Network Security Solution Documentation

A Comprehensive Network Security Solution for University Infrastructure

CS478
Paris Zhou
3/19/25

Executive Summary

Universities are high-value targets for cyber threats due to their open networks, diverse users, and vast stores of sensitive data. This report outlines a layered security strategy to safeguard the university's digital infrastructure, ensuring academic integrity, operational continuity, and data protection.

Security Strategy Overview

At the heart of this security approach is defense in depth—a system of overlapping protections that guard against threats at every level. The network perimeter is fortified with firewalls, intrusion detection, and encryption, preventing unauthorized access while allowing legitimate traffic to flow securely. Segmentation and access control ensure that critical systems are insulated from external threats, restricting movement within the network and minimizing potential damage. [6]

To combat stealthy attacks, the university employs continuous monitoring and intelligent threat detection. By analyzing network behavior and identifying anomalies, security teams can respond to attacks before they escalate. Encrypted traffic, while crucial for privacy, can also be used to conceal threats. Selective decryption and packet analysis help uncover hidden dangers while maintaining data confidentiality. [4]

A key focus is on identity security, ensuring that only the right people access the right information. Multi-factor authentication (MFA), strong password policies, and user education reinforce this layer of defense, reducing the risk of stolen credentials and unauthorized access. [3]

Mitigating Risks and Responding to Threats

Cyber threats evolve constantly, and proactive defenses are necessary to stay ahead. Routine vulnerability scans and patch management ensure that weaknesses are identified and addressed before they can be exploited. Automated response mechanisms help neutralize threats in real time, limiting their impact. [1]

Some risks, however, must be accepted. Legacy systems, budget constraints, and usability concerns mean that not every vulnerability can be eliminated immediately. Instead, these risks are documented, monitored, and controlled through strategic mitigation, such as network isolation and enhanced monitoring. [1]

Balancing Security and Usability

While strong security is essential, it must not hinder academic collaboration and research. The university's security policies strike a balance between rigid protection and flexible access, ensuring that researchers, students, and faculty can work without unnecessary restrictions. Adaptive security measures, such as risk-based authentication and contextual access controls, provide protection without disrupting workflow. [3]

No system is completely invulnerable, but a well-structured, multi-layered security strategy significantly reduces risk. By combining robust defenses, intelligent detection, and agile response mechanisms, the university maintains a resilient security posture while fostering an open, collaborative learning environment. Continuous improvement, regular assessments, and adaptation to emerging threats ensure that the institution remains secure in an ever-changing digital landscape.

