

# “Enhancing the Preparation of Next-generation Cyber Professionals”

July 22, 2020 – June 30, 2022

PI: Jorge Crichigno

FY19 Funding Opportunity Announcement (FOA) for the Office of Naval  
Research (ONR) Navy ROTC Cybersecurity Training Program

McNair Center  
February 2, 2022

# FOA Scope

- Expand the technical skills taught to university students, ROTC programs...
- Develop the research capacity of participants...
- Establish meetings of stakeholders... connect relevant people and organizations...

# USC Team

---



Dr. Jorge Crichigno  
(College of Engr. and Comp.)



Jodi Salter  
(ROTC, Walker Institute)



1LT Ebony Penton  
(ROTC Command)



MAJ Christina Knight  
(Former ROTC  
Command, Co-PI)



Anthony Dillon  
(Internships)

# ONR Education and Workforce

---



Dr. Michael Simpson  
Director of Education and Workforce at Office of Naval Research

# Project Goals

1. Develop a cybersecurity concentration
2. Establish an undergraduate research program in cybersecurity
3. Deploy virtual equipment pods on a virtual platform
4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation

# Project Goals

## 1. Develop a cybersecurity concentration

| Cybersecurity Operations, Minor |  |           |
|---------------------------------|--|-----------|
| Degree Requirements (18 Hours)  |  |           |
| Course                          | Title  | Credits   |
| Select one of the following:    |  | 3         |
| <a href="#">ITEC 101</a>        | Thriving in the Tech Age                       |           |
| <a href="#">ITEC 204</a>        | Program Design and Development                 |           |
| <a href="#">ITEC 552</a>        | Linux Programming and Administration           |           |
| <a href="#">ITEC 233</a>        | Introduction to Computer Hardware and Software | 3         |
| <a href="#">ITEC 245</a>        | Introduction to Networking                     | 3         |
| <a href="#">ITEC 293</a>        | Cybersecurity Operations                       | 3         |
| <a href="#">ITEC 445</a>        | Advanced Networking                            | 3         |
| <a href="#">ITEC 493</a>        | Information Technology Security for Managers   | 3         |
| <b>Total Credit Hours</b>       |  | <b>18</b> |

<https://tinyurl.com/4mbj3z4k>

# Project Goals

## 1. Develop a cybersecurity concentration

| Cybersecurity Operations, Minor |  |           |
|---------------------------------|--|-----------|
| Degree Requirements (18 Hours)  |  |           |
| Course                          | Title  | Credits   |
| Select one of the following:    |  | 3         |
| <a href="#">ITEC 101</a>        | Thriving in the Tech Age                       |           |
| <a href="#">ITEC 204</a>        | Program Design and Development                 |           |
| <a href="#">ITEC 552</a>        | Linux Programming and Administration           |           |
| <a href="#">ITEC 233</a>        | Introduction to Computer Hardware and Software | 3         |
| <a href="#">ITEC 245</a>        | Introduction to Networking                     | 3         |
| <a href="#">ITEC 293</a>        | Cybersecurity Operations                       | 3         |
| <a href="#">ITEC 445</a>        | Advanced Networking                            | 3         |
| <a href="#">ITEC 493</a>        | Information Technology Security for Managers   | 3         |
| <b>Total Credit Hours</b>       |  | <b>18</b> |

<https://tinyurl.com/4mbj3z4k>

### Cyber Intelligence Major

Cyber Intelligence expands the cyber world beyond code and technology. Our degree prepares you to master all sides of cybersecurity challenges — political, psychological, and global.

