



2024

NEVADA CYBER RANGE (NCR) A CYBERSECURITY SANDBOX EVERYONE CAN USE



Cybersecurity Center

University of Nevada, Reno

Shamik Sengupta, Executive Director, ssengupta@unr.edu
Nancy LaTourrette, Deputy Director, nancy@unr.edu

<https://www.unr.edu/cybersecurity>



UNIVERSITY of NEVADA, RENO

- R1 and Tier1 Institution
- Land Grant and Flagship University of Nevada
- NSF EPSCoR State
- Emerging HSI (23%)
- Serving Rural Northern Nevada
- Nevada Indigenous Students Tuition-Free
- 21,000 Student Population
- Expanding Cybersecurity Programs and Facilities
- Center of Academic Excellence in Cyber Defense (CAE-CD)
- Interdisciplinary Cybersecurity Center: Research, Education and Outreach



CYBERSECURITY CENTER - FACULTY

AFFILIATED FACULTY

- 30 Members
- 9 Disciplines
 - Computer Science & Engineering
 - Electrical & Biomedical Engineering
 - Information Systems
 - School of Journalism
 - Political Science
 - Criminal Justice
 - Psychology
 - History
 - Public Health

Multi-Disciplinary
Cybersecurity Center

RESEARCH AREAS

- Vulnerability Assessments
- Malware Analysis
- Network Security Management
- Cyber-Physical System Security
- AI-Cybersecurity
- Data and User Privacy
- Data Mining and Analytics Privacy
- Biometrics
- Surveillance and Privacy Balance
- Sociopolitical Contexts of Disaster
- Behavioral System Analysis
- Organizational Behavior and Decision Making
- Cybersecurity Literacy
- Combating Misinformation and Disinformation

CYBERSECURITY CENTER - RESEARCH



NSF FUNDED RESEARCH

- Scholarship for Service (SFS)
- Research Experiences for Teachers in Engineering and Computer Science (RET)
 - 2015-2018
 - 2019-2022
 - 2023-2026
- Campus Cyberinfrastructure (CC*)
- CyberCorps® Capacity 2015-2017
- CyberCorps® Capacity 2017-2019
- Cybersecurity Innovation for Cyberinfrastructure (CICI)
- Faculty Early Development Career Program (CAREER)
- Innovations in Graduate Education (IGE)
- Improving Undergraduate STEM Education (IUSE)
- Research Experience for Undergraduates (REU)
- Secure and Trustworthy Cyberspace (SaTC)

13 NSF funded projects
> \$8M in funding

CYBERSECURITY CENTER - EDUCATION

UNDERGRADUATE CYBERSECURITY PROGRAMS

- Minor in Cybersecurity
 - └ Hands-on, in-depth, technical expertise in cyber defense
- Minor in Interdisciplinary Cybersecurity
 - └ Well-rounded curriculum from a range of disciplinary perspectives

GRADUATE CYBERSECURITY PROGRAMS

- Graduate Certificate in Cybersecurity
 - └ Current graduate students plus working professionals
- Online M.S. in Cybersecurity
 - └ Flexible program entirely online
- Personalized Advising
 - └ Advising with deputy and executive directors

CYBERSECURITY CENTER - OUTREACH

- RET Site: Research Experience in Cybersecurity for Nevada Teachers (RECNT)
- Annual Cybersecurity Conference
- Nevada Cyber Range
- Nevada Cyber Club
- Cybersecurity Seminar Series



Nevada Cyber Range (NCR)

- Cybersecurity Sandbox
- Operational Environment for Research, Training, Education
- Physical and Remote Access

INVITED TALKS

- Department of Homeland Security, **Janet Napolitano**
- U.S. Army Research Laboratory
- U.S. Army Cyber Command
- National Security Agency
- FBI, Cyber & Counterintelligence
- National Research Labs
- IBM Research Center
- Symantec, Global Security Intelligence Operations
- State of Nevada, CISO
- Nevada Office of Cyber Defense Coordination
- National Cyber League Commissioner
- Bay Area Cyber League, Regional Coordinator
- National and Local Security Corporations
- University Faculty and Researchers

CYBERSECURITY CENTER - COMMUNITY COLLABORATORS

- Nevada Army National Guard
- Nevada Air National Guard
- Army Research Lab
- Nevada National Security Test Site
- Electronic Frontier Foundation (EFF)
- Nevada School Districts & Community Colleges
- Local, Regional and National Corporations

- NV Energy
- Sierra Nevada Corporation
- CISCO Systems
- Hewlett Packard Enterprise
- Startup companies...

