CONESTOGA

Connect Life and Learning

Conestransfer

Onyeka Ofojetu Mmesooma – 9005016

Applied Computer Science & IT

SECU8010: Fundamentals of InfoSec

Course Instructor: Baljeet S. Bilkhu

TABLE OF CONTENTS

TASK 1

1.1 INTRODUCTION

Conestransfer Inc. is a fictitious financial technology company based in Toronto, with offices in Vancouver and Ottawa. We help people and businesses send and receive money quickly, safely, and at low cost. Using smart technology like AI, we make money transfers easier for everyone, especially immigrants, students, and small business owners. Our team of 150 skilled workers is focused on giving customers simple and secure ways to manage their money.

Our goal is to make financial services open to everyone. We keep our pricing clear, offer real-time transfers, and use efficient tools to stop fraud. People who have trouble using regular banks can trust us instead. We support money transfers within Canada and to other countries. We also follow Canadian rules like PIPEDA, FINTRAC, and OSFI to keep every transaction safe and legal (Akiode,2024). By integrating AI-driven fraud detection and end-to-end encryption, we ensure that every transaction meets the highest standards of confidentiality, integrity, and availability (CIA triad).

In the future, we want to grow across Canada and around the world. We plan to add new tools like multi-currency wallets and work with global payment networks. Our dream is to be the first choice for safe, fast, and affordable money transfers. By always improving and putting our customers first, we are changing how people move money, one step at a time.

1.2 COMPANY SIZE AND STRUCTURE

Conestransfer employs 150 full-time staff across six key divisions:

1. Executive Leadership (10 Employees)

- CEO, CTO, CFO(Chief Financial Officer), CCO (Chief Compliance Officer), CHRO (Chief HR Officer)
- 5 VPs: Product, Engineering, Security, Customer Experience, and Partnerships.

2. Technology & Development (50 Employees)

Split across Toronto (HQ), Vancouver (AI/ML), and Ottawa (Cloud Security)

Team	Size	Key Responsibilities
Cybersecurity	10	Implements CIA safeguards (AES-256 encryption, Zero Trust, Intrusion detection and prevention systems)
Software Engineer	15	Develops UI/UX and real-time payment APIs and handles software development.
AI/ML	10	Builds fraud detection models and AI Investment models.
Cloud DevOps	15	Manages Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) clouds.

3. Customer Operations (50 Employees)

- **24/7 Support (30)**: Bilingual (English/French) and Real-time fraud monitoring using (e.g., Confirmation of Payee).
- **KYC/Onboarding (10)**: Verifies identities for Anti-money laundering compliance.
- **Escalations (10)**: Handles disputes (e.g., intercepted Transfers).

4. Legal & Compliance (10 Employees)

- **Regulatory Affairs (7)**: Ensures compliance with FINTRAC (anti-money laundering).
- **Privacy Officers (3)**: Ensures PCI DSS Level 1 certification for data handling and PIPEDA data requests. (Akiode, 2024)

5. HR & Talent (10 Employees)

- **Recruiting (6)**: Hires Staff in different offices.
- **Training (4)**: Ensures all staff always have the necessary certificates, qualifications, and training.

6. Finance & Risk (20 Employees)

- **Treasury (10)**: Manages liquidity for all transactions.
- **Risk Analysts (10)**: Monitors annual payments.

1.3 OFFICE LOCATIONS

- **Toronto Headquarters (HQ)**
  The Toronto office houses our executive leadership team, core technology development, and mission-critical infrastructure. The facility contains data centers, the SOC team, the regulatory team, and the HR department.
- **Vancouver Office**
  Our Vancouver office serves as the AI/ML powerhouse and also contains most of the software engineers:
- **Ottawa Office**
  This office combines cloud operations (15 DevOps engineers) with a bilingual support center that handles interactive fraud cases.

1.4 PRODUCTS AND SERVICES

- **Peer-to-Peer Payments:** It allows biometric authentication (Face ID/Touch ID) and real-time transactions.
- **MicroInvest:** AI-Driven Investing.
- **Business Hub:** Small and medium businesses Banking Portal (Automated invoicing and payroll, Fraud detection via ML).

