Is Your Network Performing at Its Best and Secure from Threats?

Network Monitoring and Maintenance Checklist

To keep your business operations running smoothly, maintaining a high-performing and secure network is crucial. Regular monitoring and maintenance help identify potential issues before they disrupt your services, while security audits ensure your infrastructure remains protected against evolving threats. Use this checklist to ensure your network is optimized for performance and security.

1. Network Performance

- ✓ Implement regular monitoring of network traffic, latency, and speed across the organization.
- ✓ Use monitoring tools like SolarWinds, PRTG, or Nagios to track performance metrics.
- ✓ Track network uptime to ensure high availability and quickly identify disruptions.
- ✓ Set up alert systems to notify administrators of performance degradation or outages.
- ✓ Analyze traffic patterns to understand peak usage times and adjust capacity accordingly.

2. Firmware & Hardware Updates

- ✓ Regularly check for firmware updates for network routers, switches, and firewalls to ensure optimal performance.
- ✓ Implement a change management process to update hardware configurations whenever changes are made.
- ✓ Perform routine hardware inspections to ensure network devices are functioning correctly.
- ✓ Schedule maintenance windows to update network hardware without causing disruptions.
- ✓ Ensure firmware rollback procedures are in place in case updates cause issues.

3. Network Security Audits

- ✓ Review and update network security configurations, including firewall rules and intrusion prevention system (IPS) settings.
- ✓ Conduct regular vulnerability scans to identify weaknesses in the network infrastructure and mitigate risks.
- ✓ Ensure all network devices are configured to follow security best practices, including strong access controls.
- ✓ Perform penetration testing to simulate potential attack vectors and evaluate network defenses.
- ✓ Regularly audit user access logs to detect any unauthorized access attempts or abnormal behavior.

4. Bandwidth Optimization

- ✓ Monitor bandwidth usage across the network to identify over-utilization or inefficiencies.
- ✓ Identify bottlenecks and adjust resources accordingly to ensure smooth operation.
- ✓ Set up Quality of Service (QoS) rules to prioritize critical applications and business operations.
- ✓ Implement traffic shaping to optimize bandwidth usage and improve overall network performance.
- ✓ Continuously evaluate and adjust bandwidth allocations based on changing business needs.

5. Wireless Security

- ✓ Ensure Wi-Fi networks are secured with WPA3 encryption for the highest level of security.
- ✓ Conduct regular audits of wireless access points (APs) to detect unauthorized devices and rogue APs.
- ✓ Limit Wi-Fi access based on roles and needs within the organization, using SSID segmentation for different departments or security levels.
- ✓ Review guest network configurations to ensure they are isolated from the corporate network.
- ✓ Regularly update Wi-Fi access point firmware to mitigate vulnerabilities.

6. Speed Tests

- ✓ Run monthly network speed tests across key departments, locations, and critical systems.
- ✓ Compare test results with the agreed service-level agreements (SLA) to ensure network performance meets expectations.
- ✓ Conduct speed tests during peak and off-peak hours to identify network fluctuations or performance issues.
- ✓ Ensure that test results are documented and analyzed for long-term performance trends.
- ✓ Set up automated speed test schedules for ongoing monitoring and trend analysis

By adhering to this comprehensive network monitoring and maintenance checklist, you'll ensure your network is not only performing optimally but also remains secure and reliable, empowering your organization to grow without interruptions. Reach out today!

axiatp