2024 CAE Community Symposium

NEVADA CYBER RANGE (NCR)

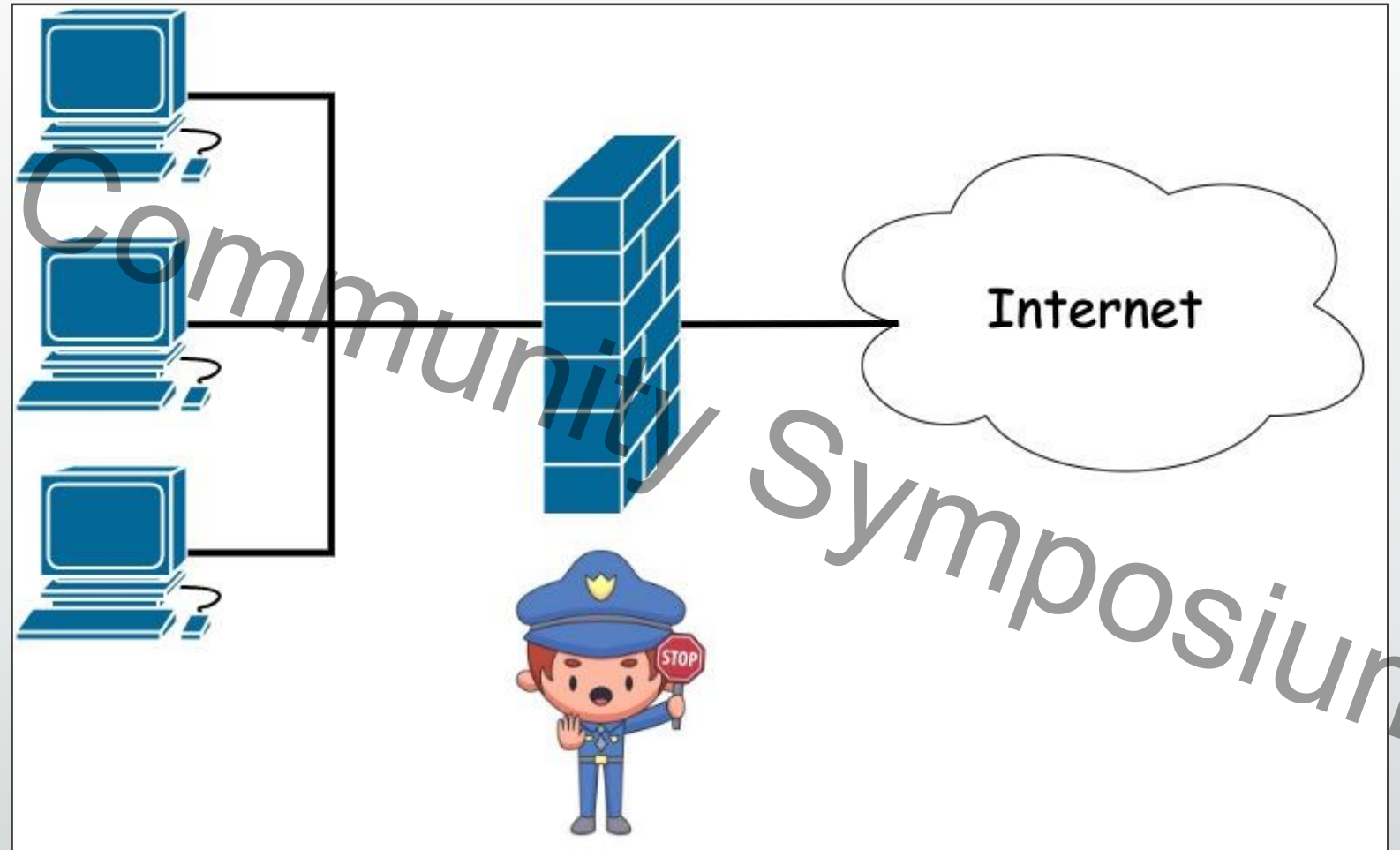
A CYBERSECURITY SANDBOX FOR RESEARCH, EDUCATION
& OUTREACH

Problems

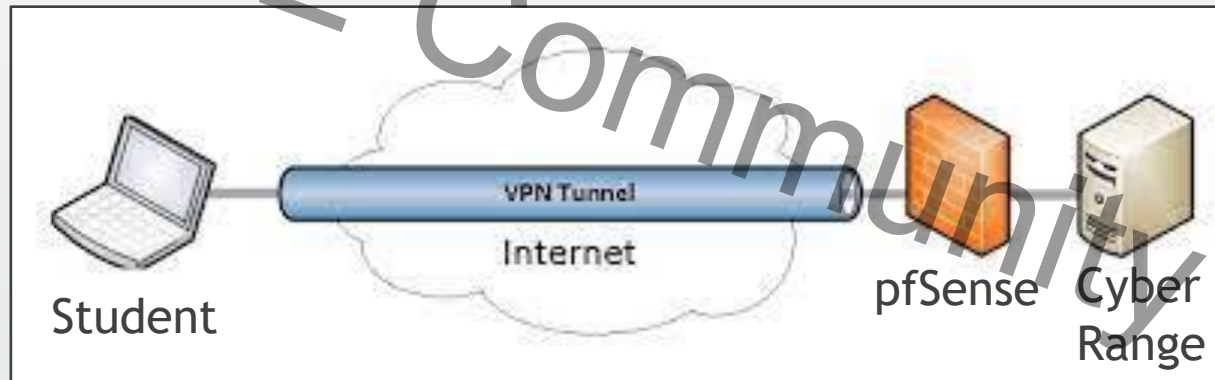
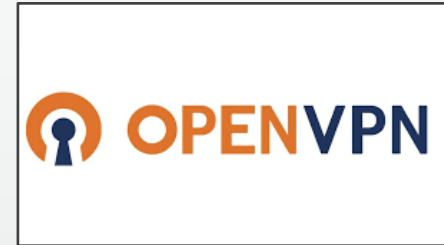
- Limited access to websites because of firewalls
- Customizable environments
- Ease of access from anywhere
- Administrative control of machine
- Instructor access to student environment
- Reproducible instances
- Realistic experience for students