1.5 KEY ASSETS AND RISK PRIORITIZATION

Asset	Threats	CIA Priority	Likelihood (L)	Impact (I)	Risk Score (L×I)	Mitigation Strategies
Customer PII	Phishing, Insider Threats	Confidentiality	4	5	20 (High)	AES-256 encryption Role-based access controls Employee training
Transaction Servers	DDoS, Ransomware	Availability	3	5	15 (High)	Air-gapped backups

						Zero Trust Architecture DDoS protection
API Gateways	SQL Injection, API Abuse	All CIA	3	4	12 (Medium)	OAuth 2.0 authentication Rate limiting Regular pen testing
AI Algorithms	Model Poisoning	Integrity	2	3	6 (Low)	Code signing Model monitoring Sandbox testing

1.6 ASSET PROTECTION BASED ON RISK AND PRIORITY

Conestransfer protects its assets based on how important they are and the risks they face. Key areas are evaluated using the CIA triad (Confidentiality, Integrity, and Availability).

High Risk:

- **Customer PII:** Breaches can lead to fines over $100k and harm customers through identity theft. It should be protected using AES-256 encryption and role-based access.
- **Transaction Servers:** Downtime affects revenue and partners.
  It should be protected with air-gapped backups and Zero Trust Security.

Medium Risk:

- **APIs:** Vulnerable to attacks like SQL injection, which can cause data leaks or service outages.
  It should be protected using OAuth and rate limiting.

Low Risk:

- **AI Algorithms:** This could be tampered with bypassing fraud detection. Risk is low but managed using code signing and model monitoring.

TASK 2

2.1 NETWORK TOPOLOGY OVERVIEW

The Cisco Packet Tracer simulation models a hybrid hub topology with Toronto as the main hub, connected to Vancouver and Ottawa via IPSec VPN tunnels (see *Figure 1*).