Network Diagram Summary & Justification

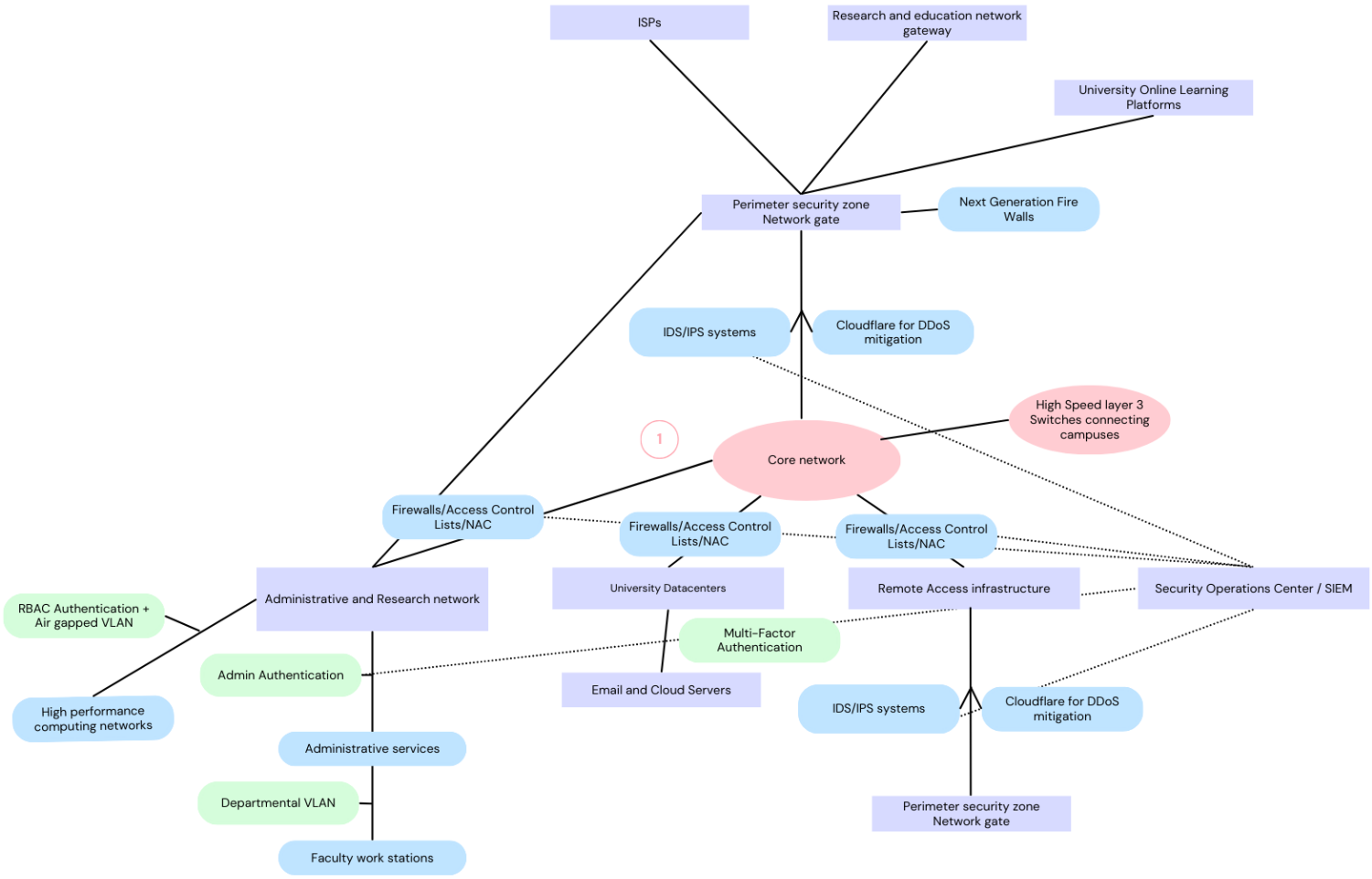
Summary of Network Design

The university's network is divided into key segments:

- **Core Network:** Backbone with redundant high-speed connections.
- **Perimeter Security:** Firewalls, DDoS protection, and network access controls.
- **Administrative & Research Network:** Strict access controls, IPS/IDS deployment.
- **Student & Faculty Network:** Segmented VLANs, Wi-Fi security with WPA3.
- **Research Labs & HPC:** Isolated environment with strict data policies.
- **VPN & Remote Access:** Enforced MFA, split/full tunnel VPN strategies.
- **Security Operations (SOC):** Centralized log collection, SIEM monitoring.

Justification

- **Segmentation:** Reduces attack surface and prevents lateral movement.
- **Redundancy:** Ensures high availability of critical resources.
- **Zero Trust Principles:** Least privilege access across all segments.
- **Threat Detection & Response:** Continuous monitoring and automated response.


ISPs
Research and education network gateway
University Online Learning Platforms
Perimeter security zone Network gate
Next Generation Fire Walls
IDS/IPS systems
Cloudflare for DDoS mitigation
High Speed layer 3 Switches connecting campuses
1
Core network
Firewalls/Access Control Lists/NAC
Firewalls/Access Control Lists/NAC
Firewalls/Access Control Lists/NAC
Administrative and Research network
University Datacenters
Remote Access infrastructure
Security Operations Center / SIEM
RBAC Authentication + Air gapped VLAN
Multi-Factor Authentication
Admin Authentication
Email and Cloud Servers
IDS/IPS systems
Cloudflare for DDoS mitigation
High performance computing networks
Administrative services
Departmental VLAN
Perimeter security zone Network gate
Faculty work stations

Security Controls & Threat Mitigation

1. Defenses Against Network Scanning

- **Firewalls** block unauthorized inbound ICMP and TCP/UDP scans, preventing attackers from discovering open ports and services [1].
- **Deception techniques** such as honeypots lure malicious reconnaissance traffic, misleading adversaries [1].
- **Network segmentation** minimizes exposed attack surfaces by restricting lateral movement within the network.

2. Packet Capture & Decryption

- **SSL/TLS interception** on secured perimeter devices detects hidden threats in encrypted traffic [4].
- **Full packet capture** for forensic investigations aids in post-attack analysis.
- **Controlled access to decryption keys** prevents unauthorized data leakage and maintains data confidentiality [4].