Limited Access from campus

- School district firewall rules can make access to resources a problem!
- Tools needed to ensure student safety on the Internet



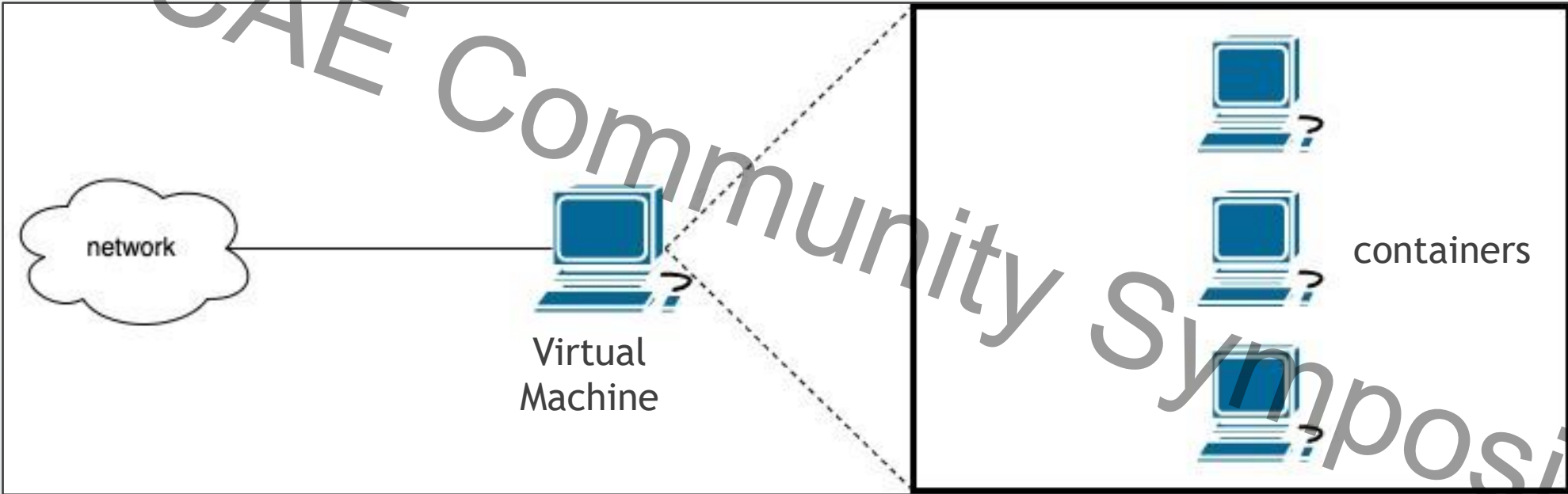
System access via vpn tunnel and remote firewall



- VPN provides tunnel access to remote network
- Users are authenticated via OpenVPN
- Student machine becomes part of the remote network
- Traffic can traverse the local firewall

Customizable environments

2024 CAE Community Symposium



Accessible from anywhere



- Remote system available via a browser
- Can be accessed from any OS
- Accessible through mobile devices
- Accessible via command line

```
Directory of C:\Program Files\Adobe\Adobe Photoshop 2022\Required\Plug-ins\Generat
or\assets.generate\node_modules\tap\lib
05/04/2022 01:48 PM <DIR> ..
05/04/2022 01:48 PM <DIR> .
05/04/2022 01:48 PM      14,895 tap.js
1 File(s)              14,895 bytes

Directory of C:\Program Files\Adobe\Adobe Photoshop 2022\Required\Plug-ins\Generat
or\assets.generate\node_modules\universalify
05/04/2022 01:48 PM <DIR> ..
05/04/2022 01:48 PM <DIR> .
05/04/2022 01:48 PM      777 index.js
05/04/2022 01:48 PM      1,100 LICENSE
05/04/2022 01:48 PM      1,585 package.json
05/04/2022 01:48 PM      1,799 README.md
4 File(s)              5,261 bytes

Directory of C:\Program Files\Adobe\Adobe Photoshop 2022\Required\Plug-ins\Generat
```



2024 CAE Community Symposium

Full administrative control

- Student has 'root' administrative privileges on their own machine
- Able to make changes to OS
- Can install/uninstall/update software
- Can destroy the environment without affecting other users
- Instances can easily be restored (with some loss of work)

Instructor Access

- Instructor can be added to all machines to provide support
- Access to machine logs to monitor activity
- Environment can be prepped to support instruction



Symposium

Recoverable instances

- Periodic backups are made of each instance
- Student VM can be replaced if destroyed
- Minimal loss of previous work



Realistic user experience

- Students have adjustable levels of control
- Changes can be made
- Realistic user experience



Scalable hosting capability

2024

The screenshot displays the Proxmox Virtual Environment (VE) 8.1.4 interface. The main window shows a list of virtual machines (VMs) under the 'Node pve' view. The interface includes a sidebar with navigation options like 'Server View', 'Datacenter', and 'Node pve'. The main area contains a table of VMs with columns for Type, Description, Disk usage, Memory usage, CPU usage, Uptime, Host CPU, Host Mem, and Tags. The VMs are listed in descending order of CPU usage.