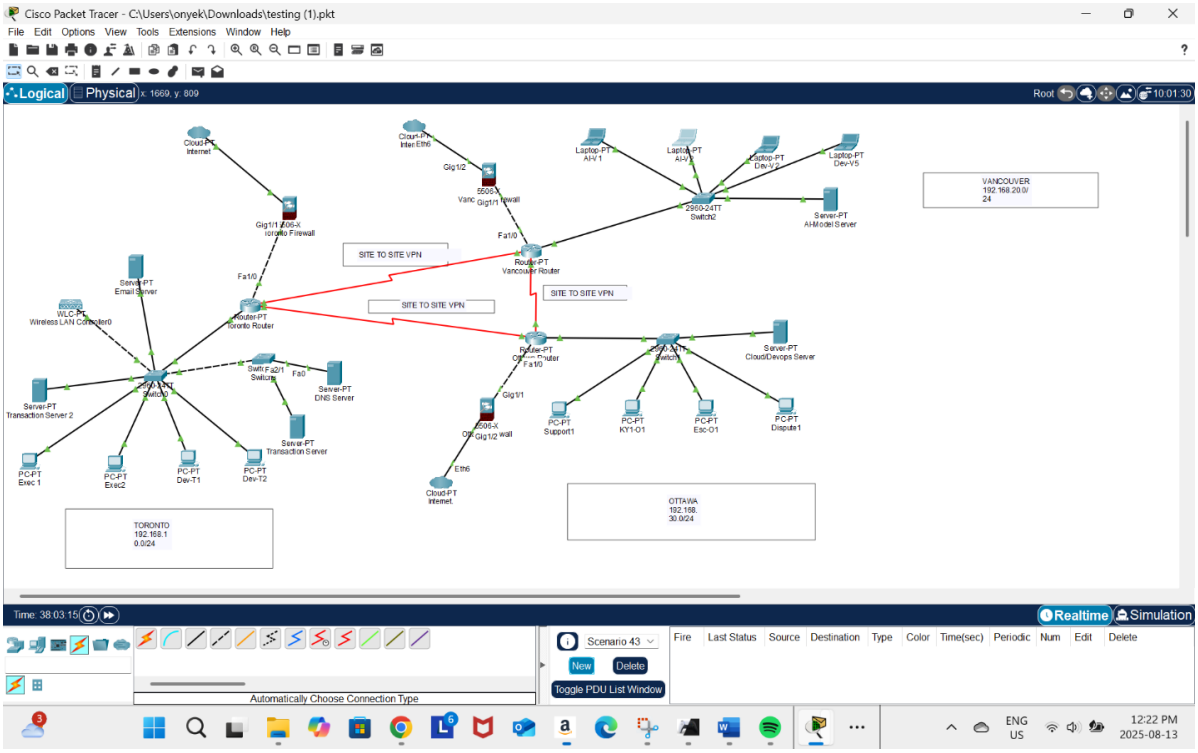

Figure 1: Enterprise Network Topology with Site-to-Site VPN Connections Across Toronto, Ottawa, and Vancouver.

- **Toronto HQ (192.168.10.0/24)** – Hosts core services including DNS/DHCP, Email, and Transaction Servers for payments and fraud detection. Secured with a Cisco ASA firewall (Zero Trust, VPN termination) and IDS/IPS for lateral traffic monitoring.

- **Vancouver Office (192.168.20.0/24)** – Runs AI Model Hosting Server for fraud detection and supports development workstations for payment API engineering. Connected to Toronto via AES-256–encrypted Site-to-Site VPN.

- **Ottawa Office (192.168.30.0/24)** – Functions as the Cloud/DevOps hub with a DevOps Server managing CI/CD for AWS/Azure and a bilingual VoIP-based support center. Uses separate VLANs for compliance team segregation.

2.2 VALIDATING AND TESTING

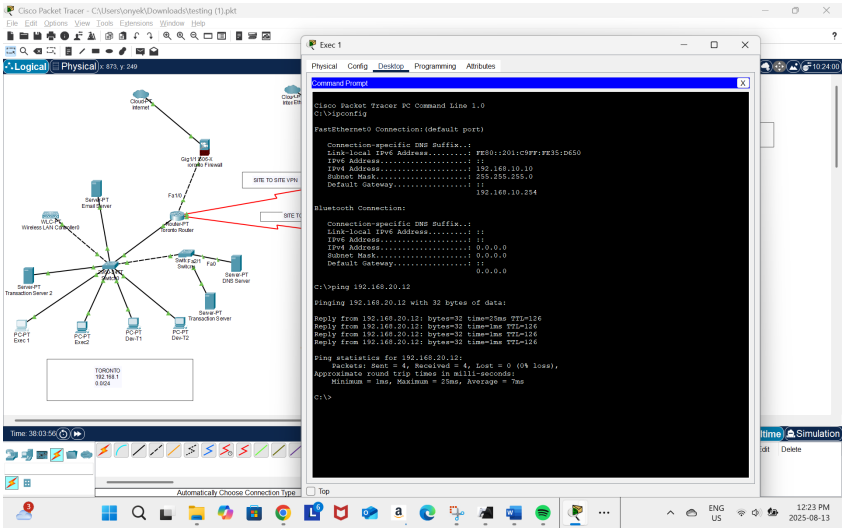

Figure 2: Successful ICMP ping from a Toronto client (192.168.10.10) to a Vancouver host (192.168.20.12), confirming VPN tunnel functionality and inter-site communication.

The ping test from a Toronto network device (IP: 192.168.10.10) to a Vancouver network host (IP: 192.168.20.12) was successful. All four ICMP echo requests received replies, indicating that the site-to-site VPN between Toronto and Vancouver is properly configured and operational. The round-trip time was minimal, showing efficient connectivity.

