Rick Abraham

My Company  Dallas, TX

Risk Assessment - Network Security Risks

Contents

[Introduction 2](#_Toc182579178)

[Purpose 2](#_Toc182579179)

[Scope 2](#_Toc182579180)

[Risk Identification 2](#_Toc182579181)

[Risk Analysis 3](#_Toc182579182)

[Mitigation Recommendations 3](#_Toc182579183)

[Firewall 3](#_Toc182579184)

[VPN 3](#_Toc182579185)

[Wireless Access Points 4](#_Toc182579186)

[Routers and Switches 4](#_Toc182579187)

[IDS/IPS Systems 4](#_Toc182579188)

[Monitoring and Review 4](#_Toc182579189)

[Frequency 4](#_Toc182579190)

[Daily 4](#_Toc182579191)

[Monthly 5](#_Toc182579192)

[Quarterly 5](#_Toc182579193)

[Bi-Annually 5](#_Toc182579194)

[Annually 5](#_Toc182579195)

[Incident Response 5](#_Toc182579196)

[Documentation and Compliance 6](#_Toc182579197)

Risk Assessment - Network Security Risks

# Introduction

Purpose: To assess, identify, and manage network security risks that may impact the organization, with a focus on minimizing exposure to unauthorized access, data breaches, and loss of network integrity.

Scope: This assessment encompasses all network-related assets and configurations, including but not limited to firewalls, VPNs, routers, switches, intrusion detection/prevention systems (IDS/IPS), and any other network security devices. This policy applies to on-premises and cloud environments, as well as remote access configurations.

# Risk Identification

| **Asset** | **Threat** | **Vulnerability** | **Impact** | **Risk Rating** |
| --- | --- | --- | --- | --- |
| Firewall | Unauthorized access through misconfigured rules | Outdated or overly permissive firewall rules | Data breaches, unauthorized system access | High |
| VPN | Credential theft or brute-force attacks | Weak authentication protocols, lack of MFA | Unauthorized access, compromised sensitive data | High |
| Wireless Access Points | Eavesdropping or man-in-the-middle (MITM) attacks | Lack of encryption and insecure configurations | Data interception, network infiltration | High |
| Routers and Switches | Exploitation of outdated firmware or open ports | Failure to apply patches or restrict management access | Network-wide disruption | Medium |
| IDS/IPS Systems | Failure to detect evolving attack vectors | Inefficient rule updates or lack of advanced monitoring | Delayed response to attacks, extended downtime | Medium |

# Risk Analysis

| **Asset** | **Likelihood** | **Impact Severity** | **Overall Risk Level** |
| --- | --- | --- | --- |
| Firewall | High | High | Critical |
| VPN | High | High | Critical |
| Wireless Access Points | High | High | Critical |
| Routers and Switches | Medium | Medium | High |
| IDS/IPS Systems | Medium | High | High |

# Mitigation Recommendations

## Firewall

* Update firewall rules to follow a **deny-all default policy**, permitting only explicitly required traffic.
* Conduct **quarterly firewall audits** to identify and correct overly permissive or outdated rules.
* Deploy real-time monitoring and automated alerts for firewall rule changes.

## VPN

* Enforce **multi-factor authentication (MFA)** for all VPN users to mitigate credential theft.
* Conduct **penetration testing** on VPN configurations to identify potential vulnerabilities.
* Regularly update VPN software and configure strong encryption protocols (e.g., AES-256).

## Wireless Access Points

* Enable **WPA3 encryption** and configure a secure passphrase for all access points.
* Use **network segmentation** to isolate wireless guest traffic from critical infrastructure.
* Regularly review wireless logs to detect unauthorized access attempts.

## Routers and Switches

* Apply firmware updates promptly and disable unnecessary ports to reduce attack vectors.
* Use **access control lists (ACLs)** to restrict management access to authorized IP ranges.
* Monitor for unusual traffic patterns that could indicate compromised devices.

## IDS/IPS Systems

* Regularly update signatures and rules to detect the latest attack vectors.
* Deploy advanced threat detection tools (e.g., behavioral analytics) to identify anomalies.
* Conduct bi-annual evaluations of IDS/IPS performance and tune configurations for optimal coverage.

# Monitoring and Review

## Frequency

Daily

* Review **firewall and VPN logs** to detect unauthorized access attempts, failed login attempts, or unusual traffic patterns.
* Monitor **IDS/IPS alerts** for suspicious activity, such as port scans, brute-force attacks, or malicious traffic.
* Ensure **network monitoring tools** (e.g., SNMP, NetFlow) are operational and generating alerts for critical network events.
* Validate **endpoint connectivity** to detect anomalies in device behavior (e.g., rogue devices or unexpected network activity).

Monthly

* Verify that firewall rules, VPN configurations, and IDS/IPS signatures are up-to-date and optimized for current threats.
* Audit logs for configuration changes in routers, switches, and other network devices.
* Review network traffic patterns to detect persistent or unusual activity, such as data exfiltration attempts.

### Quarterly

* Perform audits of access permissions for VPNs, firewalls, and wireless access points to ensure compliance with access control policies.
* Test the effectiveness of network security controls, including IDS/IPS and anti-DDoS measures.
* Review firmware and software versions for all network devices, ensuring critical updates are applied.

### Bi-Annually

* Conduct **penetration testing** on firewalls, VPNs, and other key infrastructure to evaluate vulnerabilities and assess mitigation measures.
* Perform **network segmentation audits** to confirm that sensitive systems are isolated from general traffic and guest networks.
* Run **tabletop exercises** simulating network breaches to assess incident response readiness and identify gaps in the playbook.

### Annually

* Conduct a comprehensive risk assessment to reassess network security risks based on changes in infrastructure, threat landscapes, or compliance requirements.
* Update network security policies and procedures to reflect lessons learned from incidents, audits, and penetration tests.

## Incident Response

* Maintain a **Network Incident Response Team (NIRT)** trained to handle network-specific threats, including unauthorized access, DDoS attacks, and malware outbreaks.
* Conduct **bi-annual response drills** simulating network-specific incidents, such as a firewall breach or ransomware attack.
* Document response actions, lessons learned, and improvements implemented after every network-related incident.

## Documentation and Compliance

* Maintain detailed records of daily log reviews, including firewall, VPN, and IDS/IPS activities.
* Document the results of all network audits, penetration tests, and configuration reviews.
* Ensure compliance with applicable industry standards, such as:
  + **NIST SP 800-53**: SC-7 (Boundary Protection), SI-4 (Monitoring), AC-3 (Access Enforcement).
  + ISO 27001, PCI DSS, and any industry-specific regulatory requirements.