Type	Description	Disk usage...	Memory us...	CPU usage	Uptime	Host CPU ...	Host Mem...	Tags
qemu	2030 (NeschVM)	0.0 %	60.5 %	0.2% of 2 ...	30 days 11:1...	0.0% of 96...	0.3 %	647
qemu	8002 (debTemplateDHCP)	-	-	-	-	-	-	647 debian12 template
qemu	509 (OWASP)	0.0 %	11.1 %	0.3% of 4 ...	30 days 11:2...	0.0% of 96...	0.1 %	bill
qemu	510 (OWASP2)	-	-	-	-	-	-	bill
qemu	1000 (BillOwaspDocker)	0.0 %	64.6 %	0.2% of 2 ...	30 days 11:2...	0.0% of 96...	0.2 %	bill
qemu	8000 (debian-cloud)	-	-	-	-	-	-	debian12 demo template test
qemu	8005 (debCloudTemplate)	-	-	-	-	-	-	debian12 note service template
qemu	108 (shamikDemo)	0.0 %	14.7 %	0.1% of 4 ...	30 days 11:2...	0.0% of 96...	0.2 %	demo
qemu	111 (yoinkVM)	0.0 %	93.0 %	0.3% of 8 ...	8 days 02:16...	0.0% of 96...	1.0 %	demo
qemu	112 (tester1)	0.0 %	93.1 %	0.0% of 8 ...	8 days 02:15...	0.0% of 96...	1.0 %	demo
qemu	113 (tester2)	0.0 %	92.6 %	0.0% of 8 ...	8 days 02:15...	0.0% of 96...	1.0 %	demo
qemu	114 (okkoVM)	0.0 %	93.8 %	0.0% of 8 ...	7 days 21:58...	0.0% of 96...	1.0 %	demo
qemu	115 (worldhVM)	0.0 %	92.7 %	0.4% of 8 ...	7 days 22:43...	0.0% of 96...	1.0 %	demo
qemu	116 (qemu-guest-agent)	0.0 %	94.2 %	0.4% of 8 ...	2 days 22:48...	0.0% of 96...	1.0 %	demo
qemu	197 (BillDemo)	0.0 %	14.6 %	0.1% of 4 ...	30 days 11:2...	0.0% of 96...	0.2 %	demo
qemu	198 (shamikDemo2)	0.0 %	15.2 %	0.1% of 4 ...	30 days 11:2...	0.0% of 96...	0.2 %	demo
qemu	199 (jayBeta)	0.0 %	30.0 %	0.1% of 2 ...	23 days 21:3...	0.0% of 96...	0.2 %	demo
qemu	211 (NancyWindows)	-	-	-	-	-	-	demo
qemu	100 (kali-rdp)	-	-	-	-	-	-	demo
qemu	103 (honeypot)	-	-	-	-	-	-	george
qemu	9000 (grkmail)	-	-	-	-	-	-	george
qemu	7998 (pfsense)	0.0 %	95.8 %	0.5% of 24 ...	30 days 11:1...	0.1% of 96...	8.1 %	george service
qemu	8003 (WindowsAD)	0.0 %	62.4 %	0.7% of 4 ...	30 days 11:1...	0.0% of 96...	0.7 %	george service windows
qemu	7990 (DebianDocker)	0.0 %	67.9 %	0.4% of 2 ...	30 days 11:1...	0.0% of 96...	0.2 %	note
qemu	7997 (debTempBackup)	-	-	-	-	-	-	note
qemu	7999 (backup)	-	-	-	-	-	-	note
qemu	104 (debTemp)	-	-	-	-	-	-	note

IDS capability (snort/suricata)

Alert Log View Settings

Instance to View: (LAN2) OPT1
Choose which instance alerts you want to inspect.

Save or Remove Logs: [Download](#) [Clear](#)
All alert log files for selected interface will be downloaded. Clear the currently active Alerts log file.

Save Settings: [Save](#) Refresh Refresh
Save auto-refresh and view settings. Default is ON.

Number of alerts to display. Default is 250.

