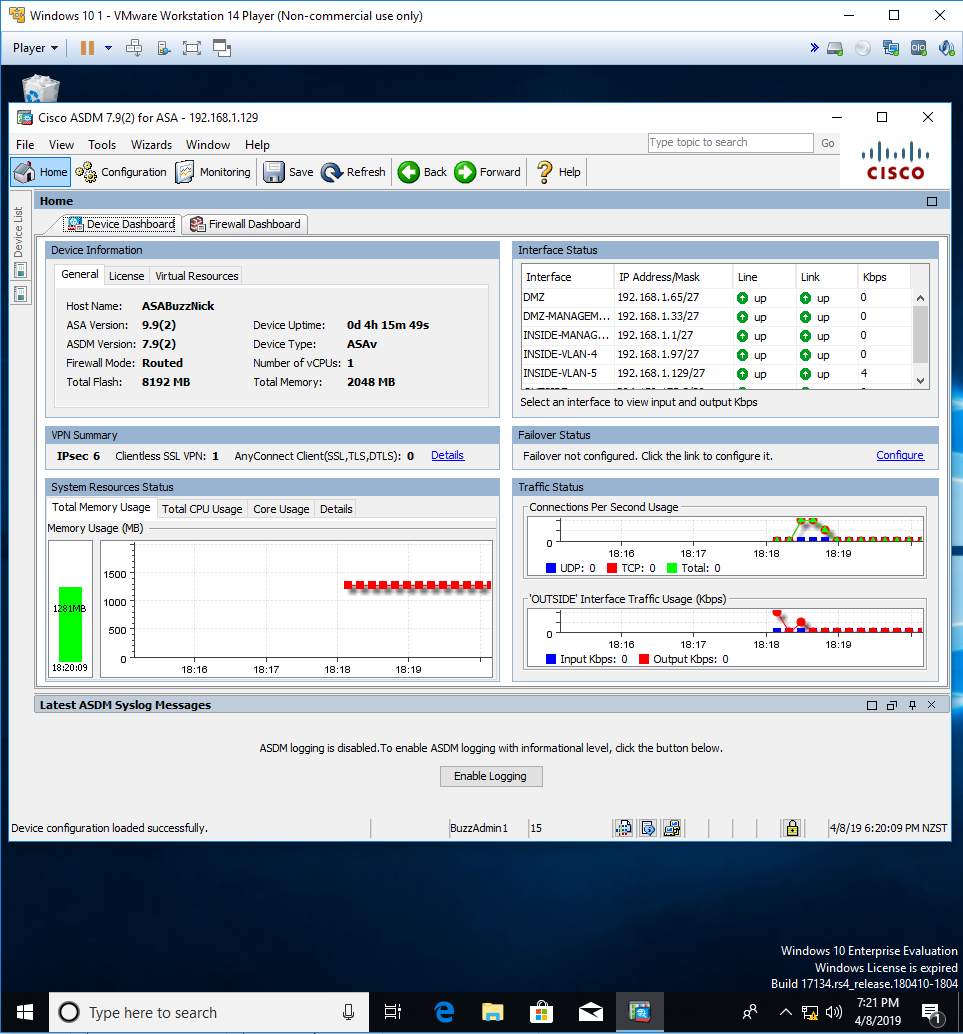
## Test 10 - Router r2 can make a SSH connection to manage the ASA



