Business Case for Implementing Cisco SD-Access 2.1.2.0

Executive Summary

The implementation of Cisco SD-Access 2.1.2.0 represents a significant opportunity for our organization to enhance its network infrastructure and address several critical challenges. By leveraging the latest features offered by SD-Access, we can improve security, operational efficiency, and reliability, all while future-proofing our network for scalability and emerging technologies. This business case emphasizes the key benefits and features that make Cisco SD-Access 2.1.2.0 a compelling choice for our organization.

Introduction

As technology evolves and our organization's network requirements become increasingly complex, it is imperative that we adapt and invest in solutions that not only address current challenges but also position us for future success. Cisco SD-Access 2.1.2.0 offers a range of advanced features that will significantly strengthen our network infrastructure and provide numerous benefits across various sectors.

Key Features and Benefits

Enhanced Security and Efficiency

Feature: C9000 Series as Policy Extended Node

- **Benefit:** Improved network security and efficiency, especially in complex environments with IoT devices.
- **Impact:** Provides greater visibility and policy management while supporting existing infrastructure.

Operational Convenience

Feature: IP Directed Broadcast

- **Benefit:** Allows remote wake-up of computers, aiding in administrative tasks and reducing energy consumption.
- **Impact:** Particularly beneficial for large organizations like universities and businesses, streamlining administrative operations.

High Availability

Feature: StackWise Virtual Support

- **Benefit:** Increases operational efficiency and redundancy, reducing risks associated with looped topologies.
- **Impact:** Crucial for sectors requiring constant server availability, such as health and public sectors.

Improved Wireless Infrastructure

Feature: Embedded Wireless Support for N+1

- **Benefit:** Enhances the reliability of wireless networks.
- **Impact:** Crucial for organizations needing uninterrupted wireless connectivity.

Efficient Multi-Site Management

Feature: Multisite Remote Border

- **Benefit:** Allows for consistent IP address management across multiple sites.
- **Impact:** Improves network environment security and traffic management.

Future-Proof Infrastructure

Feature: IPv6 Support

- **Benefit:** Ensures scalability and compliance with future network standards.
- **Impact:** Positions the organization to adapt to evolving technology standards without disruptions.

Flexibility

Feature: FlexConnect Over-the-Top Wireless

- **Benefit:** Allows for easier migration to SD-Access while maintaining existing wireless configurations.
- **Impact:** Minimizes disruption during the transition to SD-Access, ensuring business continuity.

Conclusion

The implementation of Cisco SD-Access 2.1.2.0 is a strategic decision that will empower our organization to overcome current network challenges while preparing for the future. The combination of enhanced security, operational convenience, high availability, improved wireless infrastructure, efficient multi-site management, future-proofing, and flexibility makes a compelling case for the adoption of Cisco SD-Access.

By embracing these advanced features, we will strengthen our network infrastructure, boost operational efficiency, reduce risks, and ensure scalability for years to come. Cisco SD-Access 2.1.2.0 aligns with our organization's growth and technology objectives, making it the ideal choice for our network enhancement initiative.

SD-Access Knowledge

Software-Defined Access (SD-Access) is a comprehensive network architecture and solution offered by Cisco that combines software-defined networking (SDN) principles with automation to provide a more scalable, secure, and intelligent network infrastructure. SD-Access simplifies network management, enhances security, and optimizes network traffic. Here are the key components of Cisco SD-Access:

1. Cisco DNA Center:

- **Role:** Centralized Management and Automation Platform
- **Explanation:** Cisco DNA Center is the core management and orchestration platform for SD-Access. It provides a single dashboard for end-to-end network visibility, policy management, and automation. DNA Center simplifies network provisioning, monitoring, and troubleshooting.

2. Cisco Identity Services Engine (ISE):

- **Role:** Network Access Policy Enforcement
- **Explanation:** Cisco ISE is responsible for policy enforcement in SD-Access. It defines and enforces access policies based on user and device identity, ensuring that only authorized users and devices gain network access.