<https://tinyurl.com/4x566mpu>

# Project Goals

## 2. Establish an undergraduate research program in cybersecurity

Participants include ROTC cadets (Navy, Army, Air Force), Veterans, and students from CS, IT, IS, Cyber Intelligence

| Name        | Project  |
|-------------|--|
| Christian S | Application ID   |
| Brendan C   | Protection against Bruteforce Attacks with NGFW                |
| Jack S      | Mitigating Routing Hijacking Attacks                           |
| Matthew D   | Mitigating Routing Hijacking Attacks                           |
| Chris N     | Protection against Reconnaissance and Scan Attacks             |
| Jack S      | Policy-based Forwarding  |
| Matthew D   | Policy-based Forwarding  |
| Keegan S    | An open-source library for computer networks and cybersecurity |
| Dakota M    | Distributed Denial of Service (DDoS) Protection                |
| Lauren W    | Protection against Bruteforce Attacks with NGFW                |
| Josue H     | Site to site VPN with NGFWs                                    |
| Brian N     | Distributed Denial of Service (DDoS) Protection                |

# Project Goals

## 2. Establish an undergraduate research program in cybersecurity

Participants include ROTC cadets (Navy, Army, Air Force), Veterans, and students from CS, IT, IS, Cyber Intelligence

| Name             | Project  |
|------------------|--|
| Kyle R           | Protection against Reconnaissance and Scan Attacks |
| Ryan T           | IPsec VPN with Routers                             |
| Nathan B         | Site to site VPN with NGFWs                        |
| Bryson L         | External Dynamic List                              |
| Ryan T           | IPsec VPN with Next Generation Firewalls           |
| Brad W           | Application ID                                     |
| Zach F           | External Dynamic List                              |
| Nathan L         | Geolocation and Geoblocking                        |
| Ty L             | Geolocation and Geoblocking                        |
| Gabriella P      | Access-control List in a Data Plane Switch         |
| Avery S          | Access-control List in a Data Plane Switch         |
| Dillon Barnhardt | Hardening Routing Protocols                        |



# Project Goals

## 2. Establish an undergraduate research program in cybersecurity

Participants include ROTC cadets (Navy, Army, Air Force), Veterans, and students from CS, IT, IS, Cyber Intelligence

| Name           | Project  |
|----------------|--|
| Samuel D       | Hardening Routing Protocols                            |
| Talha G        | Implementing VPN with Next-generation Firewalls        |
| Mark-Anthony B | Implementing VPN with Next-generation Firewalls        |
| Andrew C       | Preventing DoS and DDoS Attacks                        |
| Sam K          | NAT in a P4 Programmable Data Plane Switch             |
| Timothy D      | Preventing DoS and DDoS Attacks                        |
| Cameron M      | NAT in a P4 Programmable Data Plane Switch             |
| Tucker B       | Preventing Brute-force attacks using Custom Signatures |
| David Williams | Preventing Brute-force attacks using Custom Signatures |

# Project Goals

## 2. Establish an undergraduate research program in cybersecurity

Participants include ROTC cadets (Navy, Army, Air Force), Veterans, and students from CS, IT, IS, Cyber Intelligence

Chris Ngo



Jack Sadle



Brendan Curran



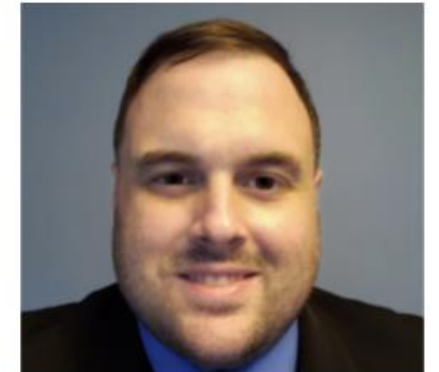
Tim Dao



Christian Tsirlis



Ryan Tallent



# Project Goals

## 2. Establish an undergraduate research program in cybersecurity

Participants include ROTC cadets (Navy, Army, Air Force), Veterans, and students from CS, IT, IS, Cyber Intelligence

Dakota  
McDaniels



David  
Williams



Brian  
Nelson



Keegan  
Sprankle



Bryson  
Livingston



Zach  
Fowler



# Project Goals

## 2. Establish an undergraduate research program in cybersecurity

Participants include ROTC cadets (Navy, Army, Air Force), Veterans, and students from CS, IT, IS, Cyber Intelligence

