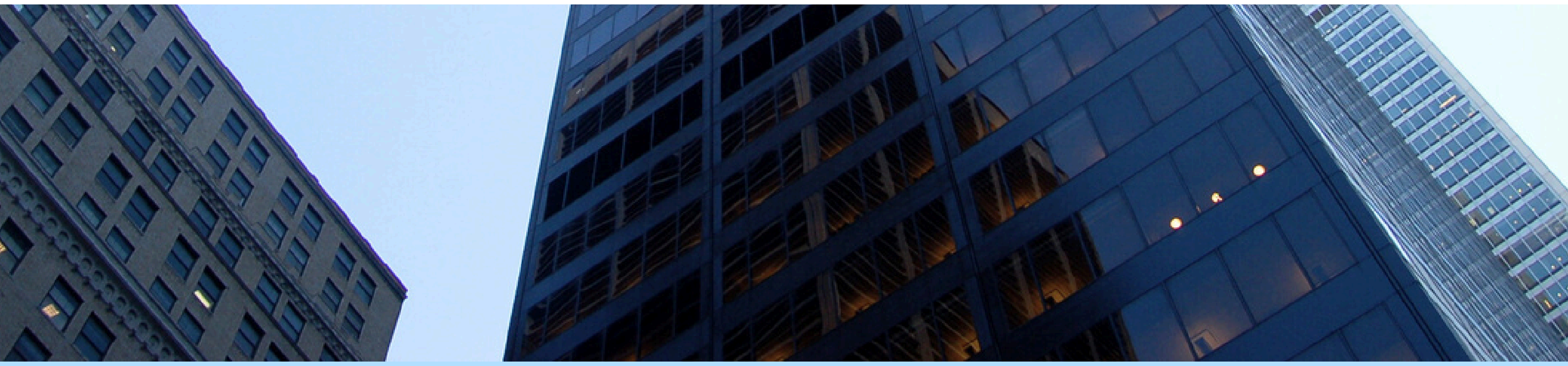
SECURZE

SECURING WHAT MATTERS MOST



ADVANCE NETWORK SECURITY CHECKLIST

www.securze.com

info@securze.com

☎ +91 84510 73938

securze

securze_com

Securze

This comprehensive network security checklist emphasizes best practices to fortify an organization's defenses. Examples include configuring firewalls with explicit rules to prevent overly permissive access, implementing intrusion detection systems with finely-tuned signatures, and enforcing secure VPN configurations with strong authentication. Network segmentation using VLANs and ACLs adds an additional layer of defense, while robust Wi-Fi security measures, such as WPA3 encryption, enhance wireless network protection. The checklist also underscores the importance of continuous monitoring, leveraging tools like Wireshark and NetFlow, and maintaining a diligent patch management process for routers, switches, and other network devices.

1. FIREWALL CONFIGURATIONS:

Review and update firewall rules.

- Example: Remove overly permissive rules like allowing any-to-any traffic. Instead, use explicit rules allowing only necessary ports and protocols.

Ensure default deny policies are in place.

- Example: Set the default rule to deny all traffic and explicitly allow only required traffic through specific rules.

Monitor for unauthorized changes to firewall settings.

- Example: Implement change detection mechanisms to alert on any modification to firewall rules.

Application Layer Filtering

- Implement application layer filtering within the firewall to scrutinize and control traffic based on specific applications or services. For instance, configure rules that allow or block traffic associated with applications like social media or peer-to-peer file sharing. This nuanced control enhances security by preventing unauthorized application usage and mitigating risks associated with unapproved services.

2. INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS):

Implement and maintain IDPS solutions.

- Example: Deploy signature-based detection rules and ML trained models to identify and detect attack patterns.

Regularly update and fine-tune intrusion detection signatures.

- Example: Adjust signature sensitivity and specificity based on the network's normal behavior.

Analyze and respond to alerts generated by the IDPS.

- Example: Develop and document incident response procedures for different IDPS alerts.

Continuous Threat Intelligence Integration

- Integrate continuous threat intelligence feeds, such as those provided by services like Open Source Threat Intelligence (OSINT) or commercial threat intelligence platforms, into the IDPS. For example, configure the system to dynamically update its signature database based on the latest indicators of compromise (IoCs) and known malicious IP addresses. This ensures that the IDPS remains informed about emerging threats, such as new malware variants or attack patterns, allowing for timely and proactive defense measures.