## GNS3 window with network topology

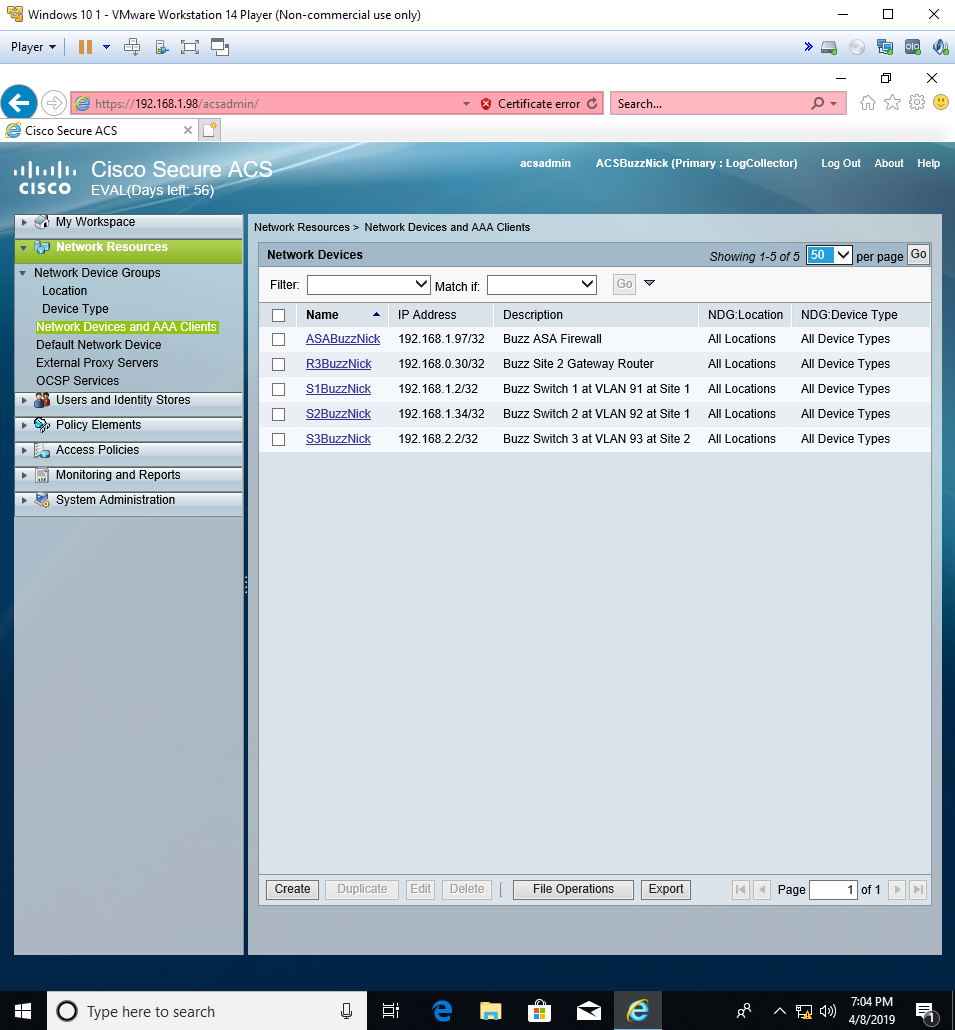


## ASDM running with a connection to the ASA

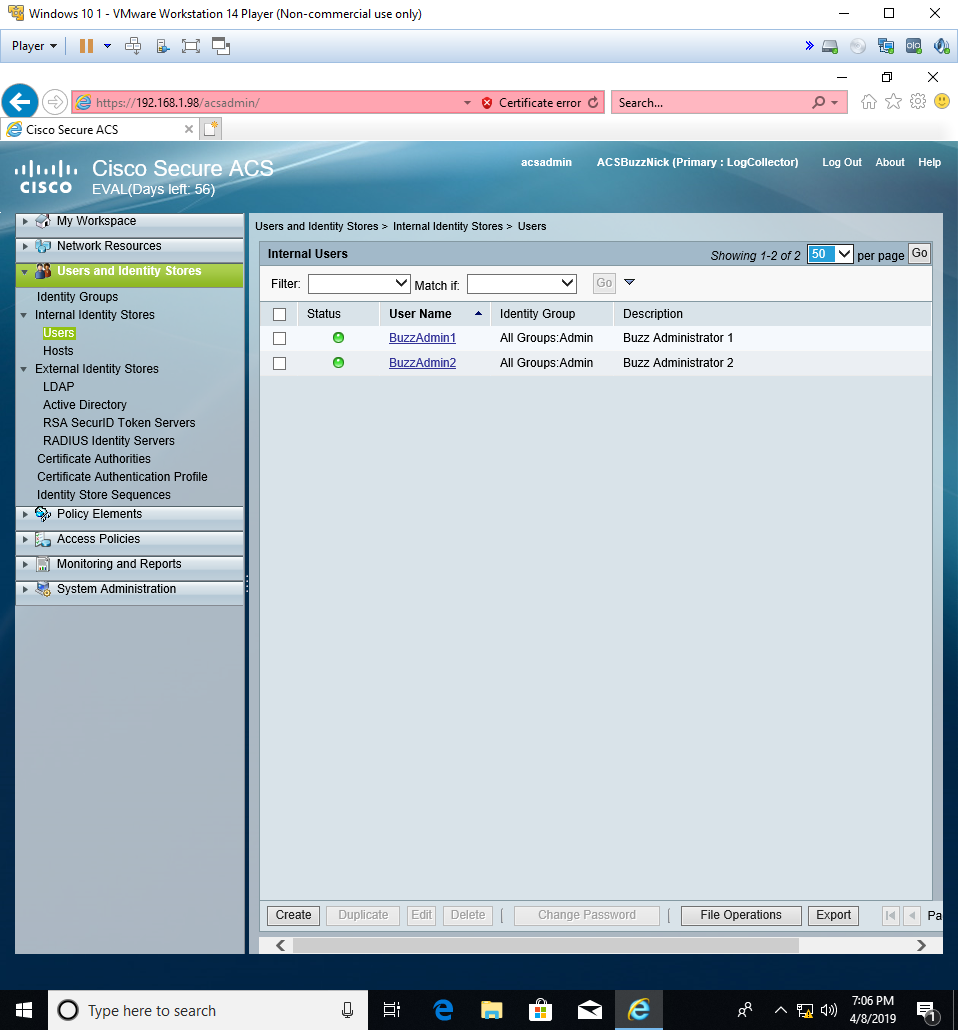


## Using the ACS

### Network Devices and AAA Clients page (under Network Resources)



### Users page (under Users and Identity Stores, Internal Identity Stores)



### Authorization page (under Access Polices, Access Services, Default Device Admin)