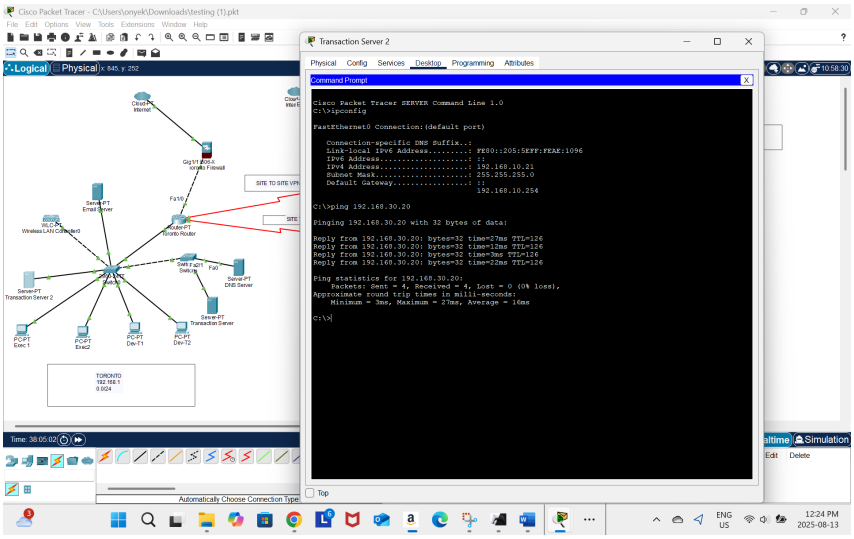

Figure 3: Successful ping from Toronto Transaction Server to Ottawa DevOps Server, verifying inter-site VPN connectivity.

This screenshot demonstrates a successful ICMP ping from the Transaction Server 2 in Toronto (192.168.10.21) to the Ottawa Cloud/DevOps Server

(192.168.30.20). The results confirm full connectivity across the Site-to-Site VPN between Toronto and Ottawa, with 0% packet loss and an average round-trip time of 16ms.

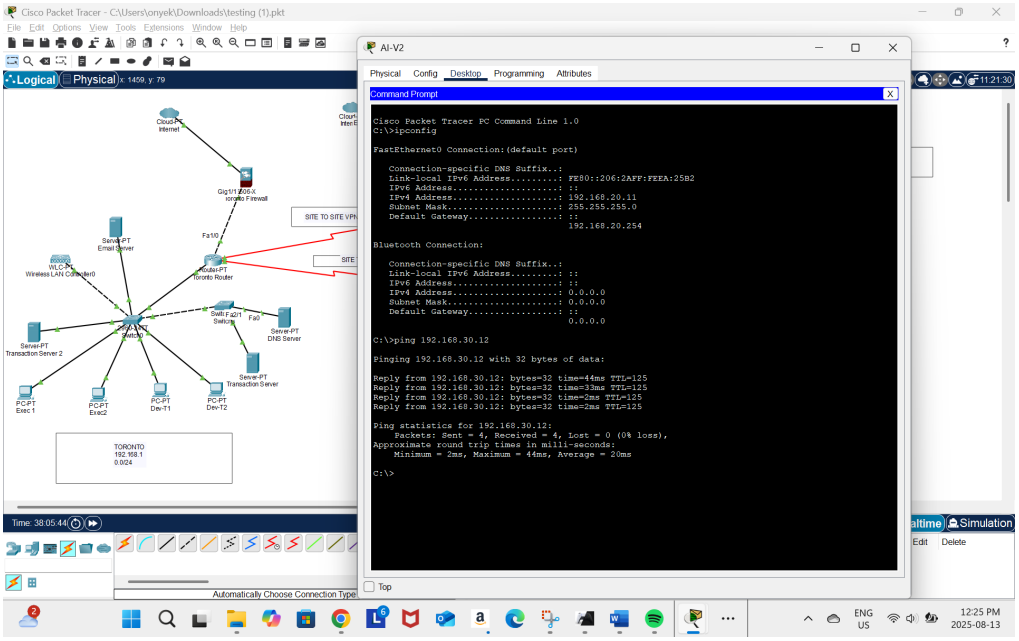

Figure 4: Successful ping from Vancouver host (192.168.20.11) to Ottawa host (192.168.30.12) confirming VPN tunnel connectivity.