Josue  
Hernandez



Ty Love-  
Baker



Nate  
Bohmer



Nathan  
Long



Kyle  
Radzak



Lauren  
Waddell





# Project Goals

## 2. Establish an undergraduate research program in cybersecurity

Participants include ROTC cadets (Navy, Army, Air Force), Veterans, and students from CS, IT, IS, Cyber Intelligence

Brad Wilson



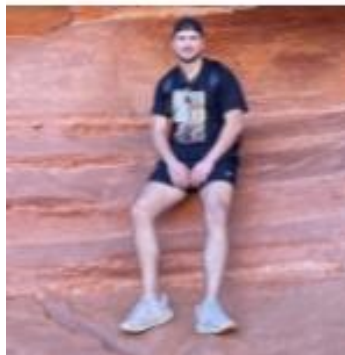
Matt Driver



Gabriella Pinto



Samuel Kelley



Dillon Barnhardt



Avery Schiro



# Project Goals

## 2. Establish an undergraduate research program in cybersecurity

Participants include ROTC cadets (Navy, Army, Air Force), Veterans, and students from CS, IT, IS, Cyber Intelligence

### Jack Sadle, ROTC

“During my semesters conducting research under ONR, I learned many valuable skills that would help me improve my chances at becoming a Cyber Operations Officer in the United States Army. The skills I learned during this period carried over into internships with 3rd Special Forces Group Cyber Effects Cell, as well as the Army Cyber Institute at West Point. Understanding the vulnerabilities with routing protocols greatly improved my value as a member of a research team examining malware and phishing attacks...”

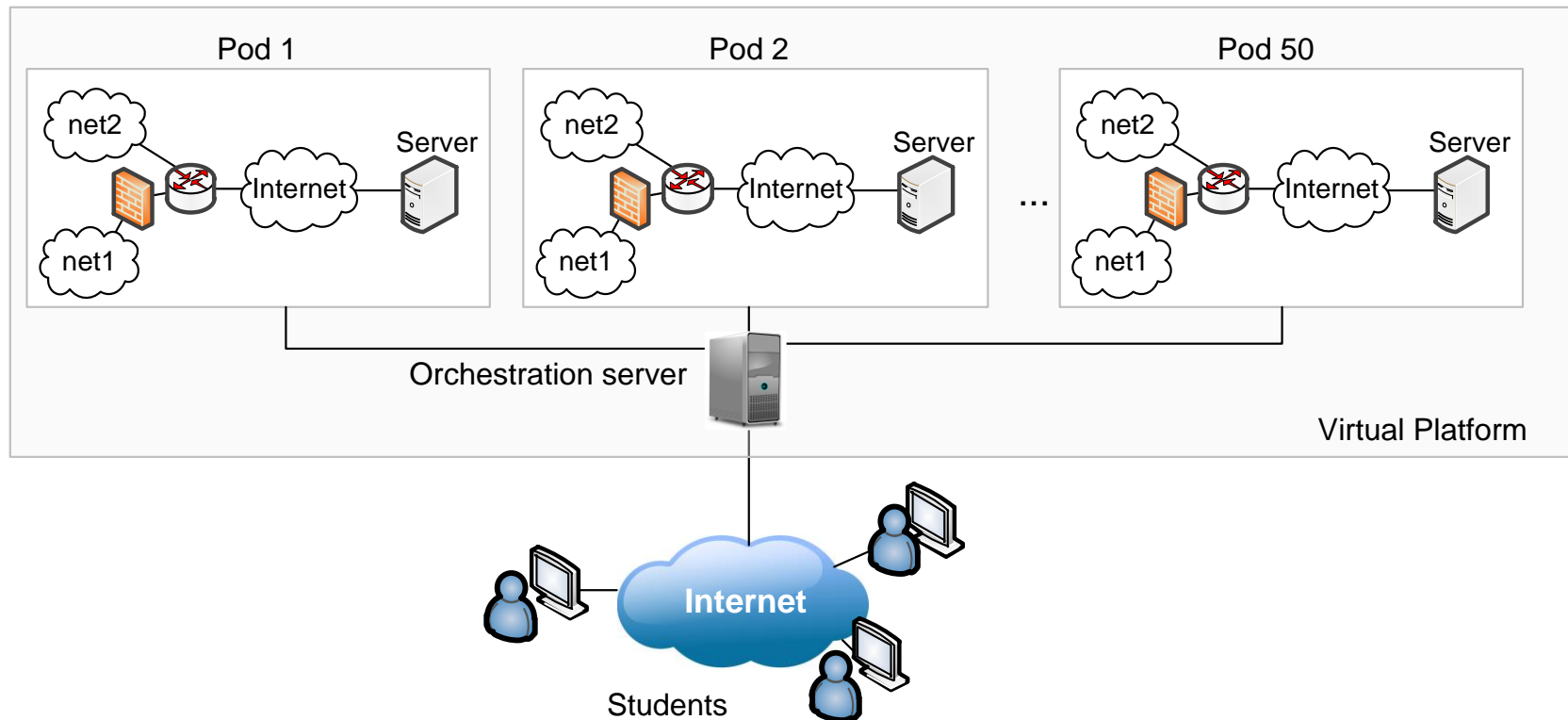
Currently senior student, employed with UofSC’s IT and at the 359th Theater Tactical Signal Brigade, Headquarters Company.