3. Cisco Catalyst Switches (e.g., Catalyst 9000 Series):

- **Role:** Hardware Network Infrastructure
- **Explanation:** Catalyst switches serve as the hardware foundation of SD-Access. These switches support software-defined segmentation and policy enforcement at the access layer, making them a crucial component.

4. Cisco Software-Defined Access Fabric:

- **Role:** Network Fabric
- **Explanation:** The SD-Access fabric is a dynamic network infrastructure created by connecting Catalyst switches. It forms the underlay network for SD-Access and provides connectivity between devices, users, and services.

5. Cisco TrustSec:

- **Role:** Security and Segmentation
- **Explanation:** Cisco TrustSec provides secure network segmentation through the use of scalable group tags (SGTs). It ensures that network traffic is only accessible by authorized users and devices, enhancing network security.

6. Software-Defined Segmentation:

- **Role:** Policy Enforcement

- **Explanation:** SD-Access allows network administrators to define and enforce policies that govern access to network resources based on user, device, and application context. This segmentation is dynamic and adapts to network changes.

7. Cisco DNA Assurance:

- **Role:** Network Monitoring and Analytics
- **Explanation:** DNA Assurance provides real-time monitoring and analytics for SD-Access networks. It uses machine learning to identify and resolve network issues proactively, ensuring optimal network performance.

8. Application Hosting Platform (AHP):

- **Role:** Application Hosting
- **Explanation:** AHP allows the deployment of third-party or custom applications on Catalyst switches within SD-Access. This enables network services and applications to run closer to users and devices.

9. Integration with Cisco DNA Services:

- **Role:** Integration with Other Cisco Services
- **Explanation:** SD-Access integrates with other Cisco DNA services such as DNA Spaces for location-based services, Cisco Umbrella for cloud security, and more to provide additional capabilities and security enhancements.

10. Cisco SD-WAN Integration:

- **Role:** Integration with SD-WAN
- **Explanation:** SD-Access can be integrated with Cisco SD-WAN to extend network segmentation and policy enforcement to the WAN edge, providing end-to-end security and policy consistency.

11. Open APIs:

- **Role:** Programmability and Integration
- **Explanation:** SD-Access offers open APIs that enable integration with third-party applications and orchestration tools, allowing for customization and automation of network processes.

These components work together to create an intelligent, secure, and automated network environment in which policies can be defined based on user and device context, ensuring that network resources are accessed securely and efficiently. SD-Access provides a foundation for organizations to adapt to evolving network requirements and digital transformation initiatives.

Question-based SD-Access awareness

Question 1:

Feature: Cisco DNA Center Question:

"Are you looking for a centralized network management solution that provides a single dashboard for end-to-end network visibility, policy management, and automation?"

Answer: Cisco DNA Center serves as the centralized management and automation platform for SD-Access, offering unified network management capabilities.

Question 2:

Feature: Cisco Identity Services Engine (ISE) Question:

"Is ensuring network security and controlling access based on user and device identity a top priority for your organization?"

Answer: Cisco ISE is a critical feature that enforces policies based on user and device identity, enhancing network security.

Question 3:

Feature: Cisco Catalyst Switches (e.g., Catalyst 9000 Series) Question:

"Is your organization in need of a robust and scalable network infrastructure to support advanced networking features?"

Answer: Cisco Catalyst switches are the hardware foundation of SD-Access, providing the necessary infrastructure for network segmentation and policy enforcement.

Question 4:

Feature: Cisco TrustSec Question:

"Does your organization require strong network segmentation and security to protect sensitive data and resources?"

Answer: Cisco TrustSec enhances network security by providing secure segmentation through scalable group tags (SGTs).

Question 5:

Feature: Software-Defined Segmentation Question:

"Do you prioritize policy-based access control and dynamic network segmentation based on user, device, and application context?"

Answer: Software-Defined Segmentation in SD-Access enables dynamic network segmentation based on policy criteria.

Question 6:

Feature: Cisco DNA Assurance Question:

"Is ensuring optimal network performance and proactively addressing network issues crucial for your organization?"

