I. INTRODUCTION

A. Overall security processes with particular emphasis on hands-on skills in the following areas: security policy design and management; security technologies, products, and solutions: secure router design, installation, configuration, and maintenance: and AAA and VPN implementation using routers and firewalls. The goal of this course is to educate the student about network security threats and technologies and the implementation of these technologies to mitigate threats to networks. Emphasis is placed on the areas of design, planning, implementation, operation and troubleshooting.

B. This course is occupationally related and serves as preparation for careers in computer internetworking and network security administration.

C. The delivery method of this course may be traditional lecture/lab, blended lecture/lab, or online.

D. Prerequisites: Departmental Approval.

II. LEARNING OUTCOMES

Upon successful completion of this course, CCNA Security, the student will be able to:
A. Explain network threats, mitigation techniques, and the basics of securing a network. (C7, C8, C9, C15, C18, F1, F9, F10, F13)
B. Secure administrative access on Cisco routers using AAA. (C5, C7, C8, C9, C16, C18, F1, F9, F13)
C. Implement firewall technologies to secure the network perimeter. (C8, C9, C15, C18, F1, F9, F10, F13)
D. Configure IPS to mitigate attacks on the network. (C1, C5, C7, C8, C9, C16, C18, F1, F9, F10, F13)
E. Implement endpoint and Layer 2 security features. (C5, C7, C8, C9, C15, C18, F1, F9, F10, F13)
F. Implement secure virtual private networks. (C1, C7, C8, C9, C16, C18, F9, F10, F13)
III. INSTRUCTIONAL MATERIALS

The instructional materials identified for this course are viewable through www.ctcd.edu/books

IV. COURSE REQUIREMENTS

A. Attend both lecture and lab or in the case of online delivery, be actively engaged in Blackboard and maintain constant progress.

B. Be prepared to participate in discussion, team projects/assignments and take unannounced assessments relating to the lecture materials.

C. Complete all exams/assessments.

D. Submit all assignments on time.

V. ASSESSMENTS

A. Student content mastery will be evaluated in the following areas:
   • Assessments (midterm exam, quizzes, projects, etc.)
   • Final Assessment (final exam and/or semester project, participation)

B. Scheduled and unscheduled assessments will be given at the discretion of the instructor.

C. Exams/assessments may be composed of both subjective and objective questions plus computer output.

D. A student must take all exams/assessments. No make-up exams/assessments will be given. Both online and on campus students who know in advance that they will be absent due to school sponsored trips, military duty or orders, or any other valid reason, must arrange to take an early exam/assessment. Unexpected absences due to illness or other extenuating circumstances will require the student to see the instructor about make-up work in lieu of the missed exam/assessment.

E. Students with unexcused absences will be given a zero for each missed assignment.
VI. SEMESTER GRADE COMPUTATIONS

<table>
<thead>
<tr>
<th>Course Requirements</th>
<th>Points</th>
<th></th>
<th>Points</th>
<th>Grade</th>
<th>Quality Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments</td>
<td>300</td>
<td></td>
<td>900-1000</td>
<td>A-Superior</td>
<td>4</td>
</tr>
<tr>
<td>Assessments</td>
<td>300</td>
<td></td>
<td>800-899</td>
<td>B-Above Average</td>
<td>3</td>
</tr>
<tr>
<td>Final Assessment</td>
<td>400</td>
<td></td>
<td>700-799</td>
<td>C-Average</td>
<td>2</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1000</td>
<td></td>
<td>600-699</td>
<td>D – Passing but Unsatisfactory</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0-599</td>
<td>F-Failure</td>
<td>0</td>
</tr>
</tbody>
</table>

VII. NOTES AND ADDITIONAL INSTRUCTIONS FROM THE INSTRUCTOR

A. **Course Withdrawal:** It is the student’s responsibility to officially withdraw from a course if circumstances prevent attendance. Any student who desires to, or must, officially withdraw from a course after the first scheduled class meeting must file a Central Texas College Application for Withdrawal (CTC Form 59). The student must sign the withdrawal form.