| Name            | Position                                  |
|-----------------|---|
| Ty Love-Baker   | 2nd Lt. at United States Marine Corps, DC |
| Dakota McDaniel | Information Security Analyst at Lowe's    |
| Lauren Waddell  | IT Specialist, SC Department of Insurance |
| Josue Hernandez | Technical Solution Specialist at IBM      |
| Kyle Radzak     | IT Specialist at Lowe's Companies         |
| Nathan Bohmer   | Project Coordinator at Black Box Networks |
| Brad Wilson     | Savannah River National Lab               |
| Zach Fowler     | IT Specialist at Blue Cross Blue Shield   |
| Nathan Long     | Technology Analyst at AIG                 |

⋮

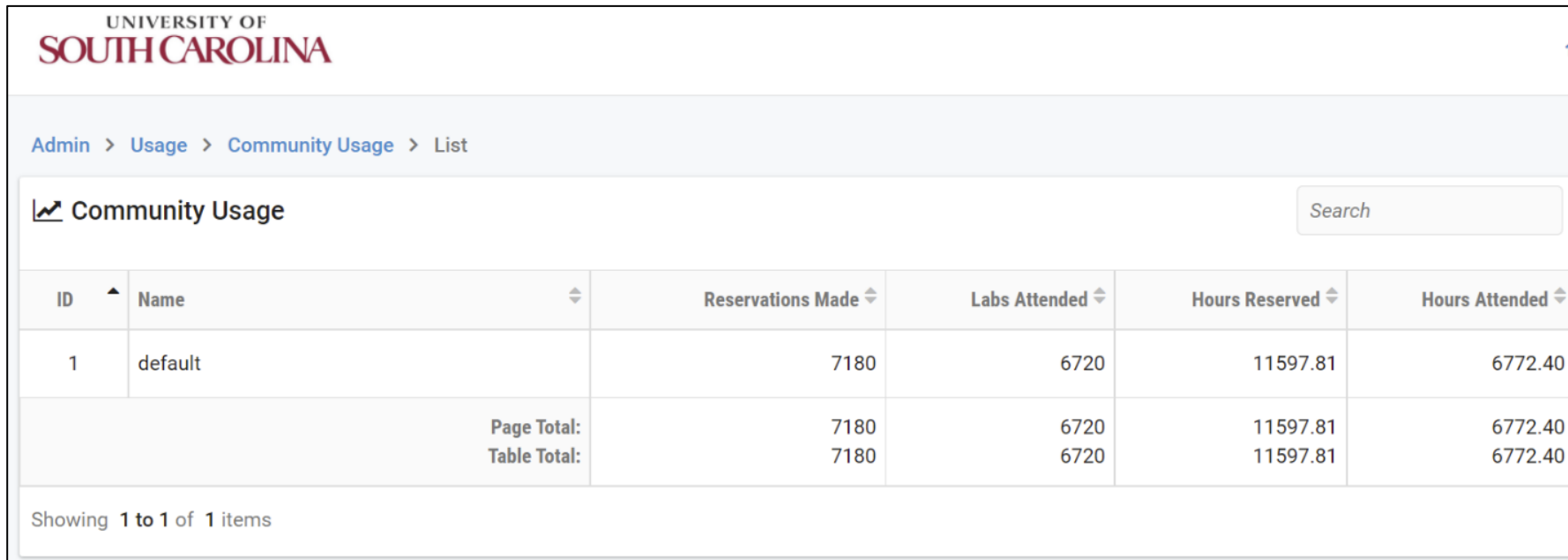
# Project Goals

## 3. Deploy virtual equipment pods on a virtual platform



# Project Goals

## 3. Deploy virtual equipment pods on a virtual platform



The screenshot shows a web interface for the University of South Carolina. At the top left is the university logo. Below it is a breadcrumb trail: Admin > Usage > Community Usage > List. The main heading is 'Community Usage' with a search bar to its right. Below the heading is a table with columns: ID, Name, Reservations Made, Labs Attended, Hours Reserved, and Hours Attended. The table contains one data row for ID 1, Name 'default', with 7180 reservations, 6720 labs attended, 11597.81 hours reserved, and 6772.40 hours attended. Below the table are summary rows for 'Page Total' and 'Table Total'. At the bottom, it says 'Showing 1 to 1 of 1 items'.

| ID           | Name    | Reservations Made | Labs Attended | Hours Reserved | Hours Attended |
|--------------|---------|-------------------|---------------|----------------|----------------|
| 1            | default | 7180              | 6720          | 11597.81       | 6772.40        |
| Page Total:  |         | 7180              | 6720          | 11597.81       | 6772.40        |
| Table Total: |         | 7180              | 6720          | 11597.81       | 6772.40        |

Showing 1 to 1 of 1 items

Use of the platform by USC students, 2021



# Project Goals

4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation

Program incorporates preparation for DoD's approved baseline credentials for Information Assurance Technical (IAT) positions, Cybersecurity Service Provider (CSSP) Analyst, and CSSP Incident Responder<sup>1</sup>

Cybersecurity courses with content for DoD's Approved 8750 baseline certifications

| Course                     | IAT 1-2 | CSSP Analyst | CSSP Incident Responder | Security Plus | NICE Framework Objectives |
|----------------------------|---------|--------------|-------------------------|---------------|---------------------------|
| Intro to Computer Security |         |              |                         | ✓             | ✓                         |
| Cybersecurity Operations   |         | ✓            | ✓                       |               | ✓                         |
| Intro to Networks          | ✓       | ✓            | ✓                       |               | ✓                         |
| IT Security for Managers   |         |              |                         | ✓             | ✓                         |
| Advanced Networks          | ✓       | ✓            | ✓                       |               | ✓                         |

