

# NTW216: Final Project

**JACKSON NESTLER**

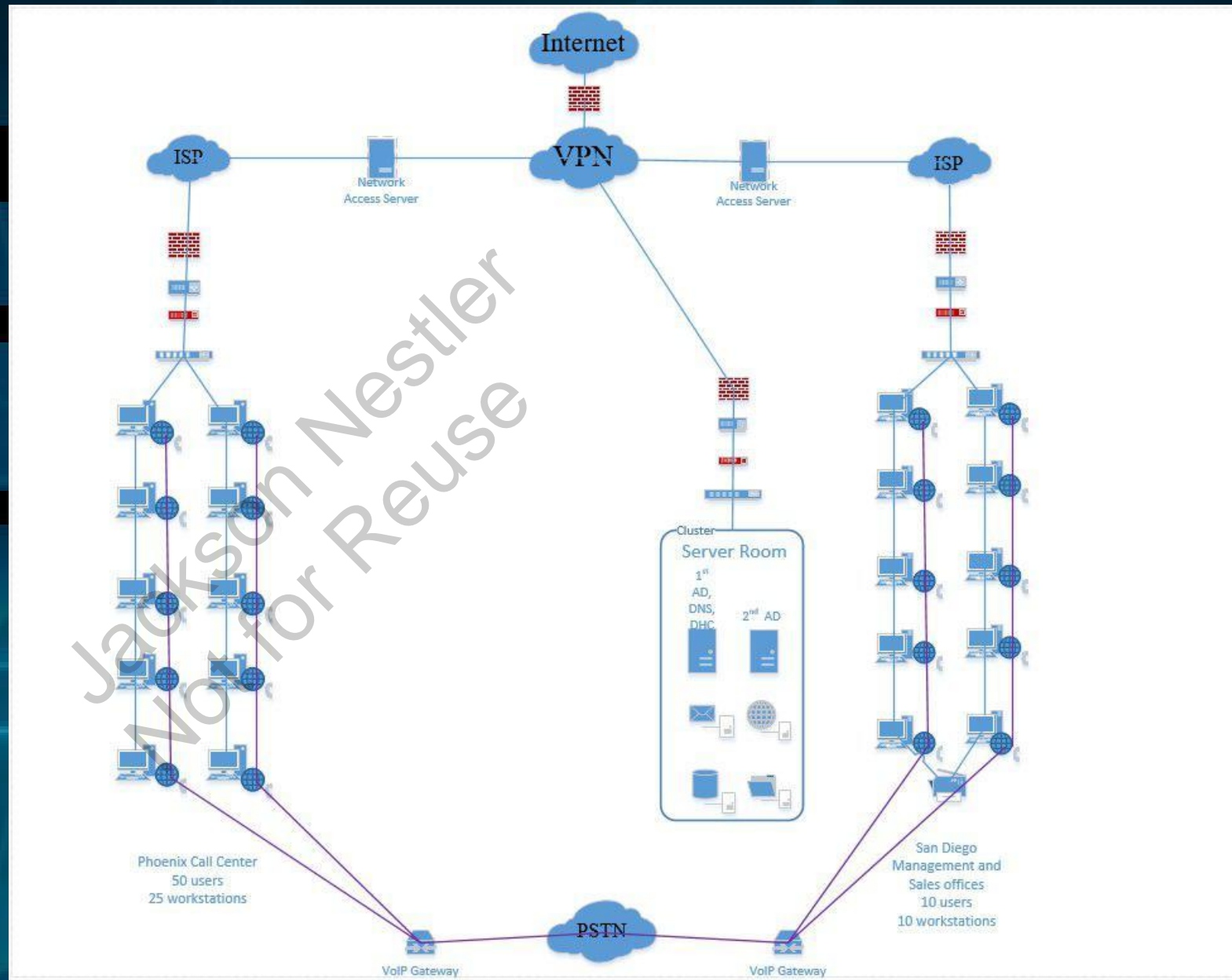
[REDACTED]

[REDACTED]

## Scenario

- 2x locations (San Diego, Phoenix)
- 50 users in call center, in Phoenix
- 10 users in management/sales, in San Diego.
- Include: VOIP, DNS, DHCP, Windows 2012/2016, Windows 10.

# Visio



# User Creation

- Ashley found a script that imports users from the contents of a csv into AD users & groups.
- Initially struggled to get the script to run; seemed code wasn't written properly.
- Due to time constraints, manually added users via the GUI.
- To-Do: Write a script that fills in information from a CSV or TXT.
  - Python imports the content of the CSV, using a "for x in NumUsers" loop create prepared PowerShell statements & saves prepared statements to a text file.
  - Admin copy and pastes the contents from the new text file into PowerShell.

## DNS/DHCP

- DNS is configured the same way it ships with AD...Any changes to it felt unwarranted.
- DHCP is enabled & configured but it's recommended that the machines receive a static address and fall back to DHCP when an image needs to be made.