CTC Form 59 will be accepted at any time prior to Friday of the 12th week of classes during the 16-week fall and spring semesters. The deadline for sessions of other lengths is:

- 10-week session: Friday of the 8th week
- 8-week session: Friday of the 6th week
- 5-week session: Friday of the 4th week

The equivalent date (75% of the semester) will be used for sessions of other lengths. The specific last day to withdraw is published each semester in the Schedule Bulletin.

For non-GoArmyEd active military students, the effective date of withdrawal is the filing date with the Education Center. For all other students, the effective date of withdrawal is the date that the withdrawal application is received by the Central Texas College representative.

Students who used financial aid, military tuition assistance, VA benefits, or other non-personal funds may be required to repay tuition and fees to the funding agency. For specific repayment requirements, contact the Office of Student Financial Aid or Veterans Services Office before withdrawing. Military tuition assistance students should visit their military Education Center or Navy College Office.

A student who officially withdraws will be awarded the grade of “W” provided the student’s attendance and academic performance are satisfactory at the time of official withdrawal. Students must file a withdrawal application with the College before they may be considered for withdrawal.
A student may not withdraw from a class for which the instructor has previously issued a grade of “F,” “FI,” “FN,” “IP,” or “XN.”

B. Instructor Initiated Withdrawals: Faculty are authorized to withdraw students who are not making satisfactory course progress to include failure to meet College attendance requirements as outlined in the section of the Catalog entitled “Satisfactory Progress Standards.” The instructor will assign the appropriate grade on CTC Form 59 for submission to the registrar.

Students enrolled in distance learning courses are expected to maintain constant progress throughout the course. Failure to do so may result in the student being administratively withdrawn by the instructor.

Students who have not attended class by the 12th class day of a 16-week course or the 6th class day of an 8-week term may be administratively withdrawn by the instructor with a grade of "W." Students may be administratively withdrawn from any class when their absences reach a total equal to 12.5% of the class hours for the course; and in the opinion of the instructor, the student cannot satisfactorily complete the course. An example: Students attending a 48-hour class during an 8-week period normally meet 180 minutes each session for 16 sessions. Those students accumulating two (2) unexcused absences are subject to Administrative Withdrawal since the total unexcused absences equal 12.5% of class hours for the course. Those students attending a 48 hour class during a 16-week period normally meet 90 minutes each session for 32 sessions. Those students accumulating four (4) unexcused absences are subject to Administrative Withdrawal since the total unexcused absences equals 12.5% of class hours for the course. In a distance learning course the last date of attendance is the last activity by the student in the course.

C. Administrative Withdrawal: A student may be administratively withdrawn by a designated member of the administrative staff of the College when the student has been placed on Academic Suspension or Disciplinary Suspension; the student has an outstanding financial obligation owed to the college; or the student registered for a course without the required prerequisite or departmental permission.

The College is under no obligation to refund tuition and fees, or other costs associated with an administrative or instructor initiated withdrawal.

D. Incomplete Grade: The College catalog states, “An incomplete grade may be given in those cases where the student has completed the majority of the coursework but, because of personal illness, death in the immediate family, or military orders, the student is unable to complete the requirements for a course...” Prior approval from the instructor is required before the grade of “IP” for Incomplete is recorded.
E. **Cell Phones and Pagers:** Students will silence cell phones and mobile devices while in the classroom or lab.

F. **Americans with Disabilities Act (ADA):** Disability Support Services provide services to students who have appropriate documentation of a disability. Students requiring accommodations for class are responsible for contacting the Office of Disability Support Services (DSS) located on the central campus. This service is available to all students, regardless of location. Review the website at [www.ctcd.edu/disability-support](http://www.ctcd.edu/disability-support) for further information. Reasonable accommodations will be given in accordance with the federal and state laws through the DSS office.

G. **Instructor Discretion:** The instructor reserves the right of final decision in course requirements and may make changes to the course outline and/or assignments as needed.