3. Vulnerability Scanning

- **Scheduled scans** using Nessus/OpenVAS to detect misconfigurations and vulnerabilities [1].
- **Automated patching and remediation** ensures security updates are applied promptly.
- **Risk-based prioritization** helps focus resources on fixing critical vulnerabilities first.

4. Defenses Against MITM Attacks

- **Encrypted communication** using TLS 1.3 and IPsec ensures data integrity.
- **Strict DNSSEC implementation** prevents DNS spoofing and cache poisoning.
- **802.1X authentication** for wired and wireless networks enforces device verification [3].

5. Credential Stealing Prevention

- **Enforced password policies** and MFA reduce risks of unauthorized access [3].
- **User education on phishing awareness** minimizes social engineering attacks.
- **Endpoint security software** detects keyloggers and credential theft malware.

6. Defenses Against Session Hijacking

- **Secure session cookies** with HTTPOnly and Secure flags mitigate cross-site scripting (XSS) risks [2].
- **Automatic session timeouts and re-authentication** for critical services prevent long-lived sessions from being hijacked.

7. Multi-Factor Authentication (MFA) Implementation

- **Mandatory MFA** for administrative and research accounts strengthens authentication security.
- **Adaptive MFA** adjusts authentication factors based on login risk levels[3].

8. Encryption Key Management

- **AES-256 encryption** ensures secure data protection both at rest and in transit.
- **Regular key rotation** and secure key storage mitigate cryptographic key compromise[4].

9. Firewall Deployment

- **Next-Gen Firewalls (NGFWs)** with deep packet inspection (DPI) detect and block advanced threats [5].
- **Geo-blocking** for high-risk countries reduces attack surface exposure.
- **Regular audits and rule updates** ensure firewalls remain effective against evolving threats.

10. IDS/IPS Deployment

- **Snort/Suricata for real-time anomaly detection** enables proactive threat identification [2].
- **Detection rules** improve accuracy and reduce false positives.

11. Logging Strategies

- **SIEM-based centralized log management (Splunk/ELK)** provides comprehensive threat visibility.
- **Automated log rotation, retention, and encryption** protect log integrity and confidentiality [1] [4].

12. Secure Routing

- **BGP route validation** prevents route hijacking attacks [5].
- **OSPF authentication** secures routing updates against unauthorized injections

13. DDoS Mitigation

- **Cloud-based scrubbing services (Cloudflare, Arbor)** offload malicious traffic.
- **Rate limiting and anomaly-based detection** prevents volumetric and application-layer attacks [3].

14. Remote-Based Fuzzing Attack Prevention

- **Input validation and fuzzing tests** during software development mitigate unknown vulnerabilities.
- **Application-layer firewalls (WAFs)** protect against web-based exploits [5].

15. VPN Security Policies

- **Strict authentication and logging** for VPN connections prevent unauthorized remote access[1].
- **Split vs. full tunneling** strategies balance security and performance.

16. Onion Routing Detection

- **Deep packet inspection (DPI)** identifies Tor traffic.
- **Blocking known Tor exit nodes** via threat intelligence reduces anonymity abuse risks[6].

17. Proxy Deployment

- **Forward proxies** enable web filtering and caching for security and performance.
- **Reverse proxies** enhance application security and load balancing[1].

18. Network Redundancy

- **Dual ISPs with automatic failover** ensure uninterrupted connectivity.
- **Redundant data centers** enhance disaster recovery capabilities [5].

19. Covert Channel Detection

- **AI-driven traffic anomaly detection** identifies hidden data exfiltration channels.
- **Packet timing analysis** detects covert communication methods[6].

20. Beaconing Detection

- **Behavioral analytics** detects periodic network activity from compromised hosts.
- **Isolation of compromised endpoints** prevents malware propagation [6].

Risk Acceptance & Justification

While the above security controls significantly enhance the university's cybersecurity posture, no security model is completely risk-free**.** Some residual risks must be accepted based on feasibility, cost, and operational impact. The following factors outline the **risk acceptance strategy** and **rationale** for these decisions:

1. Documenting and Monitoring Residual Risks

- Every security measure has some level of bypass potential by sophisticated attackers using advanced techniques.
- **Regular risk assessments** and penetration testing help identify gaps and prioritize improvements.
- A **risk register** is maintained, documenting vulnerabilities that cannot be mitigated immediately, with ongoing monitoring.