# Group Policy

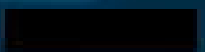
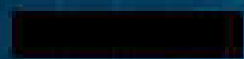
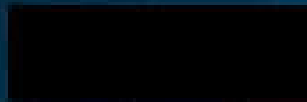
- The previous work-order that requested Group Policy had a few less-than-ideal choices. As security contractors we've made changes.
- DoD Secure Baseline:  
<https://github.com/iadgov/Secure-Host-Baseline>
  - Auto-magically configured Group Policy for common software (BitLocker, Chrome, EMET, Internet Explorer, Windows & Windows Firewall)
  - Left out some configuration (ie Adobe Reader) as it's proprietary and hasn't shown up in a work-order.
  - Enforced on the Domain Controller and Clients.

# Lab

- Small sample set of actual users

 Administrator	User	Built-in account for ad...	
 Alice Cooper	User		Alice Cooper
 [Redacted]	User		[Redacted]
 [Redacted]	User		[Redacted]
 Bob Thorn	User		Bob Thorn
 DefaultAccount	User	A user account manage...	
 Guest	User	Built-in account for gue...	
 [Redacted]	User		[Redacted]
 Jackson Nestler	User		Jackson Nestler
 Jane Doe	User		Jane Doe
 John Doe	User		John Doe
 krbtgt	User	Key Distribution Center ...	
 [Redacted]	User		[Redacted]
 SharePoint Farm Account	User		SharePoint Farm Account
 SharePoint Install Account	User		SharePoint Install Account
 SharePoint Profile Account	User		SharePoint Profile Account
 SharePoint Search Conten...	User		SharePoint Search Content Crawl
 SharePoint Service App A...	User		SharePoint Service App Account
 SharePoint Web App Acc...	User		SharePoint Web App Account
 SQL Install Account	User		SQL Install Account
 SQL Service Account	User		SQL Service Account
 Todd Bowman	User		Todd Bowman
 Wayne Kibbe	User		Wayne Kibbe
 Janet Jackson	User		Janet Jackson

# Lab



Jackson Nestler  
Not for Reuse

Properties

Security	Environment	Sessions	Remote control		
Remote Desktop	Services Profile	COM+	Attribute Editor		
General	Address	Account	Profile	Telephones	Organization
Published Certificates	Member Of	Password Replication	Dial-in	Object	

Member of:

Name	
Active Directory Domain Services Folder	
Domain Users	Pearson.local/Users
Management	Pearson.local/Users

Add... Remove

Primary group: Domain Users

Set Primary Group

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

OK Cancel Apply Help



# Splunk

localhost:8000/en-US/app/search/search

Home | Splunk 7.0.3

splunk > App: Search & Reporting

Administrator Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As New Table Close

host="WIN-T5ISR9S7DB" Last 24 hours

✓ 1,437 events (4/21/18 2:00:00.000 PM to 4/22/18 2:01:07.000 PM) No Event Sampling

Events (1,437) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page

< Hide Fields All Fields

Selected Fields  
a host 1  
a source 2  
a sourcetype 2

Interesting Fields  
a Account\_Domain 6  
a Account\_Name 10  
a Authentication\_Package 4  
a ComputerName 1  
# date\_hour 3  
# date\_mday 1  
# date\_minute 60

i	Time	Event
>	4/22/18 2:01:04.000 PM	04/22/2018 02:01:04 PM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4634 EventType=0 Show all 22 lines host = WIN-T5ISR9S7DB   source = WinEventLog:Security   sourcetype = WinEventLog:Security
>	4/22/18 2:01:04.000 PM	04/22/2018 02:01:04 PM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4624 EventType=0 Show all 70 lines host = WIN-T5ISR9S7DB   source = WinEventLog:Security   sourcetype = WinEventLog:Security
>	4/22/18 2:00:04.000 PM	04/22/2018 02:00:04 PM LogName=Security

# Splunk

- Utilizing the free version of Splunk and IIS, we have a working logging platform running locally on the Domain Controller.
- In the screenshot, we're monitoring for events from a Windows client. We could refine these searches to include failed logins, attempts to enumerate ports, etc.

# Services

**ROLES AND SERVER GROUPS**  
Roles: 6 | Server groups: 1 | Servers total: 1

<b>AD DS</b> 1 Manageability Events Services Performance BPA results	<b>DHCP</b> 1 Manageability Events Services Performance BPA results	<b>DNS</b> 1 Manageability Events Services Performance BPA results	<b>File and Storage Services</b> 1 Manageability Events Services Performance BPA results
<b>IIS</b> 1 Manageability Events Services Performance BPA results	<b>Remote Access</b> 1 Manageability Events Services Performance BPA results	<b>Local Server</b> 1 Manageability Events 1 Services 1 Performance BPA results 4/22/2018 1:59 PM	<b>All Servers</b> 1 Manageability Events 1 Services 1 Performance BPA results 4/22/2018 1:59 PM

\* Local server & All Servers are denoted in red are due to Splunk.