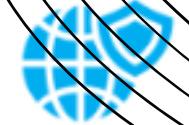




# NullSec

**YOUR SHIELD IN THE DIGITAL BATTLE**

**A NEW HORIZON FOR SUNTOWATER**



**NullSec**

# CONTENT

- 01** OUR TEAM
- 02** PROBLEM DOMAIN
- 03** GOALS & OBJECTIVES
- 04** TOPOLOGY DESIGN
- 05** DEMO
- 06** BIBLIOGRAPHY
- 07** Q&A



**NullSec**

# OUR TEAM



**Bruno  
Fernandes**

CyberSec  
Specialist



**Diogo  
Figueiredo**

Network Systems  
Designer & Engineer



**Hugo  
Ferraz**

Penetration  
Testing  
Specialist



**Rafael  
Silva**

CyberSec  
Specialist



NullSec

# BRUNO FERNANDES

## Cybersecurity Specialist

Background in operations and logistics:

- Process management, processing and distribution of mail.
- Responsible for dispatching and receiving international and Portuguese islands mail.
- Team leader currently one hundred and ten people.



**Fun fact:** I was a betfair exchange gambler, I saw more than 1300 football games in two and a half years.

# DIOGO FIGUEIREDO

Network Systems Designer and Engineer



Background in Biology and Hospitality:

Skillset:

- Customer Service oriented
- Attention to detail
- Interdisciplinary ability



**Fun fact:** ability to memorize numbers very easily, especially phone numbers.



NullSec

# HUGO FERRAZ

Penetration Testing Specialist



Background in Aviation Security:

Skillset: in risk assessment and management, crisis response, and compliance with aviation security protocols. Additionally, I have a solid background in team leadership and effective communication in challenging situations.



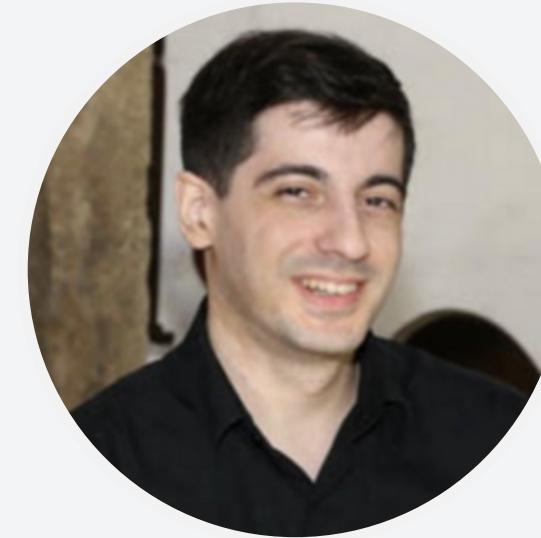
**Fun fact:** I have seen live the most renowned derbies and classics in world football, noting that none of them is the Barcelona vs Real. Which one is the best? I still have doubts between Casablanca or Belgrade! Buenos Aires ranks 4th behind Mostar (Herzegovina).



**NullSec**

# RAFAEL SILVA

Cybersecurity Specialist



Background in Digital Communications and Journalism:

Skillset:

- Hardware and software specialist (enthusiast)
- Knowledgeable on digital security and good practices
- Journalist-oriented researcher



**Fun fact:** I give free tech tips.

# SUNTOWATER: PROBLEM DOMAIN



**SUNTOWATER**, A RECENT GLOBEX ACQUISITION, FOCUSES ON ENHANCING ATMOSPHERIC WATER GENERATION.

CURRENT IT INFRASTRUCTURE LACKS ALIGNMENT WITH ECO-FRIENDLY OBJECTIVES.



REGULATORY COMPLIANCE FOR FEDERAL CONTRACTS REQUIRES UPDATING AND RECONFIGURING SUBSIDIARY IT INFRASTRUCTURE.



# GOALS AND OBJECTIVES

## Objective 1: VPN Tunnel

- Establish a site-to-site VPN tunnel between SunToWater network and server created by NullSec.

## Objective 2: Radius Authentication Server

- Implement RADIUS system with Active Directory (AD) integration.
- Captive portal for new network users.
- Authenticated users use their AD credentials for network access.

## Objective 3: Automated PowerShell script

- Design a PowerShell script for Windows Server DC setup.
- Final script encompass all requisite services for a DC setup on new installations.