Answer: Cisco DNA Assurance offers real-time monitoring and analytics, helping identify and resolve network issues proactively.

Question 7:

Feature: Application Hosting Platform (AHP) Question:

"Are you interested in deploying applications closer to users and devices to improve network efficiency?"

Answer: The Application Hosting Platform (AHP) allows for application deployment on Catalyst switches within SD-Access.

Question 8:

Feature: Integration with Cisco DNA Services Question:

"Does your organization require additional capabilities and security enhancements, such as location-based services or cloud security?"

Answer: SD-Access integrates with other Cisco DNA services, providing additional features and security enhancements.

Question 9:

Feature: Cisco SD-WAN Integration Question:

"Is optimizing and securing WAN connectivity a priority for your organization?"

Answer: SD-Access can be integrated with Cisco SD-WAN to extend network segmentation and policy enforcement to the WAN edge.

Question 10:

Feature: Open APIs Question:

"Does your organization value programmability and integration flexibility for network customization and automation?"

Answer: SD-Access offers open APIs, allowing integration with third-party applications and orchestration tools for customization and automation.

These complete questions and feature explanations can assist organizations in assessing their specific network needs and priorities when considering the adoption of Cisco SD-Access.

Network Challenges Without Cisco SD-Access

In today's digital age, organizations rely heavily on their network infrastructure to support business operations, applications, and connectivity. However, many enterprises encounter significant issues and problems in their network environment when they do not have Cisco SD-Access in place. Here are some of the most pressing challenges faced by organizations without SD-Access:

1. Lack of Network Segmentation and Access Control

Issue: Traditional networks often lack robust segmentation, making it difficult to control who has access to specific network resources. This can lead to security vulnerabilities, unauthorized access, and data breaches.

Problem: Without proper segmentation and access control, sensitive data may be exposed, and network resources may be vulnerable to cyber threats, potentially resulting in financial and reputational damage.

2. Complex Network Provisioning and Management

Issue: Managing and provisioning network services in a traditional network can be time-consuming and error-prone. Manual configurations and troubleshooting are often required, leading to operational inefficiencies.

Problem: Complexity in network management increases the risk of misconfigurations, downtime, and delays in service delivery. IT teams struggle to keep up with the demands of a rapidly evolving network landscape.

3. Limited Network Visibility

Issue: Traditional networks lack comprehensive visibility into network traffic and user behavior. This lack of insight makes it challenging to identify and address performance issues, security threats, and compliance violations.

Problem: Without adequate visibility, IT teams struggle to monitor network health, troubleshoot problems efficiently, and make data-driven decisions. This can result in increased downtime and user frustration.

4. Inefficient Troubleshooting and Root Cause Analysis

Issue: When network issues arise, identifying the root cause and resolving problems in traditional networks can be a time-consuming and complex process. Troubleshooting often involves manual tasks and guesswork.

Problem: Inefficient troubleshooting leads to prolonged network outages, increased downtime costs, and frustrated end-users. IT teams face pressure to restore services quickly without a clear understanding of the problem's source.

5. Ineffective Network Security

Issue: Legacy network security models struggle to keep up with evolving cyber threats. Perimeter-based security measures alone are insufficient to protect against advanced attacks.

Problem: Organizations are at risk of security breaches, data loss, and compliance violations. The lack of adaptive and context-aware security measures leaves networks vulnerable to emerging threats.

6. Limited Network Scalability

Issue: Traditional networks often lack the agility and scalability required to accommodate the growing number of devices and applications in modern business environments.

Problem: Scalability limitations hinder organizational growth and digital transformation efforts. Expanding the network to support new users, devices, or locations becomes a complex and costly endeavor.

7. Compliance and Policy Enforcement Challenges

Issue: Enforcing network policies and compliance requirements across a diverse network can be challenging without automation and policy-driven solutions.

Problem: Organizations may fail to meet regulatory and compliance standards, resulting in legal and financial repercussions. Manual policy enforcement is prone to errors and inconsistencies.