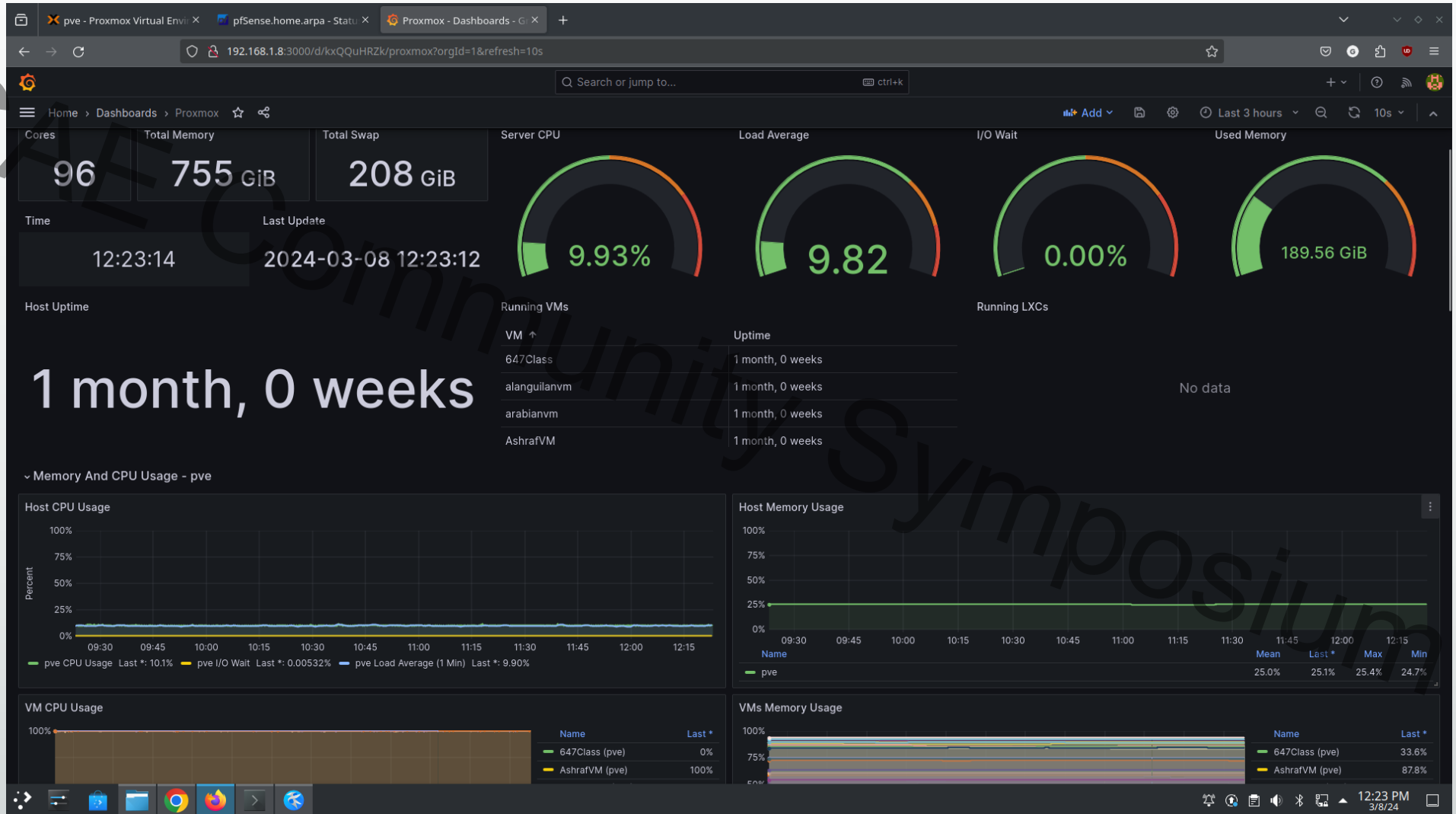
Alert Log View Filter [+](#)

Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
03/06/2024 16:18:39	⚠	3	TCP	Misc activity	96.16.55.145	80	192.168.2.102	55703	1-2014819	ET INFO Packed Executable Download
03/01/2024 17:23:52	⚠	3	TCP	Not Suspicious Traffic	192.168.1.27	52632	192.168.2.102	7680	1-2027766	ET POLICY Windows Update P2P Activity
03/01/2024 17:23:11	⚠	3	TCP	Not Suspicious Traffic	192.168.1.27	52631	192.168.2.102	7680	1-2027766	ET POLICY Windows Update P2P Activity
03/01/2024 17:22:31	⚠	3	TCP	Not Suspicious Traffic	192.168.1.27	52630	192.168.2.102	7680	1-2027766	ET POLICY Windows Update P2P Activity
03/01/2024 17:21:50	⚠	3	TCP	Not Suspicious Traffic	192.168.1.27	52629	192.168.2.102	7680	1-2027766	ET POLICY Windows Update P2P Activity
03/01/2024 17:21:10	⚠	3	TCP	Not Suspicious Traffic	192.168.1.27	52627	192.168.2.102	7680	1-2027766	ET POLICY Windows Update P2P Activity
03/01/2024 17:20:30	⚠	3	TCP	Not Suspicious Traffic	192.168.1.27	52626	192.168.2.102	7680	1-2027766	ET POLICY Windows Update P2P Activity
03/01/2024 17:19:49	⚠	3	TCP	Not Suspicious Traffic	192.168.1.27	52625	192.168.2.102	7680	1-2027766	ET POLICY Windows Update P2P Activity
03/01/2024 17:19:09	⚠	3	TCP	Not Suspicious Traffic	192.168.1.27	52623	192.168.2.102	7680	1-2027766	ET POLICY Windows Update P2P Activity
03/01/2024 17:18:28	⚠	3	TCP	Not Suspicious Traffic	192.168.1.27	52621	192.168.2.102	7680	1-2027766	ET POLICY Windows Update P2P Activity