# TOPLOGIES & FLOWCHARTS



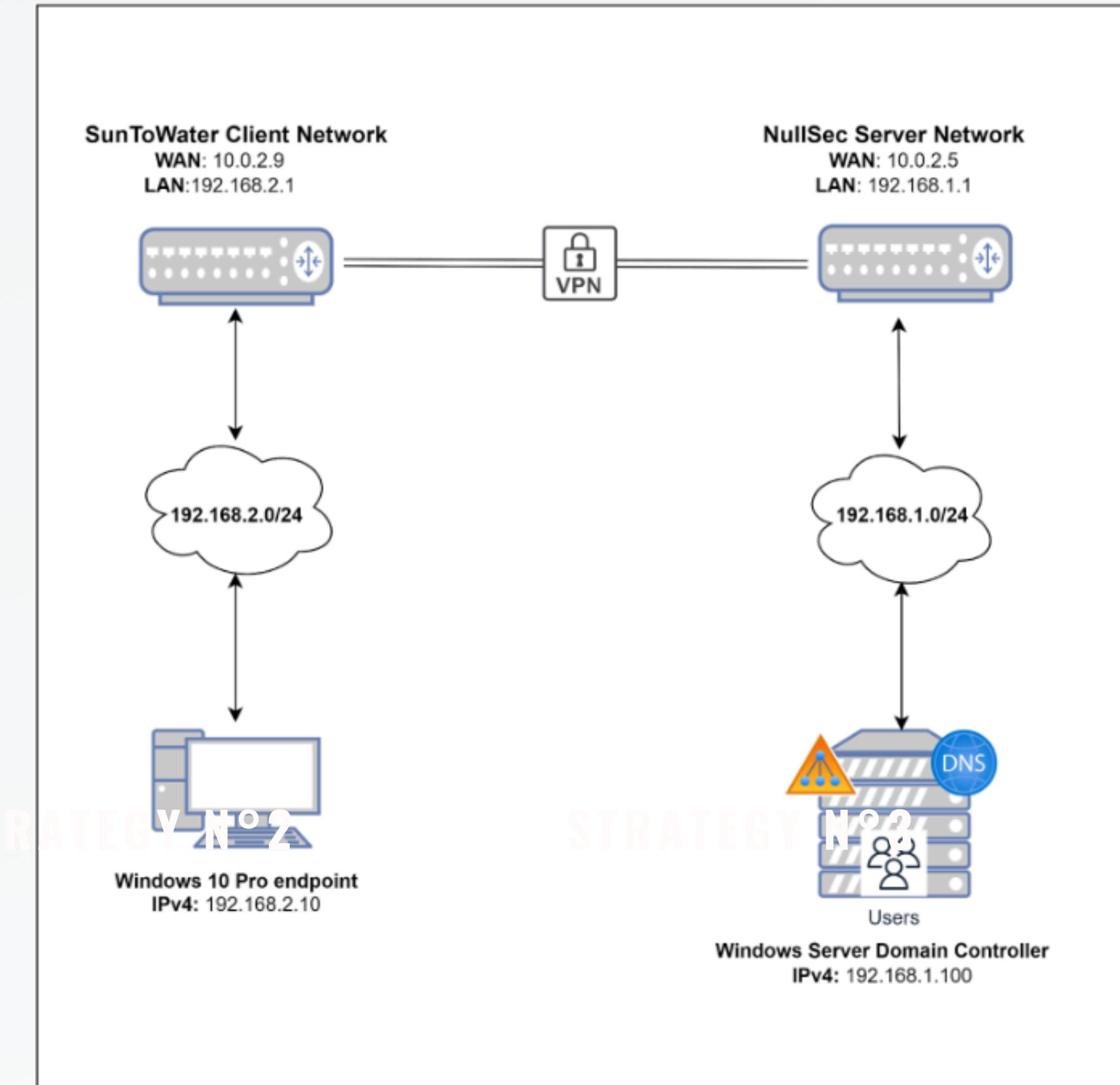
NullSec

Network Topology Design  
**VPN tunnel Site-to-Site**

STRATEGY N°1

STRATEGY N°2

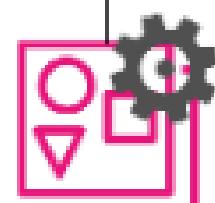
STRATEGY N°3



# Active Directory Organizational Chart



NullSec



OPERATIONS

Michael Scott, COO

Dwight Schrute

Andy Bernard

Phyllis Lapin-Vance



FINANCIAL

Bob Slydell, CFO

Jim Halpert

Kelly Kapoor

Meredith Palmer



SECURITY

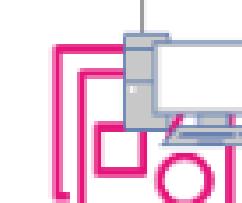
Courtney Hans, CISO

Luca Pacioli

Kevin Malone

Angela Martin

Oscar Martinez



IT

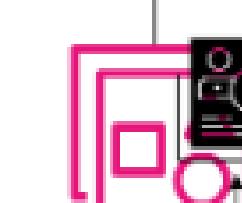
Bade Habib, CIO

Milton Waddams

Brian Krebs

Perry Cox

Bob Kelso



HR

Minerva McGonagall

Sybill Trelawney

John Dorian

Elliot Reid

Chris Turk



MARKETING

Peter Gibbons, CMO

Ron Weasley

Harry Potter

Hermione Granger

# DEMO



## IMPLEMENTATION OF VIRTUAL PRIVATE NETWORKING (VPN)

### 1. Environment Setup

Nullsec

- Pfsense Nullsec (Snapshot VPN TUNNEL) Running
- PfsenseSunToWater (Snapshot VPN TUN...) Running
- Windows10SuntoWater (Snapshot 1) Running
- WServerNullsec (Snapshot 12) Running

### 2. PfSense configuration

**Tunnels** Mobile Clients Pre-Shared Keys Advanced Settings

**General Information**

Description: Phase1SunToWater  
A description may be entered here for administrative reference (not parsed).

Disabled  Set this option to disable this phase1 without removing it from the list.

IKE ID: 1

**IKE Endpoint Configuration**

Key Exchange version: IKEv2  
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol: IPv4  
Select the Internet Protocol family.

Interface: WAN  