2. Legacy System Risks & Network Segmentation

- Some **legacy systems** cannot be updated due to software dependencies.
- To mitigate risks, these systems are **segmented from critical networks** and monitored for anomalies.
- Risk is accepted because replacing such systems would be **cost-prohibitive** or **disrupt essential university operations**.

3. Cost vs. Benefit Analysis for Security Investments

- While **full implementation** of all security controls would be ideal, financial constraints require **prioritization**.
- Investments focus on **high-impact mitigations** such as MFA, IDS/IPS, and NGFWs.
- Lower-priority risks, such as **low-impact vulnerabilities**, are documented and monitored rather than immediately patched.

4. User Behavior & Awareness Limitations

- **Human error remains a major security risk** despite strong technical controls.
- Even with phishing education, some users may fall for sophisticated social engineering attacks.
- **Continuous security awareness training** and simulated phishing campaigns help minimize this risk.

5. Balancing Security & Usability

- **Excessive security measures** can negatively impact research, collaboration, and productivity.
- For example, **strict VPN policies** improve security but may disrupt remote work.
- **Adaptive security controls** (e.g., risk-based MFA) balance usability with strong security measures.

6. Third-Party & Supply Chain Risks

- The university relies on third-party services, including cloud platforms and research networks.
- While contractual agreements enforce security requirements, supply chain attacks remain a risk.
- Vendor security assessments and monitoring of third-party integrations reduce exposure to such risks.

7. Insider Threats & Access Control Limitations

- Despite role-based access control policies, insider threats remain a non-zero risk.
- Risks include misuse of privileged accounts, accidental data leaks, or malicious intent.
- Strict logging, auditing, and behavior monitoring help detect anomalies early.

8. Zero-Day Exploits & Evolving Threats

- Advanced attackers leverage zero-day vulnerabilities that have no available patch.
- Threat intelligence, IDS, and anomaly detection help mitigate these risks until patches become available.
- Cyber incident response plans ensure rapid action in case of zero-day exploitation.

Conclusion: Accepting Residual Risks Strategically

- No system is 100% secure, but a layered security approach minimizes attack surfaces.
- Regular assessments, security audits, and incident response readiness ensure risks remain at an acceptable level.
- The university continuously evaluates new threats and technologies, adapting its security policies accordingly.

References

[1] J. J. Hughes, *Employing Deceptive Dynamic Network Topology Through Software-Defined Networking*, Monterey, CA, USA: Naval Postgraduate School, Mar. 2014. [Online]. Available: https://hdl.handle.net/10945/41392.

[2] S. E. Vadakkethil Somanathan Pillai and K. Polimetla, "Mitigating DDoS Attacks using SDN-based Network Security Measures," *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)*, Raichur, India, 2024, pp. 1-7, doi: 10.1109/ICICACS60521.2024.10498932.

[3] S. Mishra, S. Mishra, Y. C. Toh, S. Mishra, and P. T. Vi, “Mitigating the threat of multi-factor authentication (MFA) bypass through man-in-the-middle attacks using EvilGinx2,” in *Creative Approaches Towards Development of Computing and Multidisciplinary IT Solutions for Society*, A. Bijalwan, R. Bennett, G. B. Jyotsna, and S. N. Mohanty, Eds. 2024. [Online]. Available: https://doi.org/10.1002/9781394272303.ch5.

[4] T. Radivilova, L. Kirichenko, D. Ageyev, M. Tawalbeh, and V. Bulakh, "Decrypting SSL/TLS traffic for hidden threats detection," *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2018, pp. 143-146, doi: 10.1109/DESSERT.2018.8409116.

[5] A. Shameli-Sendi, Y. Jarraya, M. Pourzandi, and M. Cheriet, "Efficient Provisioning of Security Service Function Chaining Using Network Security Defense Patterns," *IEEE Transactions on Services Computing*, vol. 12, no. 4, pp. 534-549, July-Aug. 2019, doi: 10.1109/TSC.2016.2616867.

[6] . A. A. Qahtani and E.-S. M. El-Alfy, "Anonymous connections based on onion routing: A review and a visualization tool," *Procedia Computer Science*, vol. 52, pp. 121-128, 2015. doi: 10.1016/j.procs.2015.05.040.