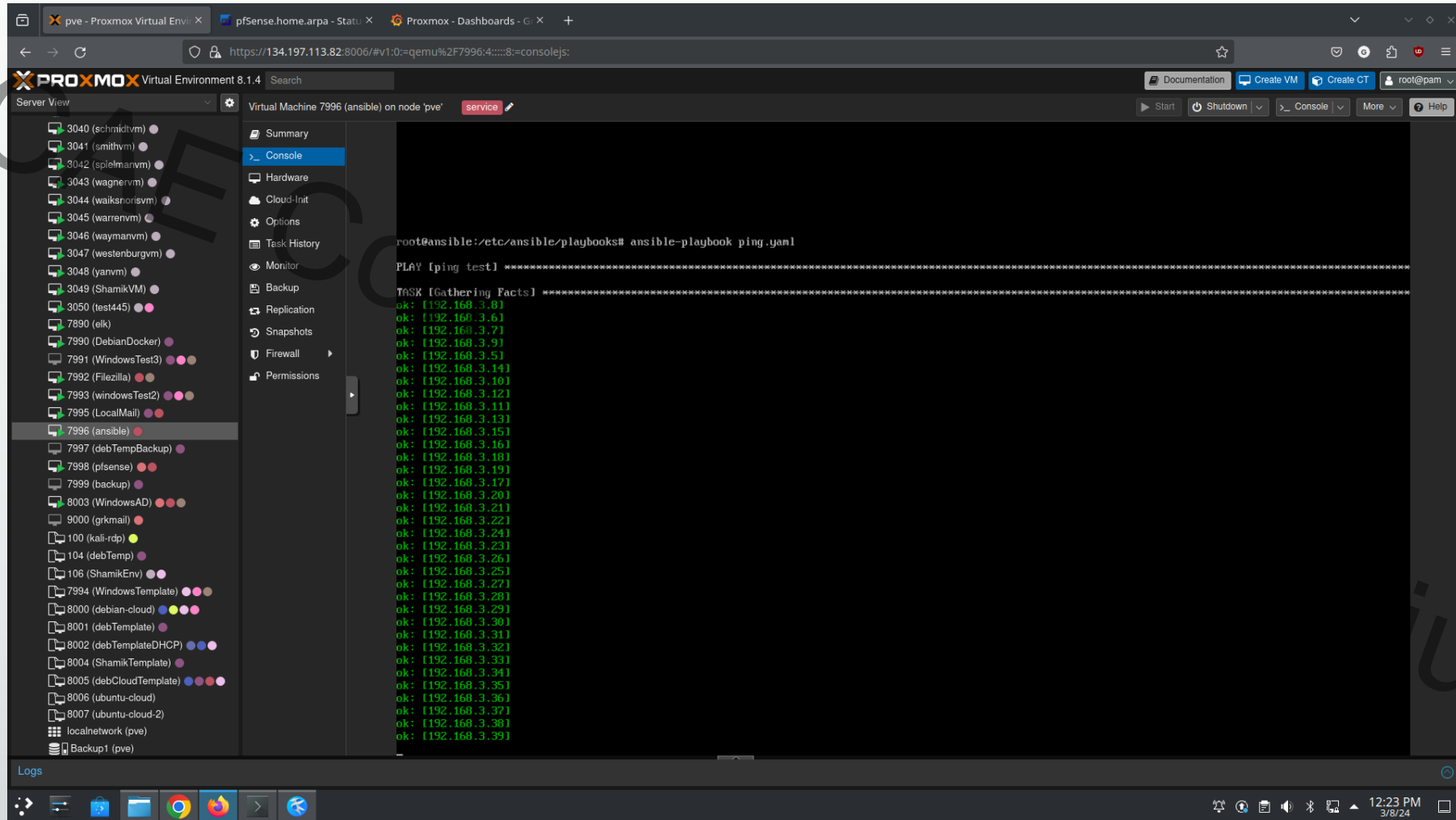
System monitoring

2024 CTF



Automated management via Ansible

2024



The screenshot displays the Proxmox Virtual Environment (VE) interface. On the left, a server view shows a list of virtual machines, with '7996 (ansible)' selected. The main console window shows the execution of an Ansible playbook named 'ping.yml'. The output indicates that the 'Gathering Facts' task is successful for all 32 IP addresses in the range 192.168.3.81 to 192.168.3.112. The interface includes a navigation menu on the left with options like Summary, Console, Hardware, and Options. The bottom status bar shows the time as 12:23 PM on 3/8/24.

```
root@ansible:/etc/ansible/playbooks# ansible-playbook ping.yml

PLAY [ping test] *****

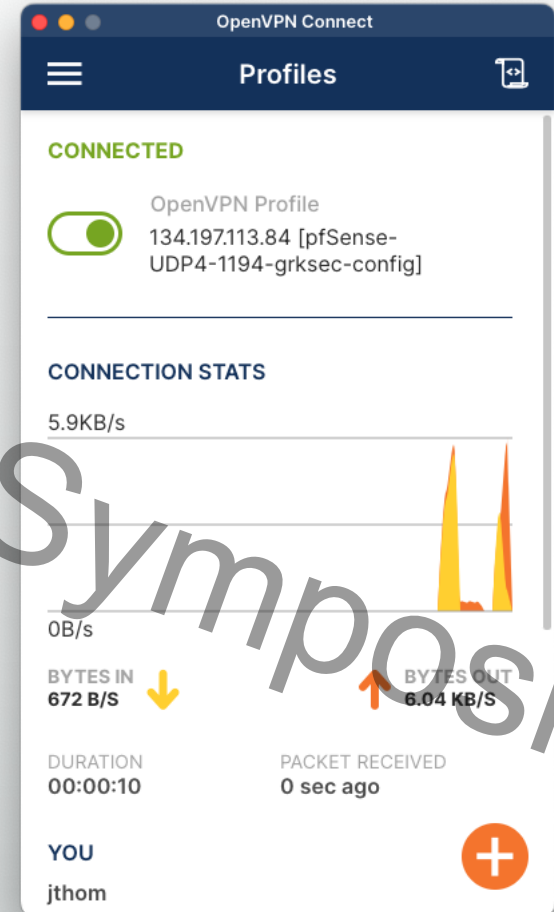