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway: 10.0.2.5  
Enter the public IP address or host name of the remote gateway.

**IPsec Tunnels**

ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
1	V2	WAN	Mutual PSK	AES (256 bits)	SHA256	14 (2048 bit)	Phase1SunToWater	<span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>
								<span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>
								<span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>

**IPsec Status**

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1	Phase1SunToWater	ID: 10.0.2.9	ID: 10.0.2.5	IKEv2	Rekey: 3087s (0:51:27)	AES_CBC (256)	Established
#2		Host: 10.0.2.9:500	Host: 10.0.2.5:500	Initiator	24012s (06:40:12)	HMAC_SHA2_256,128	115 seconds ago
		SPI: 526b1f991433bc22	SPI: b708dad9f05ea044			PBF_HMAC_SHA2_256	(00:01:55 ago)
						MODP_2048	
						Reauth: Disabled	

### 3. VPN tunnel connectivity

**IPsec Status**

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1	Phase2SunToWater	192.168.2.0/24	192.168.1.0/24	Rekey: 3087s (0:51:27)	128s (00:58:05)	AES_GCM_16	Bytes-In: 0 (0 B)
#3		c4162687	c0a86917	Responder	3485s (00:36:15)	IPComp: None	Bytes-Out: 0 (0 B)
				Install: 115s		Packets-In: 0	Packets-Out: 0

**IPsec Status**

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1	Phase2nullsec	ID: 10.0.2.5	ID: 10.0.2.9	IKEv2	Rekey: 23779s (0:46:18)	AES_CBC (256)	Established
#1		Host: 10.0.2.5:500	Host: 10.0.2.9:500	Responder	23779s (00:57:15)	HMAC_SHA2_256,128	165 seconds ago
		SPI: b708dad9f05ea044	SPI: 526b1f991433bc22			PBF_HMAC_SHA2_256	(00:02:45 ago)
						MODP_2048	
						Reauth: Disabled	