Automated Threat Remediation

- Implement automated threat remediation capabilities within the IDPS to respond swiftly to identified threats. For instance, configure the system to automatically block or quarantine malicious IP addresses and devices, reducing the response time and minimizing the potential impact of security incidents. This automated remediation feature enhances the efficiency of the IDPS, allowing it to actively thwart threats in real-time without manual intervention.

3. NETWORK SEGMENTATION:

Segment the network to limit lateral movement in case of a breach.

- Example: Use VLANs to isolate departments or sensitive areas from each other.

Apply access controls between network segments.

- Example: Use access control lists (ACLs) to restrict traffic between segments.

Review and update segmentation policies.

- Example: Regularly assess and adjust segmentation policies based on changes in network architecture or security requirements.

Application-Centric Segmentation

- Implement application-centric segmentation, tailoring network segmentation based on the specific requirements of critical applications. For example, isolate web servers, databases, and application servers into dedicated segments with customized access controls. This approach optimizes security measures for the unique needs of each application, enhancing overall network protection.

Zero Trust Network Architecture

- Embrace a Zero Trust Network Architecture, wherein trust is never assumed, and strict access controls are enforced irrespective of the user or device's location. Employ technologies like identity-based access controls and multifactor authentication. This approach ensures that every network communication is verified, reducing the risk of unauthorized access and providing a robust security framework for modern business environments.

4. VPN AND REMOTE ACCESS:

Securely configure virtual private network (VPN) access.

- Example: Use strong encryption protocols like IKEv2 or OpenVPN.

Enforce strong authentication for remote access.

- Example: Implement multi-factor authentication for VPN connections.

Monitor VPN logs for suspicious activity.

- Example: Set up logging for VPN connections and regularly review logs for anomalies.

Geo-Fencing for Access Control

- Implement geo-fencing capabilities to restrict VPN access based on geographical locations. Configure the VPN to allow connections only from approved regions or countries, adding an extra layer of access control. This approach helps prevent unauthorized access attempts from regions with higher cybersecurity risks and aligns with a more stringent security posture.

Multi-Factor Authentication (MFA) Integration

- Integrate multi-factor authentication (MFA) seamlessly with the VPN to enhance user authentication. For instance, configure the VPN to require a combination of passwords and temporary authentication codes from a secondary device. This adds an extra layer of security, mitigating the risk of unauthorized access even if credentials are compromised.

5. WIRELESS NETWORK SECURITY:

Secure Wi-Fi networks with strong encryption.

- Example: Use WPA3 encryption for Wi-Fi networks.

Change default credentials for Wi-Fi routers.

- Example: Replace default usernames and passwords on Wi-Fi routers.

Regularly audit and update wireless access point configurations.

- Example: Conduct periodic reviews of Wi-Fi settings, including SSID, encryption, and access controls.

6. NETWORK MONITORING:

Implement continuous network monitoring.

- Example: Use tools like Wireshark or Snort to capture and analyze network traffic and review any malicious activities.

Analyze network traffic for anomalies and security events.

- Example: Set up alerts for unusual patterns, such as a sudden spike in traffic or multiple failed login attempts.

Use network flow analysis tools for visibility.

- Example: Utilize NetFlow or sFlow to gain insights into network traffic patterns.

7. PATCH MANAGEMENT:

Establish a robust process for applying security patches.

- Example: Implement a regular patching schedule, applying critical patches promptly.

Regularly update network devices, including routers and switches.

- Example: Check for firmware updates from device manufacturers and apply them as needed.

Monitor vendor security advisories for patch releases.

- Example: Subscribe to vendor mailing lists and promptly apply patches in response to security advisories.

8. ENDPOINT SECURITY MEASURES:

Implement comprehensive security measures on endpoint devices, including desktops, laptops, and mobile devices.

- Example: Utilize endpoint protection software with features such as antivirus, anti-malware, and device control to safeguard individual devices from a variety of security threats.

Application Whitelisting

- Implement application whitelisting to allow only approved and authorized applications to run on endpoints. This mitigates the risk of unauthorized or malicious software execution.

Securze

Be Secured, Be Assured.

For business inquiries, **contact us.**

- I find security issues in applications before a hacker finds them and damages the business, thus helping businesses identify and fix security issues at a very early stage.

Harsh Parekh
Founder, Securze

---

www.securze.com	securze
info@securze.com	securze_com
+91 84510 73938	Securze