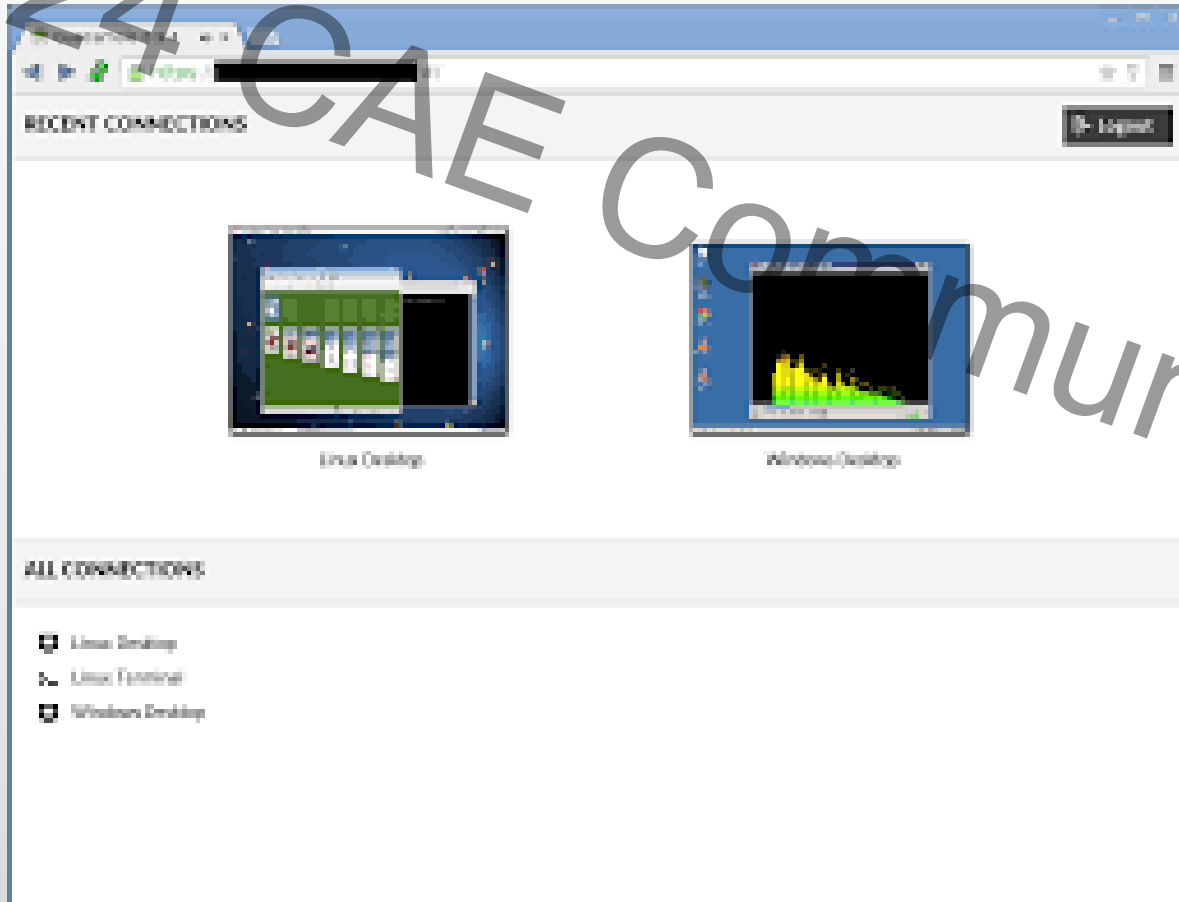
TASK [Gathering Facts] *****
ok: [192.168.3.81]
ok: [192.168.3.61]
ok: [192.168.3.71]
ok: [192.168.3.91]
ok: [192.168.3.51]
ok: [192.168.3.141]
ok: [192.168.3.101]
ok: [192.168.3.121]
ok: [192.168.3.111]
ok: [192.168.3.131]
ok: [192.168.3.151]
ok: [192.168.3.161]
ok: [192.168.3.181]
ok: [192.168.3.191]
ok: [192.168.3.171]
ok: [192.168.3.201]
ok: [192.168.3.211]
ok: [192.168.3.221]
ok: [192.168.3.241]
ok: [192.168.3.231]
ok: [192.168.3.261]
ok: [192.168.3.251]
ok: [192.168.3.271]
ok: [192.168.3.281]
ok: [192.168.3.291]
ok: [192.168.3.301]
ok: [192.168.3.311]
ok: [192.168.3.321]
ok: [192.168.3.331]
ok: [192.168.3.341]
ok: [192.168.3.351]
ok: [192.168.3.361]
ok: [192.168.3.371]
ok: [192.168.3.381]
ok: [192.168.3.391]
```