**IPsec Tunnels**

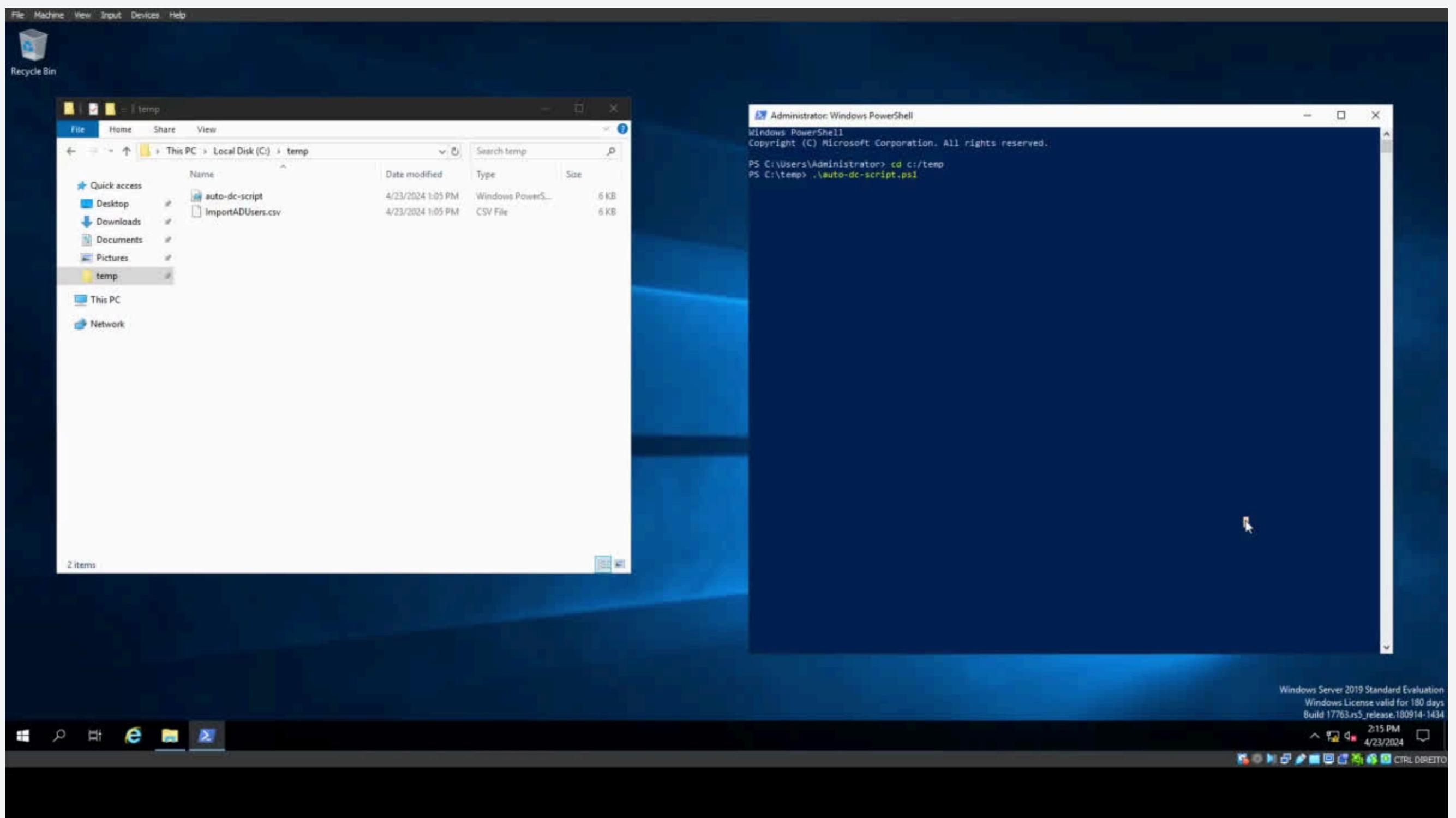
ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
1	V2	WAN	Mutual PSK	AES (256 bits)	SHA256	14 (2048 bit)	Phase1nullsec	<span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>
								<span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>
								<span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>