H. ** Civility:** Individuals are expected to be aware of what a constructive educational experience is and be respectful of those participating in a learning environment. Failure to do so can result in disciplinary action up to and including expulsion.

I. **Degree Progression:** Students who receive a grade of “D” are advised not to enroll in the next course for which this course was a prerequisite.

J. **Failing Grade:** The grade of “F” or “FN” will be given for academic failure, non-attendance or scholastic dishonesty.

K. **Scholastic Honesty:** All students are expected to maintain the highest standards of scholastic honesty in the preparation of all course work and during examinations. The college policy on scholastic honesty, including definitions on plagiarism, collusion, and cheating can be found at the following URL: [http://online.ctcd.edu/plagiarism.cfm](http://online.ctcd.edu/plagiarism.cfm)
VIII. COURSE OUTLINE

A. Lesson One: Modern Network Security Threats

1. Learning Outcomes: Upon successful completion of this lesson the student will be able to:
   a. Identify threats to networks
   b. Discuss the role of network security organizations
   c. Describe best practices in creating network security policies
   d. Describe tools available for threat mitigation

2. Learning Activities:
   a. Research and discuss the topics of the Lesson in class and in an online collaborative discussion forum (C7, C8, C9, C15, C18, F1, F9, F10, F13)
   b. Perform skills and functions in the section (C1, C5, C7, C8, C9, C16, C18, F1, F9, F10, F13)

3. Unit Outline:
   a. Fundamental Principles of a Secure Network
   b. Viruses, Worms, and Trojan Horses
   c. Attack Methodologies

B. Lesson Two: Securing Network Devices

1. Learning Outcomes: Upon successful completion of this lesson the student will be able to:
   a. Identify methods of hardening network devices
   b. Select methods based on network device type
   c. Implement network device hardening methods
   d. Describe tools available for threat mitigation

2. Learning Activities:
   a. Research and discuss the topics of the Lesson in class and in an online collaborative discussion forum (C7, C8, C9, C15, C18, F1, F9, F10, F13)
   b. Perform skills and functions in the section (C1, C5, C7, C8, C9, C16, C18, F1, F9, F10, F13)

3. Unit Outline:
   a. Securing Device Access
   b. Assigning Administrative Roles
   c. Monitoring and Managing Devices
   d. Using Automated Security Features
C. **Chapter Three: Authentication, Authorization, and Accounting**

1. **Learning Outcomes:** Upon successful completion of this lesson, the student will be able to:
   a. Identify Authentication, Authorization and Accounting (AAA) methods of securing network devices.
   b. Select AAA methods based on network device type.
   c. Implement network AAA methods.

2. **Learning Activities:**
   a. Research and discuss the topics of the Lesson in class and in an online collaborative discussion forum (C7, C8, C9, C15, C18, F1, F9, F10, F13)
   b. Perform skills and functions in the section (C1, C5, C7, C8, C9, C16, C18, F1, F9, F10, F13)

3. **Unit Outline:**
   a. Introduction
   b. Purpose of AAA
   c. Local AAA Authentication
   d. Server-Based AAA
   e. Server-Based AAA Authorization and Accounting

D. **Chapter Four: Implementing Firewall Technologies**

1. **Learning Outcomes:** Upon successful completion of this lesson, the student will be able to:
   a. Identify types of firewalls.
   b. Select a firewall based on network device type.
   c. Implement firewall mechanisms.

2. **Learning Activities:**
   a. Research and discuss the topics of the Lesson in class and in an online collaborative discussion forum (C7, C8, C9, C15, C18, F1, F9, F10, F13)
   b. Perform skills and functions in the section (C1, C5, C7, C8, C9, C16, C18, F1, F9, F10, F13)

3. **Unit Outline:**
   a. Introduction
   b. Access Control Lists
   c. Firewall Technologies
   d. Context-Based Access Control
   e. Zone-Based Policy Firewall
E. Chapter Five: Implementing Intrusion Prevention

1. Learning Outcomes: Upon successful completion of this lesson, the student will be able to:
   a. Identify types of intrusion prevention systems (IPS) and intrusion detection systems (IDS).
   b. Select a IPS and IDS system based on network threats.
   c. Implement IPS and IDS mechanisms.