In summary, the absence of Cisco SD-Access leaves organizations vulnerable to a multitude of issues, including inadequate security, operational inefficiencies, limited scalability, and compliance risks. Implementing SD-Access addresses these challenges by providing network segmentation, automation, enhanced visibility, and robust security, ultimately enabling organizations to thrive in a connected world.

Cisco SD-Access Implementation Plan for Company ABC

Phase 1: Pre-Deployment Assessment

1.1 Define Objectives and Goals for Company ABC

- Company ABC's primary objectives include:
  - Modernizing network infrastructure for improved scalability and agility.
  - Enhancing network security through segmentation and policy enforcement.
  - Simplifying network operations and management.
  - Ensuring seamless connectivity for 1000 users.

1.2 Assemble Company ABC Project Team

- The project team at Company ABC consists of:
  - Network Architects
  - Network Engineers
  - Security Experts
  - IT Administrators
  - User Training Specialists

1.3 Assess Current Network Environment at Company ABC

- Conduct a comprehensive assessment, including:
  - Review of existing network infrastructure and devices.
  - Evaluation of network performance and scalability.
  - Identification of security and compliance gaps.

1.4 Define Network Policies and Security Requirements for Company ABC

- Define network policies and security requirements, specifying access controls, segmentation, and compliance standards.

Phase 2: Infrastructure Setup

2.1 Acquire Cisco SD-Access Licensing for Company ABC

- Procure the necessary Cisco SD-Access licenses and hardware for Company ABC's network transformation.

2.2 Set Up Cisco SD-Access Fabric for Company ABC

- Deploy Cisco SD-Access fabric, including Catalyst switches and DNA Center appliances, and configure network profiles and policies.

2.3 Configure Network Connectivity for Company ABC

- Ensure network connectivity is optimized for Cisco SD-Access, including proper routing, VLANs, and VPN configurations.

Phase 3: Device Onboarding and Enrollment

3.1 Choose Device Enrollment Methods for Company ABC

- Implement device enrollment methods, such as Plug and Play (PnP) or manual onboarding, based on Company ABC's device types and requirements.

3.2 Create Device Profiles for Company ABC

- Configure device profiles and policies to enforce security settings, Quality of Service (QoS), and segmentation.

3.3 Communicate Device Enrollment Process at Company ABC

- Prepare clear instructions and user guides for Company ABC employees, explaining the device enrollment process and its benefits.

3.4 Pilot Device Onboarding at Company ABC

- Initiate a pilot device onboarding with a representative group of users and devices to test the process and gather feedback.

Phase 4: Configuration and Policies

4.1 Define Network Segmentation for Company ABC

- Define segmentation policies to logically separate network traffic, ensuring that sensitive data is isolated from less critical traffic.

4.2 Configure Network Access Policies for Company ABC

- Implement network access policies that govern user and device access, based on roles, locations, and compliance requirements.

4.3 Implement Security Policies for Company ABC

- Configure security policies, including firewall rules, Intrusion Prevention System (IPS), and content filtering, to enhance network security.

4.4 Deploy Wireless LAN and IoT Policies for Company ABC

- Define policies for wireless LANs and IoT devices, ensuring secure and efficient connectivity.

4.5 Define Policy Enforcement for Company ABC

- Specify policy enforcement mechanisms, including TrustSec, to ensure that policies are consistently applied across the network.

Phase 5: Security and Monitoring

5.1 Implement Threat Detection and Response for Company ABC

- Set up threat detection and response solutions, including Cisco Stealthwatch, to monitor network traffic for security threats and anomalies.

5.2 Configure Network Monitoring and Alerts for Company ABC

- Implement network monitoring and alerting systems to proactively detect and respond to network issues and security incidents.

5.3 Set Up Compliance Monitoring for Company ABC

- Configure compliance monitoring to ensure that the network adheres to security and regulatory standards.

Phase 6: User Training and Support

6.1 Provide User Training at Company ABC

- Offer comprehensive training sessions and documentation to educate Company ABC employees on SD-Access features and best practices.