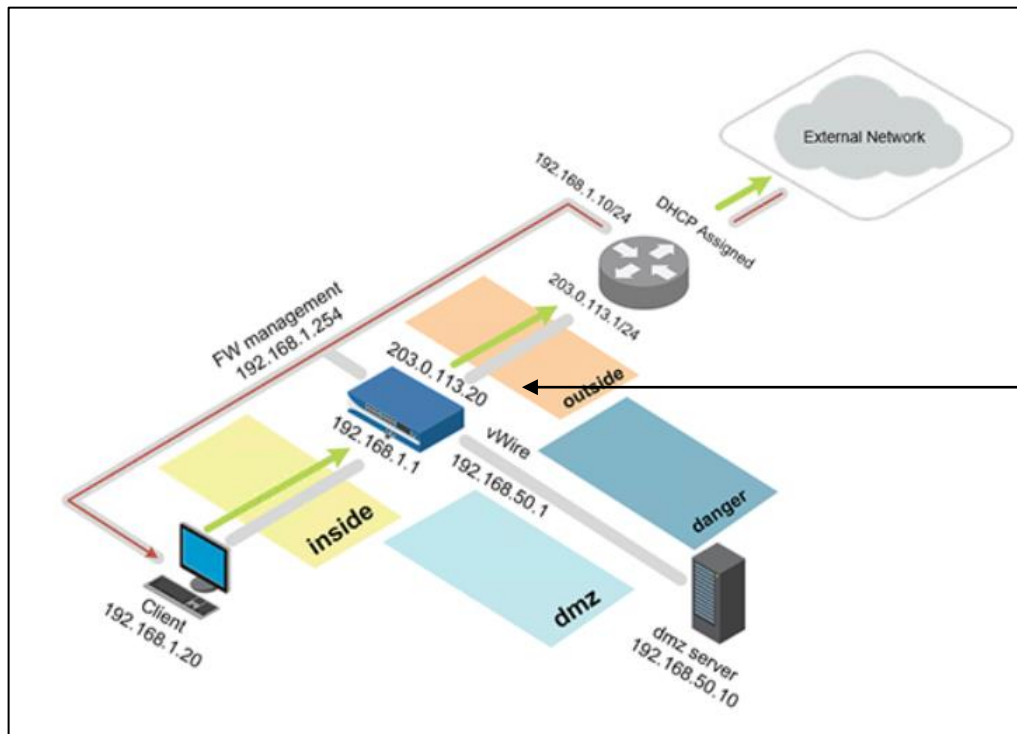
NICE: National Initiative for Cybersecurity Education

<sup>1</sup>Department of Defense (DoD) Cyber Workforce Management Program Website. <https://tinyurl.com/55t7sdnm>

# Project Goals

- Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation

Industry partners enrich the academic curriculum and undergraduate research experience with their tools and platforms: Palo Alto Networks, Cisco Systems, VMware, Intel