2. Learning Activities:
   a. Research and discuss the topics of the Lesson in class and in an online collaborative discussion forum (C7, C8, C9, C15, C18, F1, F9, F10, F13)
   b. Perform skills and functions in the section (C1, C5, C7, C8, C9, C16, C18, F1, F9, F10, F13)

3. Unit Outline:
   a. Introduction
   b. IPS Technologies
   c. IPS Signatures
   d. Implementing IPS
   e. Verify and Monitor IPS

F. Chapter Six: Securing the Local Area Network

1. Learning Outcomes: Upon successful completion of this lesson, the student will be able to:
   a. Identify types of endpoint security applications.
   b. Select endpoint security applications based on network device type.
   c. Implement security applications on network devices.

2. Learning Activities:
   a. Research and discuss the topics of the Lesson in class and in an online collaborative discussion forum (C7, C8, C9, C15, C18, F1, F9, F10, F13)
   b. Perform skills and functions in the section (C1, C5, C7, C8, C9, C16, C18, F1, F9, F10, F13)

3. Unit Outline:
   a. Introduction
   b. Endpoint Security
   c. Layer 2 Security Considerations
   d. Configuring Layer 2 Security
   e. Wireless, VoIP, and SAN Security
G. Chapter Seven: Cryptographic Systems

1. Learning Outcomes: Upon successful completion of this lesson, the student will be able to:
   a. Describe protocols and algorithms used with cryptographic systems.
   b. Select a cryptographic system based on network traffic type and security need.
   c. Implement a cryptographic system on network devices and end user computers.

2. Learning Activities:
   a. Research and discuss the topics of the Lesson in class and in an online collaborative discussion forum (C7, C8, C9, C15, C18, F1, F9, F10, F13)
   b. Perform skills and functions in the section (C1, C5, C7, C8, C9, C16, C18, F1, F9, F10, F13)

3. Unit Outline:
   a. Introduction
   b. Cryptographic Services
   c. Confidentiality
   d. Public Key Cryptography

H. Chapter Eight: Implementing Virtual Private Networks

1. Learning Outcomes: Upon successful completion of this lesson, the student will be able to:
   a. Identify components of a virtual private network (VPN).
   b. Select VPN components based on network traffic type and security need.
   c. Implement a VPN on network devices and end user computers.

2. Learning Activities:
   a. Research and discuss the topics of the Lesson in class and in an online collaborative discussion forum (C7, C8, C9, C15, C18, F1, F9, F10, F13)
   b. Perform skills and functions in the section (C1, C5, C7, C8, C9, C16, C18, F1, F9, F10, F13)

3. Unit Outline:
   a. Introduction
   b. VPNs
   c. GRE VPNs
   d. IPsec VPN Components and Operation
   e. Implementing Site-to-Site IPsec VPNs with CLI
   f. Implementing Site-to-Site IPsec VPNs with SDM
   g. Implementing Remote-Access VPNs
I. Chapter Nine: Managing a Secure Network

1. Learning Outcomes: Upon successful completion of this lesson, the student will be able to:
   a. Identify components of a comprehensive security plan and policies.
   b. Select a security plan and policy components based on organizational security needs.
   c. Create security plan and policies.
   d. Implement security plan and policies.

2. Learning Activities:
   a. Research and discuss the topics of the Lesson in class and in an online collaborative discussion forum (C7, C8, C9, C15, C18, F1, F9, F10, F13)
   b. Perform skills and functions in the section (C1, C5, C7, C8, C9, C16, C18, F1, F9, F10, F13)

3. Unit Outline:
   a. Introduction
   b. Principles of Secure Network Design
   c. Cisco Self-Defending Network
   d. Operations Security
   e. Network Security Testing
   f. Business Continuity Planning and Disaster Recovery
   g. System Development Life Cycle
   h. Developing a Comprehensive Security Policy