ium

VPN or browser-based access

Openvpn - ssh connection to VM

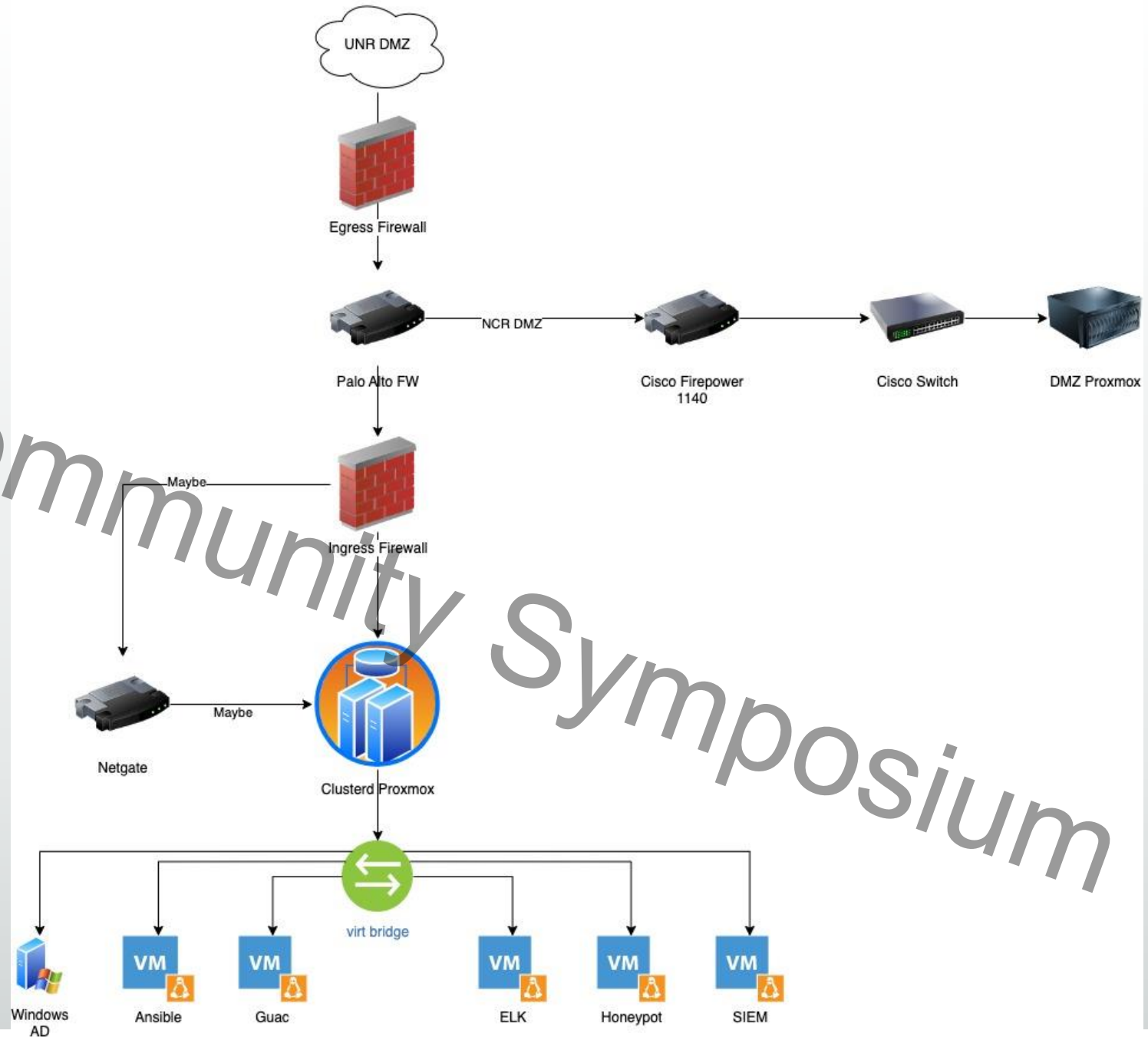
Guacamole - access via smart device or computer



Future Plans...

2024 CAE

- Expanded Proxmox system
- Clustered servers for capacity
- DMZ within the UNR DMZ
- Multiple firewalls
- Multiple IDS/IPS
- Honeypots
- ELK stack SIEM
- Large visual monitor to view attacks
- Cisco subnet with routing (CCNA)



CYBERSECURITY CENTER

Are you interested to use Nevada Cyber Range for your class or lab? Reach out to Dr. Shamik Sengupta, Executive Director, UNR Cybersecurity Center at ssengupta@unr.edu

<https://www.unr.edu/cybersecurity>