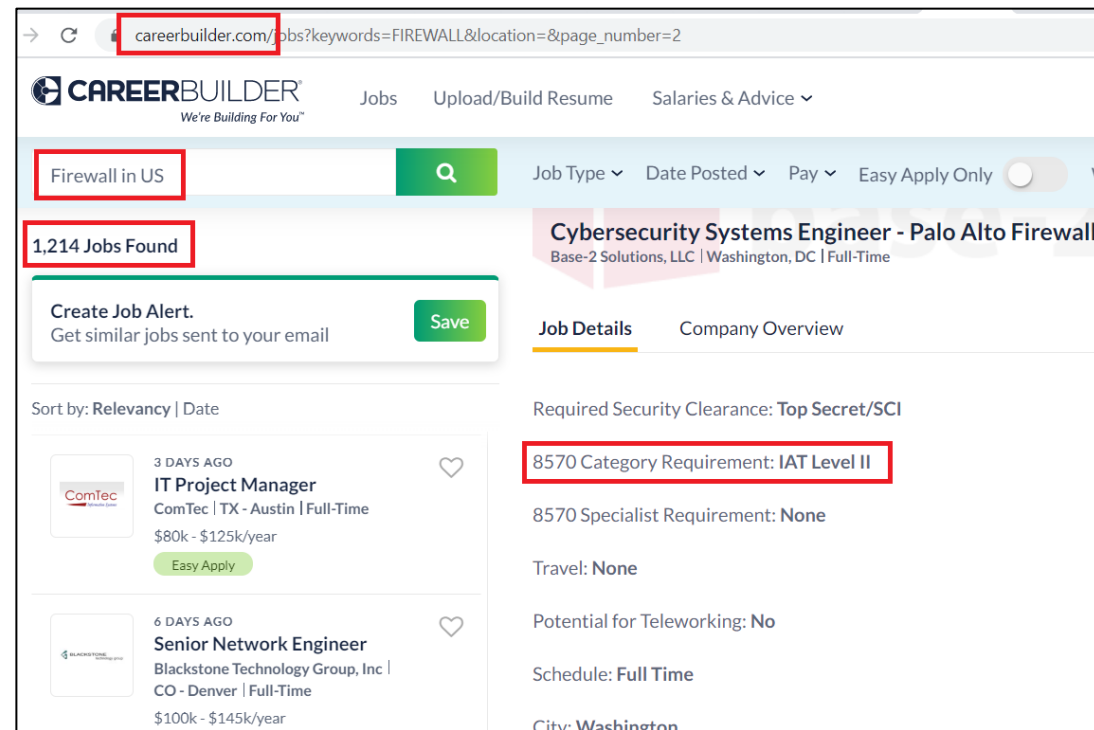
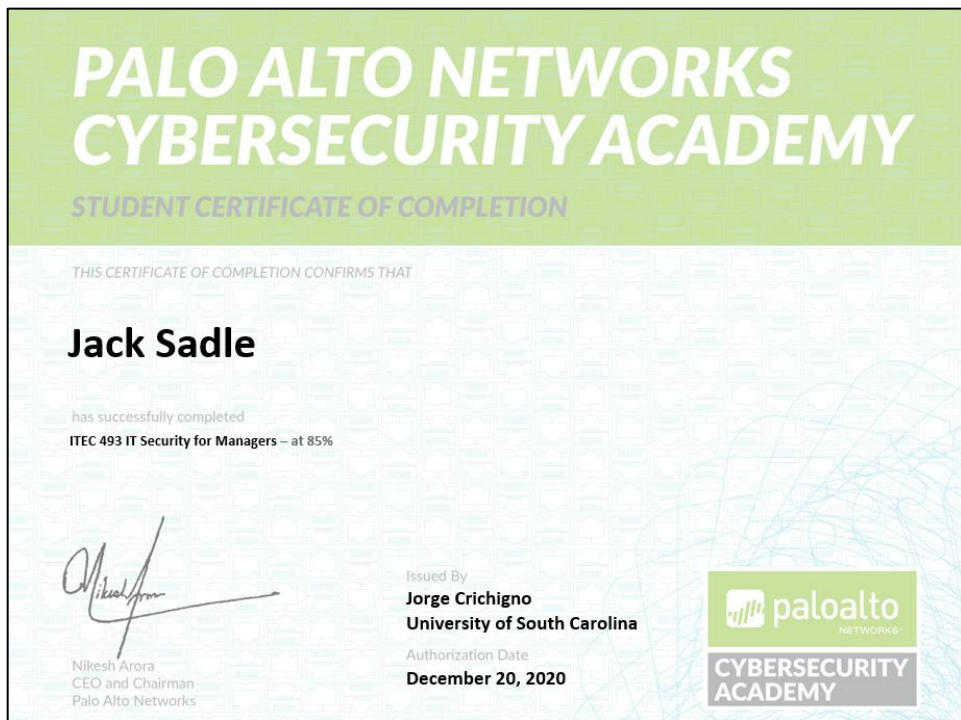


Next-generation Firewall Virtual Machine + licenses

# Project Goals

4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation

Industry partners enrich the academic curriculum and undergraduate research experience with their tools and platforms: Palo Alto Networks, Cisco Systems, VMware, Intel