The ping test from Vancouver (host 192.168.20.11) to Ottawa (host 192.168.30.12) was successful. All four packets were received with no loss, and round-trip times were within acceptable limits, confirming inter-site connectivity via the site-to-site VPN.

TASK 3

3.1 CIA ANALYSIS

CIA Protections Across the Network

3.1.1 CONFIDENTIALITY

- **Encryption & Access Control:** AES-256 encryption for data at rest, TLS/IPSec for data in transit, VPN enforcement, and DNSSEC to secure DNS records (NIST, 2007).
- **Authentication:** MFA for email, DevOps, and critical servers; RBAC for restricting access to roles; SSH key-based authentication (NIST, 2022) (SANS Institute, 2020).
- **Segmentation:** VLANs for isolating departments; private subnets for sensitive servers; ACLs to limit traffic to trusted IPs (CISA, 2021).
- **Specialized Protections:** DHCP snooping, 802.1X for device authentication, API token rotation for AI servers, encrypted credentials vaults in DevOps (NIST, 2022).

3.1.2 INTEGRITY

- **Verification & Signing:** Digital signatures on DNS records, firmware verification for firewalls/routers, code signing for transaction servers, Git commit signing for DevOps pipelines (Cisco, 2022).
- **Data Integrity Tools:** Checksums, hashing, SPF/DKIM/DMARC for email, file integrity monitoring (FIM) on endpoints and servers (CISA, 2021).
- **Change Controls:** Immutable logging to SIEM, configuration backups, change approval workflows, secure routing protocol authentication (CISA, 2021).

3.1.3 AVAILABILITY

- **Redundancy & Failover:** Secondary/backup servers for DNS/DHCP, email, DevOps, and transaction servers; HA firewall and router pairs; backup MX; failover VPN routes (CISA, 2021).
- **DDoS Protection:** Firewalls with rate limiting, IPS, SMTP throttling, and DNS query rate limiting (Cloudflare, 2023).
- **Resilience Measures:** RAID storage, UPS power backup, Anycast DNS, load balancing, clustering for transaction systems, and model caching for AI workloads (SANS, 2020).

3.1.4 CURRENT THREATS & VULNERABILITIES

- **DNS/DHCP:** DNS cache poisoning, DHCP starvation, unauthorized zone transfers, DNS amplification DDoS.
- **Email:** Phishing, ransomware via attachments, DoS/DDoS on SMTP ports (SANS Institute, 2020).
- **Transaction Servers:** SQL injection, credential brute force, insider fraud, ransomware, data exfiltration by APTs (OWASP, 2023).
- **Firewalls:** Misconfigured rules, unpatched firmware CVEs, DDoS on VPN concentrators, weak segmentation.
- **AI Model Server:** Model extraction, adversarial inputs, model/data poisoning, exposed APIs without rate limiting.
- **Workstations:** Phishing-based malware, insider threats, USB exploits.
- **DevOps:** Credential leakage in code, build pipeline injection, supply chain compromises.
- **Switches:** VLAN hopping, MAC flooding, STP misconfiguration.
- **Routers:** Route hijacking, outdated firmware exploits, routing table poisoning, and SNMP misconfigurations.
- **Site-to-Site VPN:** Weak PSKs, tunnel instability, replay attacks.

3.1.5. CIA-BASED MITIGATION MEASURES

Confidentiality Protections

- **Harden Access:** Enforce MFA, RBAC, SSH key auth; disable unused ports/services; rotate API tokens and PSKs.
- **Encrypt Everything:** Apply AES-256 for storage, TLS/IPSec for transit, DNSSEC/TSIG for DNS (NIST, 2007).
- **Segregate Traffic:** Maintain VLAN segmentation, ACLs, and private subnets; implement Split-Horizon DNS.

Integrity Protections

- **Validation & Monitoring:** SPF/DKIM/DMARC for email; checksums/digital signatures for code, configs, and models; input validation for transactions (MITRE, 2023).
- **Controlled Changes:** Immutable logs to SIEM, approval workflows, firmware signing verification, secure route authentication.
- **Tamper Detection:** FIM on endpoints/servers; zone file validation for DNS; ARP inspection on switches (MITRE, 2023).