**IPsec Tunnels**

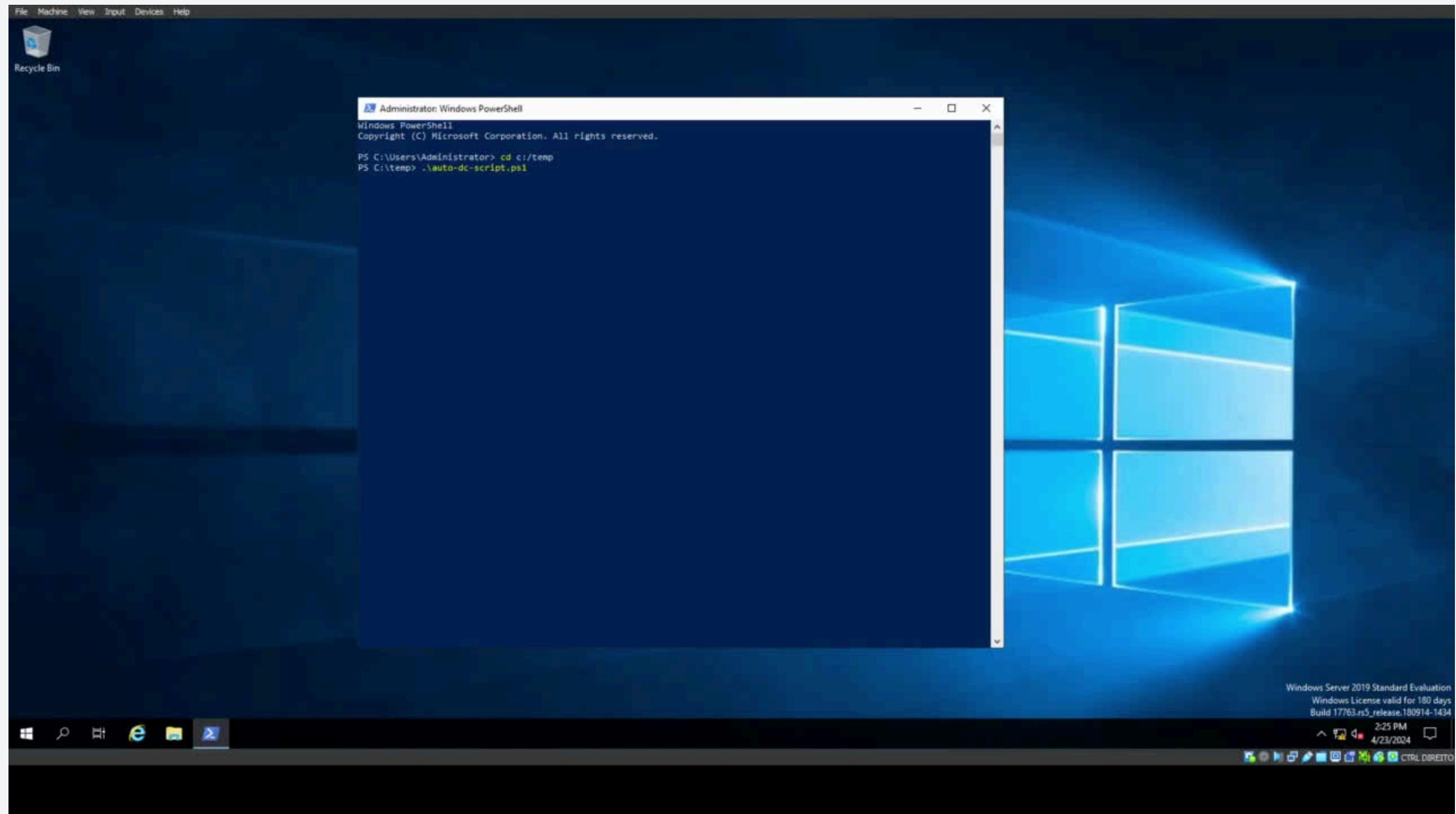
ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
1	V2	WAN	Mutual PSK	AES (256 bits)	SHA256	14 (2048 bit)	Phase2nullsec	<span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>
								<span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>
								<span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>