6.2 Offer Technical Support for Company ABC

- Establish a dedicated helpdesk and support team to assist users with network-related issues and questions, ensuring a smooth transition to SD-Access.

Phase 7: Deployment and Rollout

7.1 Pilot Rollout at Company ABC

- Initiate a pilot rollout with a select group of users and devices to validate configurations and gather feedback.

7.2 Full Deployment at Company ABC

- Gradually expand the SD-Access deployment to cover all 1000 users and devices, monitoring for any issues and providing additional training and support as needed.

7.3 Post-Deployment Testing and Optimization for Company ABC

- Conduct thorough post-deployment testing to ensure all devices comply with policies, segmentation is effective, and the network is secure and performant.

SD-Access Test Case

Test Case Overview

Objective: To verify the functionality of all key features of Cisco SD-Access in Company ABC's network environment.

Test Environment:

- Hardware: Cisco Catalyst switches (models XYZ).
- Software: Cisco DNA Center version XYZ.
- Network Topology: Include a description of Company ABC's network layout.

Test Plan

1. Device Onboarding

Test 1.1: Device Enrollment

- **Actions**:
  - Enroll a set of devices using Plug and Play (PnP) and manual onboarding methods.
  - Verify device profiles and configurations.
- **Expected Outcomes**:
  - Devices should be successfully enrolled and appear in Cisco DNA Center.
  - Device profiles and configurations should match predefined policies.

Test 1.2: Device Authentication

- **Actions**:
  - Attempt to connect unauthorized devices to the network.
- **Expected Outcomes**:
  - Unauthorized devices should be denied network access.
  - Authorized devices should successfully authenticate and gain network access.

2. Network Segmentation

Test 2.1: Segmentation Policies

- **Actions**:
  - Send traffic between devices in different segments.
- **Expected Outcomes**:
  - Traffic between devices in separate segments should be blocked.

  - Traffic within the same segment should be allowed.

Test 2.2: User Segmentation

- **Actions**:
  - Assign users to different roles and observe the network segment they are placed in.
- **Expected Outcomes**:
  - Users should be placed in the correct segments based on their roles and access policies.

3. Network Policies

Test 3.1: Access Policies

- **Actions**:
  - Apply different access policies to devices and users.
- **Expected Outcomes**:
  - Devices and users should have the appropriate level of access based on policy configurations.
  - Policy enforcement should be consistent.

Test 3.2: Security Policies

- **Actions**:
  - Generate network traffic that violates predefined firewall rules and security policies.
- **Expected Outcomes**:
  - Unauthorized traffic should be blocked as per security policies.
  - Intrusion Prevention System (IPS) should detect and log security violations.

4. Wireless LAN and IoT

Test 4.1: Wireless LAN Policies

- **Actions**:
  - Connect and authenticate wireless devices.
- **Expected Outcomes**:
  - Wireless LAN policies should provide secure and efficient wireless connectivity.
  - Devices should seamlessly transition between wired and wireless access.

Test 4.2: IoT Device Integration

- **Actions**:

- Integrate IoT devices into the SD-Access fabric.

- **Expected Outcomes**:
  - IoT devices should be correctly segmented and monitored.
  - Policies for IoT devices should be enforced as specified.

5. Policy Enforcement

Test 5.1: TrustSec Implementation

- **Actions**:
  - Apply TrustSec policy changes and observe their impact.
- **Expected Outcomes**:
  - TrustSec policy changes should be consistently applied across the network.
  - Integration with other security measures should work effectively.

6. Threat Detection and Response

Test 6.1: Threat Detection

- **Actions**:
  - Generate simulated security threats and anomalies.
- **Expected Outcomes**:
  - Cisco Stealthwatch or similar solutions should detect and alert on security threats and anomalies in network traffic.

7. Network Monitoring and Alerts

Test 7.1: Network Monitoring

- **Actions**:
  - Monitor real-time network performance and security using monitoring tools.
- **Expected Outcomes**:
  - Administrators should have visibility into network status, device health, and security events.

