Cyber Tree Systems
A Business IT Solution Company

Firewall and VPN Security Policy

1.0 Statement of Purpose:

The purpose of this policy is to establish clear guidelines for the implementation, configuration, and management of firewall and VPN security controls within the organization. Firewalls serve as a critical security barrier, protecting internal systems from unauthorized access, while VPNs ensure secure remote connectivity for employees and authorized third parties. This policy defines the rules and responsibilities for maintaining these security measures to safeguard sensitive data, prevent unauthorized access, and support compliance with organizational and regulatory requirements.

2.0 Scope:

The policy applies to all employees, contractors, vendors and third parties who interact with the organization’s network infrastructure. It governs the design, deployment, monitoring and maintenance of both internal and external firewalls, as well as VPN connections used for remote access. The policy extends to all company-owned and managed devices that connect to the network, whether on-premises or remote.

3.0 Firewall and VPN Security Policy

3.1 Objectives

This policy aims to ensure the security and integrity of network resources by implementing robust firewall and VPN configurations. These measures help mitigate external and internal threats, enforce access control, and comply with industry standards. Regular monitoring and security assessments will ensure continued protection against evolving cyber risks.

- Ensure that firewalls and VPNs are properly configured to protect network resources from external and internal threats.
- Define access control policies to regulate network traffic and prevent unauthorized connections.
- Implement security best practices for remote access, including encryption, authentication, and logging.
- Establish clear monitoring, auditing, and incident response procedures for firewall and VPN-related security events.
- Maintain compliance with relevant cybersecurity standards, such as NIST, ISO 27001, and industry-specific regulations.
- Ensure that firewall and VPN configurations are optimized for both security and network performance, with regular penetration testing and security assessments.

3.2 Firewall Policy

Firewalls are essential for enforcing network security by filtering and blocking unauthorized traffic. By defining proper configuration standards and access control policies, the organization can reduce exposure to cyber threats. Logging and monitoring ensure timely detection and response to potential security incidents.

3.2.1 Firewall Configuration Standards

Firewalls must adhere to a minimum security baseline, which includes denying all inbound traffic by default and allowing only authorized services.

- Only approved firewall vendors and configuration tools specified by the organization may be used.
- Firewalls must be configured to prevent unauthorized access and mitigate potential threats, including malware, denial-of-service attacks, and unauthorized data exfiltration.

3.2.2 Access Control Policies

To minimize unauthorized access, well-defined traffic filtering rules and network segmentation must be enforced. These measures help limit lateral movement within the network and restrict access to sensitive resources.

- Traffic filtering rules must be clearly defined for inbound and outbound network traffic, ensuring that only authorized services and applications are permitted.
- Internal network segmentation must be enforced to isolate sensitive data and minimize the potential impact of a security breach.
- Firewall rules must be reviewed periodically to ensure compliance with security standards and evolving threat landscapes.

3.2.3 Firewall Logging and Monitoring

Continuous monitoring and logging provide visibility into network activity and help detect security breaches in real time. Proper retention of logs supports forensic investigations and compliance requirements.

- Firewall logs must be retained for a minimum of 90 days to support security investigations and audits.
- Real-time monitoring and alerting mechanisms must be established to detect and respond to unauthorized access attempts promptly.
- Logs must be securely stored and accessible only to authorized personnel for forensic analysis and compliance audits.

3.3 VPN Policy

VPNs provide secure remote access to organizational resources, ensuring that data remains protected while in transit. Proper authentication and encryption mechanisms help prevent unauthorized access and data breaches.

3.3.1 VPN Access Requirements

To maintain a secure remote access environment, only authorized personnel should be granted VPN access. Users must meet security prerequisites to minimize risks associated with compromised credentials or vulnerable devices.

- VPN access is limited to authorized personnel, including employees, contractors, and approved third-party vendors.
- Users must complete security training and adhere to multi-factor authentication (MFA) requirements before being granted VPN access.
- Devices connecting to the VPN must comply with organizational security standards, including up-to-date patches and endpoint protection software.

3.3.2 VPN Encryption Standards

Strong encryption ensures the confidentiality and integrity of data transmitted over VPN connections. Implementing industry-recommended encryption protocols prevents unauthorized interception of network traffic.

- All VPN connections must use strong encryption, with a minimum of AES-256 for data encryption and TLS 1.2 or higher for secure connections.

- Approved VPN tunneling protocols include IPsec, OpenVPN, and WireGuard.
- VPN traffic must be inspected for anomalies and potential security threats.

3.3.3 Remote Access Control

Strict remote access policies ensure that VPN users do not inadvertently expose internal network resources to security threats. Session timeouts and access restrictions minimize risk from compromised accounts or stolen devices.

- VPN sessions must automatically terminate after a defined period of inactivity to prevent unauthorized access.
- Remote users must only be granted access to necessary network resources based on the principle of least privilege.
- A review of remote access permissions must be conducted periodically to ensure security compliance.

3.4 Firewall and VPN Change Management

Uncontrolled changes to firewall and VPN settings can introduce security vulnerabilities and misconfigurations. A structured approval and review process ensures that changes are thoroughly vetted before implementation.

- Any modifications to firewall rules or VPN configurations must undergo an approval process, including review by the security and network administration teams.
- Changes must be documented and tested in a controlled environment before deployment.
- A periodic review of firewall rulesets and VPN access lists must be conducted to identify and remove obsolete or unnecessary configurations.

3.5 Incident Response and Monitoring

Timely detection and response to security incidents involving firewalls and VPNs are crucial for minimizing damage. Implementing a dedicated incident response framework ensures rapid containment and remediation.

- A dedicated Incident Response Team (IRT) must be established to investigate and respond to security incidents involving firewalls and VPNs.
- Firewall and VPN security events must be logged and correlated with other security monitoring tools to detect potential breaches.
- Incident response procedures must include predefined escalation protocols and communication plans.
- Post-incident reviews must be conducted to identify lessons learned and implement improvements to security policies and procedures.

4.0 Enforcement

Strict enforcement of this policy ensures compliance with security standards and mitigates risks associated with unauthorized access. Violations will result in disciplinary actions as appropriate.

- Any violation of this policy may result in disciplinary actions, including but not limited to revocation of access, formal warnings, and termination of employment or contract.
- Regular compliance monitoring and periodic audits must be conducted to ensure adherence to firewall and VPN security policies.
- Employees and contractors must acknowledge their understanding of this policy as a condition of accessing network resources.

5.0 Definitions

Term	Definition
Security Administrator	Responsible for configuring, maintaining, and monitoring firewall and VPN security settings
Network Administrator	Ensures that the Firewall and VPN configurations align with network architecture and performance requirements.
Incident Response Team	Investigates and responds to security events related to firewall and VPN breaches
End User	Must follow remote access security procedures when creating VPNs and report anomalies.

6.0 Revision History

Revision Number	Date	Editor	Reason
1.0	2/19/2025	Aidan Schmeckpeper	Created.