Availability Protections

- **Build in Redundancy:** HA clusters, backup servers/sites, failover VPN routes, backup MX and DNS servers (MITRE, 2023).
- **Defend Against DoS/DDoS:** Query rate limiting, IPS/IDS, SMTP throttling, firewall rate limiting, protocol filtering.
- **Rapid Recovery:** RAID storage, UPS, automated backups (air-gapped for critical systems), model caching, hot-spare equipment (SANS, 2020).

3.2 CYBERSECURITY TEAMS AT CONESTRANSFER

ConesTransfer employs a **hybrid cybersecurity model** consisting of **Red, Blue, and Purple Teams** to provide full-spectrum security across its multi-site infrastructure and critical services.

Blue Team – Defense & Monitoring
Responsible for maintaining defenses, detecting threats, and responding to incidents. Key duties include:

- Monitoring network/endpoint logs via SIEM for indicators of compromise.
- Managing patch deployment, vulnerability scanning, and firewall/IPS rule updates.
- Ensuring VPN tunnel health, backup validation, and disaster recovery readiness.
- Performing log integrity checks and maintaining incident response protocols.

Red Team – Offensive Testing
Simulates real-world cyberattacks to uncover vulnerabilities before they are exploited. Responsibilities include:

- Conducting penetration tests on firewalls, VPNs, and exposed services.
- Running phishing and social engineering simulations.
- Identifying misconfigurations in VLANs, ACLs, and DNS.
- Testing physical security controls when applicable.

Purple Team – Coordination & Improvement
Bridges Red and Blue Teams to enhance detection and defense capabilities. Responsibilities include:

- Translating Red Team findings into actionable Blue Team improvements.
- Coordinating tabletop exercises, SOC drills, and incident simulations.
- Establishing continuous feedback loops for security enhancement.
- Defining and tracking cybersecurity performance metrics.

Overall Strategy Role

This three-team model enables proactive threat identification (Red Team), strong defense and rapid response (Blue Team), and strategic integration of lessons learned (Purple Team). It ensures that ConesTransfer can adapt to evolving cyber threats while safeguarding sensitive data, maintaining system availability, and improving resilience over time.

REFERENCES

Akiode, H. (2024, July 5). *Regulatory compliance for fintech startups in Canada*. Retrieved from Youverify: https://youverify.co/blog/regulatory-compliance-fintech-startups-canada

CISA. (2021, August). *Protecting VPNs and Remote Access*. Retrieved from Cybersecurity and Infrastructure Security Agency (CISA):, like DNS servers, email systems, and transaction servers,https://www.cisa.gov

Cisco. (2022). Catalyst 2960-X Series S*witches Security Best Practices*. Retrieved from Cisco: https://www.cisco.com

Cisco. (2023). *Email Authentication Technologies: SPF, DKIM, and DMARC*. Retrieved from Cisco: https://www.cisco.com

Cloudflare. (2023). *Email Security Best Practices*. Retrieved from Cloudflare: https://www.cloudflare.com/learning/email-security/

MITRE. (2023). *ATT&CK Framework for Endpoint Security*. Retrieved from MITRE ATT&CK®: https://attack.mitre.org

MITRE Corporation. (2023). *Enterprise Techniques - T1010: Application Layer Protocol*. Retrieved from MITRE ATT&CK: https://attack.mitre.org/techniques/T1010

National Institute of Standards and Technology (NIST). (2007). *SP 800-111: Guide to Storage Encryption Technologies for End User Devices*. Retrieved from NIST: https://csrc.nist.gov

NIST. (2022). *SP 800-53 Revision 5: Security and Privacy Controls*. Retrieved from NIST: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

OWASP. (2023). *OWASP Top 10 Web Application Security Risks*. Retrieved from OWASP: https://owasp.org/www-project-top-ten/

SANS. (2020). *VPN Configuration for Secure Enterprise Networks*. Retrieved from SANS Institute: https://www.sans.org

SANS Institute. (2020). *Security Awareness Planning*. Retrieved from SANS Institute: https://www.sans.org