Job search

# Project Goals

---

## 4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation

Industry partners enrich the academic curriculum and undergraduate research experience with their tools and platforms:  
Palo Alto Networks, Cisco Systems, VMware, Intel

Two examples of employment categories:

- Demand of certificates for Information Security Analyst is over 95% (345,000 job listings studied in<sup>1</sup>)
- Demand of certificates for Computer Network Architect is over 52% (38,000 job listings studied in<sup>1</sup>)

1. M. Tannian, W. Coston, “The Role of Professional Certifications in Computer Occupations,” Communications of the ACM, Vol. 64, No. 10, October 2021.

# Project Goals

---

## 4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation

Platform and material are available to other organizations

- Lawrence Berkeley National Lab
- SANS institute (“girlsgocyber”)
- Multiple higher-ed institutions
- International Networks at Indiana
- Fort Gordon (~2 cyber courses per semester)
- Texas’ Lonestart Education and Research
- Great Plains Network
- New York State Education and Research Network
- U.S. Army Cyber Center of Excellence (CCoE) (Signal School)

# Project Goals

## 4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation

Industry partners enrich the academic curriculum and undergraduate research experience with their tools and platforms: Palo Alto Networks, Cisco Systems, VMware, Intel

### Offloading Media Traffic to Programmable Data Plane Switches

Elie F. Kfoury\*, Jorge Crichigno\*, Elias Bou-Harb†, Vladimir Gurevich‡

\*Integrated Information Technology, University of South Carolina, USA

†The Cyber Center For Security and Analytics, University of Texas at San Antonio, USA

‡Barefoot Networks, an Intel Company, USA

**Abstract**—According to estimations, approximately 80% of Internet traffic represents media traffic. Much of it is generated by end users communicating with each other (e.g., voice, video sessions). A key element that permits the communication of users that may be behind Network Address Translation (NAT) is the relay server.

This paper presents a scheme for offloading media traffic from relay servers to programmable switches. The proposed scheme relies on the capability of a P4 switch with a customized parser to de-encapsulate and process packets carrying media traffic. The switch then applies multiple switch actions over the packets. As these actions are simple and collectively emulate a relay server, the scheme is capable of moving relay functionality to the data plane operating at terabits per second. Performance

results [8] reveal that CGN has a widespread adoption and that over half of operators have deployed or will deploy CGN. NAT introduces issues such as violation of the end-to-end principle, scalability and reliability concerns, and traversal of end-to-end sessions. The latter is a problem that severely affects media traffic. For example, for an end user to be reachable for an end-to-end media session (voice, video), the user must wait and accept incoming connections at a well-known port. With NAT, the user is not reachable because it is assigned a private IP address. Furthermore, port numbers are also allocated dynamically. Moreover, these dynamic allocations

- Improving system's performance w/ NG switches
- Offloading computational tasks to network switches
- Agreement with Intel (chips, software development environment)

Application example: media (voice) relay server

|                 | Programmable Switch                | General-purpose CPU              |
|-----------------|------------------------------------|----------------------------------|
| <b>Cost</b>     | \$6,000                            | \$ 10,000 - 25,000               |
| <b>Capacity</b> | ~35,000,000 connections per switch | ~500 connections per core        |
| <b>Latency</b>  | 400 nanoseconds                    | Tens to hundreds of milliseconds |

# Next Steps - FOA N00014-22-S-F003

---

- Leverage the technologies and facilities developed at USC, to strengthen the education and research capacity of regional communities
- Implement an inter-institutional undergraduate research program
  - 40 students trained on cybersecurity from the previous FOA are from USC
  - Extend program to partner institutions to address diversity-equity-inclusion: HBCUs, HSIs, and tribal colleges
- Expand the collaboration with industry and agencies, to continue adding tools, professional development opportunities, access to credentials, and internships
  - Increase the number of professionals with high-demand skills / credentials for the workforce, and for military occupation specialties (MOS)