UNIVERSITY OF THE FRASER VALLEY

ORIGINAL COURSE IMPLEMENTATION DATE: January 2005
REVISED COURSE IMPLEMENTATION DATE: January 2027
COURSE TO BE REVIEWED (six years after UEC approval)**:** March 2032
Course outline form version: 28/10/2022

OFFICIAL UNDERGRADUATE COURSE OUTLINE FORM

Note: The University reserves the right to amend course outlines as needed without notice.

Course Code and Number: CIS 321	**Number of Credits:** 4 Course credit policy (105)
Course Full Title: Networking Security Architecture **Course Short Title:** Network Security Architecture	
Faculty: Faculty of Business and Computing	**Department (or program if no department):** School of Computing

Calendar Description:

This course focuses on network security architectures, procedures, and processes. Practical hands-on skill development is provided in security system technologies, security policy design, firewall design and implementation, router security architectures, authentication and authorization systems, Intrusion detection, and VPNs. The course integrates Indigenous knowledge systems, emphasizing relationality to help students view network security threats as both technical issues and part of a broader interconnected system.

Prerequisites (or NONE):	CIS 221 and CIS 292.
Corequisites (if applicable, or NONE):	None.
Pre/corequisites (if applicable, or NONE):	None.

Antirequisite Courses *(Cannot be taken for additional credit.)*

Former course code/number:

Cross-listed with:

Equivalent course(s):

(If offered in the previous five years, antirequisite course(s) will be included in the calendar description as a note that students with credit for the antirequisite course(s) cannot take this course for further credit.)

Typical Structure of Instructional Hours

Lecture/seminar	45
Supervised laboratory hours (design lab)	15
	15
Total hours	**60**

Scheduled Laboratory Hours

Labs to be scheduled independent of lecture hours: ☒ No ☐ Yes

Course Details

Special Topics course: **No**
(If yes, the course will be offered under different letter designations representing different topics.)

Directed Study course: **No**
(See policy 207 for more information.)

Grading System: **Letter grades**

Delivery Mode: **May be offered in multiple delivery modes**

Expected frequency: **Every other year**

Maximum enrolment (for information only)**: 35**

Prior Learning Assessment and Recognition (PLAR)

PLAR is available for this course.

Transfer Credit *(See bctransferguide.ca.)*

Transfer credit already exists: **No**

Submit outline for (re)articulation: **No**
(If yes, fill in transfer credit form.)

Department approval	**Date of meeting:**	April 2025
Faculty Council approval	**Date of meeting:**	September 12, 2025
Undergraduate Education Committee (UEC) approval	**Date of meeting:**	March 27, 2026

Learning Outcomes

Upon successful completion of this course, students will be able to:

1. Identify network threats, attacks, and endpoint vulnerabilities, along with mitigation tools and procedures.
2. Configure advanced firewall installations and other security measures to mitigate network attacks.
3. Implement authentication, authorization and accounting (AAA) as well as an intrusion detection system on routers and firewalls.
4. Implement virtual private networks (VPNs).
5. Design secure networks.
6. Apply public key infrastructure to ensure data confidentiality, integrity, and authentication.
7. Integrate Indigenous knowledge systems that emphasize relationality — the interconnectedness of all things — to support holistic network security approaches.

Recommended Evaluation Methods and Weighting *(Evaluation should align to learning outcomes.)*

Final exam:	30%	Quizzes/tests:	20%	Assignments:	20%
Lab work:	30%				

Details:

NOTE: The following sections may vary by instructor. Please see the course syllabus available from the instructor.

Typical Instructional Methods *(Guest lecturers, presentations, online instruction, field trips, etc.)*

Lectures and hands-on laboratory-based exercises and case studies.

Texts and Resource Materials [Textbook selection varies by instructor. Examples for this course might be:]

	Type	Author or description	Title and publication/access details	Year
1.	Textbook	Cisco	CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide (2nd Edition)	2023
2.	Textbook	Joseph Migga Kizza	Guide to Computer Network Security (6th Edition)	2024
3.	Textbook	Mark Ciampa	Security+ Guide to Network Security Fundamentals (7th Edition)	2021
4.	Journal	Lauren Tynan	What is relationality? Indigenous knowledges, practices and responsibilities with kin	2021
5.	Online resource		Various websites for reference material	

Required Additional Supplies and Materials *(Software, hardware, tools, specialized clothing, etc.)*

Lab book and Network Simulator Software such as Packet Tracer

Course Content and Topics *[Course content varies by instructor. An example of course content might be:]*

- Overview of network security and threats
- Mitigating threats and network security policies
- Securing switches and LAN access
- Device monitoring and management
- Basic integrity and authenticity
- Authentication, authorization, and accounting (AAA)
- Access control lists (ACLs)
- Firewall technologies
- Firewall configuration
- Endpoint security and layer 2 security considerations
- Cryptographic services
- Public key cryptography
- Virtual private networks (VPNs)
- Implement site-to-site IPsec VPNs
- Intrusion detection systems (IDS)
- Ip protocol security
- Network security testing
- Relational impacts of a cyber breach