# WINDOWS SERVER DEPLOYMENT WITH POWERSHELL SCRIPT

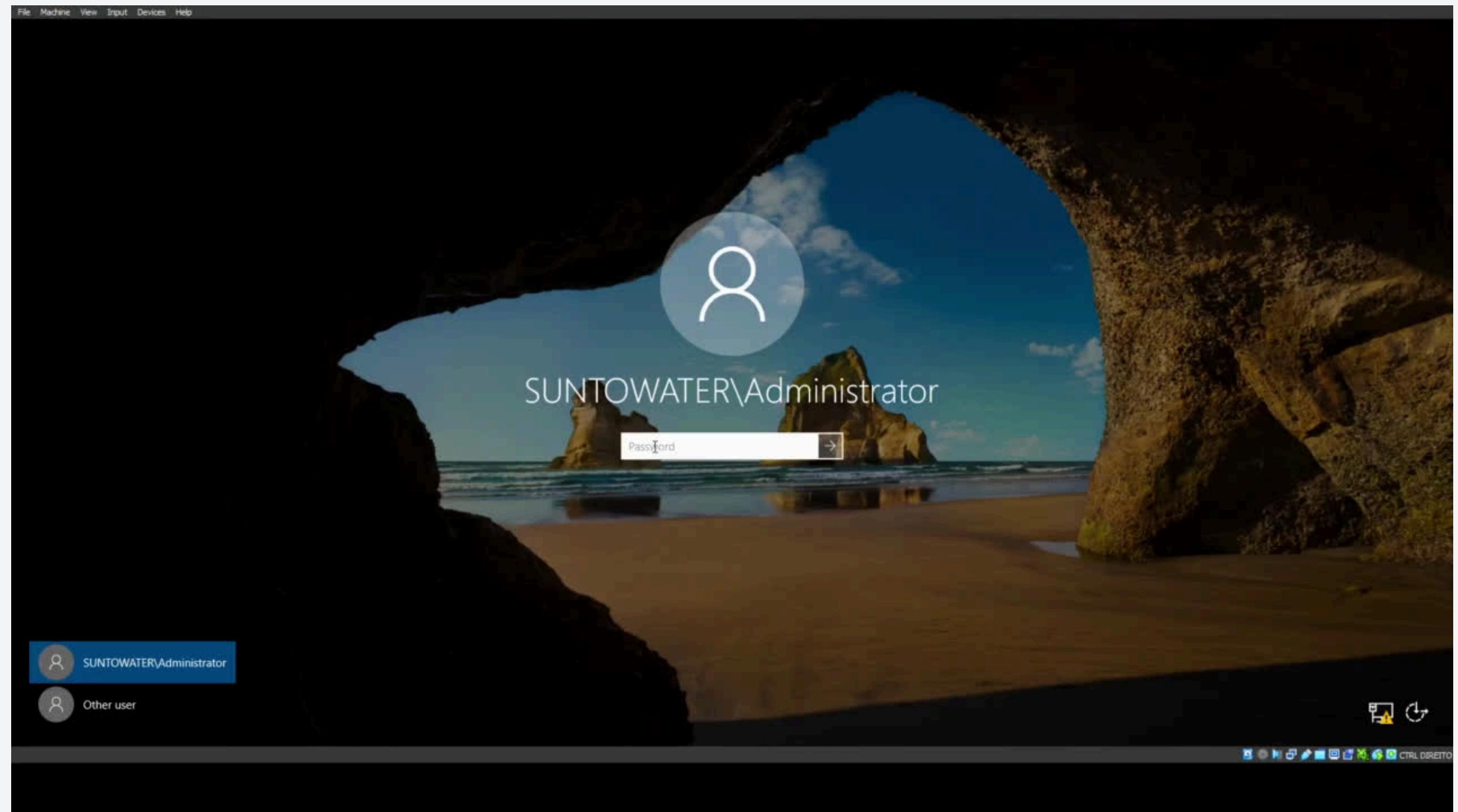
Network changes and  
system rename



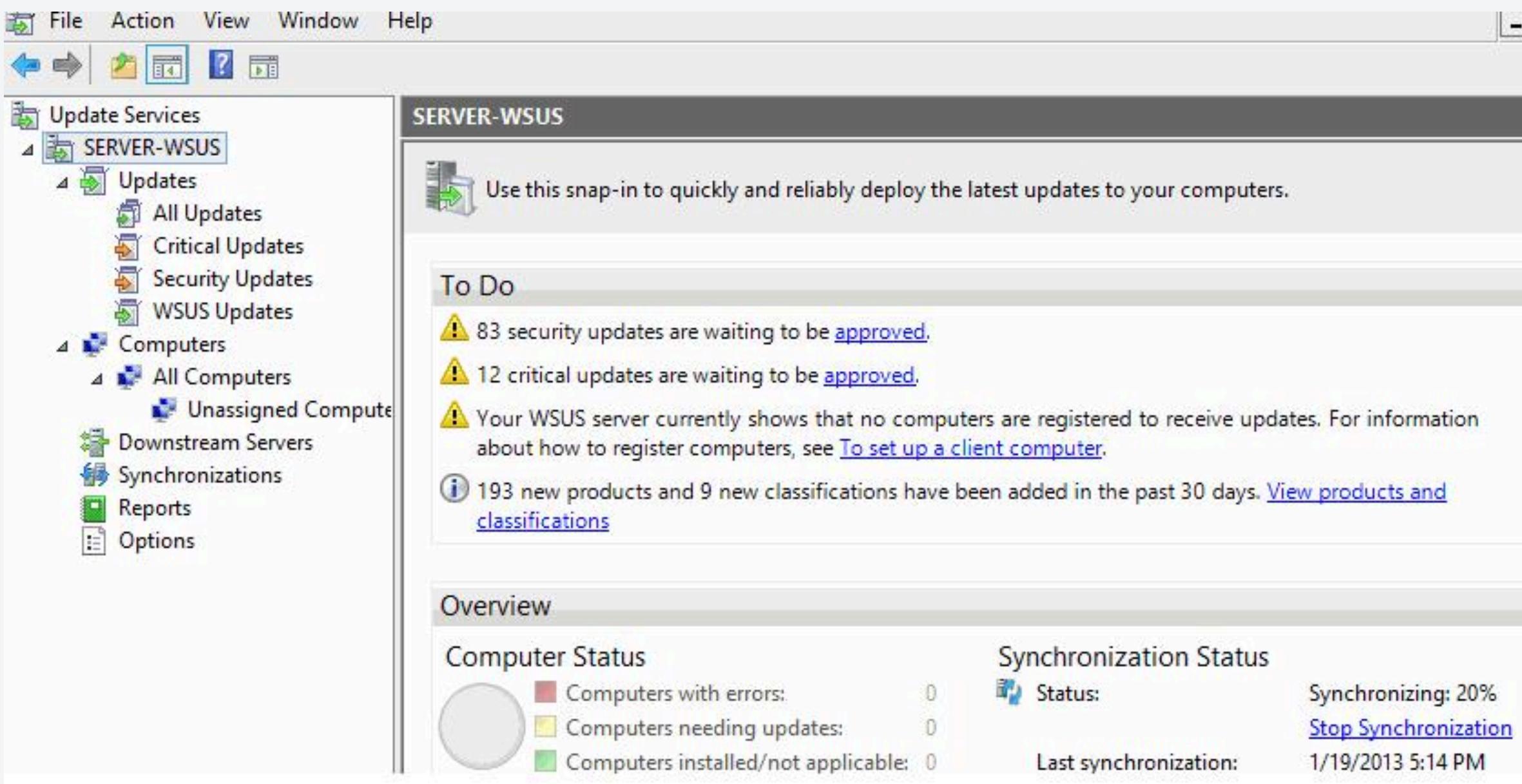
# Installation of AD and system elevation to DC



Active Directory configuration,  
creating OUs, importing Users  
from .csv



# OS VERSION CONTROL - WINDOWS SERVICE UPDATE SERVICE



- Domain Controller will control endpoint OS updates to endpoints

# BIBLIOGRAPHY



RADIUS config:

<https://securew2.com/blog/configure-windows-server-2019>

Set static & DHCP IP addresses in PowerShell

<https://www.pdq.com/blog/how-to-use-powershell-to-set-static-and-dhcp-ip-addresses/>

**GITHUB ORG LINK:** [HTTPS://GITHUB.COM/RMSVA/NULLSEC-PROJECT.GIT](https://github.com/rmsva/nullsec-project.git)

## LINKEDIN PROFILES:

- BRUNO FERNANDES: [HTTPS://WWW.LINKEDIN.COM/IN/BRUNO-FERNANDES-45735B304](https://www.linkedin.com/in/BRUNO-FERNANDES-45735B304)
- DIOGO FIGUEIREDO: [HTTPS://WWW.LINKEDIN.COM/IN/DIOGOFIGUEIREDO1904](https://www.linkedin.com/in/DIOGOFIGUEIREDO1904)
- HUGO FERRAZ: [HTTPS://WWW.LINKEDIN.COM/IN/!!!/](https://www.linkedin.com/in/!!!/)
- RAFAEL SILVA: [HTTPS://WWW.LINKEDIN.COM/IN/RAFAEL-S-38959B2B5/](https://www.linkedin.com/in/RAFAEL-S-38959B2B5/)



Windows



draw.io





# THANKS FOR WATCHING.

A huge shoutout to Code For All\_ for the help and support!

Any questions?