8. Compliance Monitoring

Test 8.1: Compliance Checks

- **Actions**:
  - Assess network compliance against predefined policies.

- **Expected Outcomes**:
    - The network should adhere to security and regulatory standards as specified in policies.

Test Execution

- Execute each test case with predefined test scenarios.
- Document the test results, including any issues, anomalies, or deviations.
- Provide a summary of the test outcomes.

SD-Access implementation sample question and answers

Project Scope and Objectives:

1. What are the primary objectives and goals of implementing Cisco SD-Access in your organization?
2. What specific network infrastructure modernization and security improvements are you aiming to achieve with SD-Access?
3. How does Cisco SD-Access align with your organization's long-term IT and business objectives?
4. What is the expected timeline for the implementation of Cisco SD-Access, and are there any critical deadlines?

Current Network Assessment:

5. Can you provide an overview of your current network infrastructure, including the types of network devices and their configurations?
6. Have you conducted a network assessment to evaluate the performance, scalability, and security of your existing network?
7. Are there any known network performance bottlenecks or security vulnerabilities that need to be addressed with the SD-Access implementation?
8. What are the critical applications and services running on your existing network?

Infrastructure Requirements: 9. What is the size and scale of your network in terms of the number of users, devices, and locations?

10. Do you have a clear understanding of your network's access, distribution, and core layers?
11. Are there any specific hardware requirements for SD-Access, such as Catalyst switches and routers?
12. What types of network access points (wired, wireless) need to be integrated into the SD-Access solution?

Security and Compliance: 13. What are your organization's specific security requirements and compliance standards that must be met by Cisco SD-Access?

14. Are there any data privacy regulations or industry-specific compliance requirements that need to be considered?
15. How do you plan to enforce access control policies and segmentation to enhance network security?

Network Policies and Segmentation: 16. Have you defined your network policies, including user access policies, device onboarding, and network segmentation requirements?

17. What is the desired level of network segmentation, and how will it be configured within the SD-Access fabric?

18. Are there specific user roles and groups that need customized access policies?

Integration with Existing Systems: 19. Are there any existing network management and monitoring tools that need to be integrated with Cisco SD-Access?

20. How will user authentication and authorization be handled, and do you plan to integrate with identity providers such as Active Directory?

21. Do you have existing security solutions (e.g., firewalls, intrusion detection systems) that need to be integrated with SD-Access for threat detection and prevention?

User Training and Change Management: 22. What is your plan for user training and change management to ensure a smooth transition to SD-Access?

23. How will you communicate changes and new network access procedures to end-users and IT staff?

Disaster Recovery and Redundancy: 24. What is your disaster recovery plan for SD-Access, including data backup, failover mechanisms, and disaster response procedures?

25. Are there redundancy requirements for critical network components in the SD-Access fabric?

Budget and Resources: 26. Have you allocated a budget for the Cisco SD-Access implementation, including hardware, software, and professional services?

27. What internal and external resources (e.g., IT staff, Cisco certified professionals) will be involved in the implementation?

28. Are there any potential cost-saving opportunities or cost optimization strategies you'd like to explore with SD-Access?

Testing and Validation: 29. How do you plan to validate and test the Cisco SD-Access solution to ensure it meets performance and security expectations?

30. Will there be a phased approach to testing and deployment?

Documentation and Knowledge Transfer: 31. What documentation and network diagrams are needed to ensure proper SD-Access management and maintenance?

32. How will knowledge transfer and training be provided to your IT team for ongoing SD-Access management?

Support and Maintenance: 33. What are your expectations for ongoing support and maintenance of the SD-Access infrastructure, and do you require a service-level agreement (SLA) with Cisco or a third-party provider?

34. How will software updates, patches, and security updates be managed for the SD-Access components?

Performance Metrics and KPIs: 35. Have you defined key performance indicators (KPIs) and metrics to measure the success and performance of Cisco SD-Access?

Sample Answers

Project Scope and Objectives:

1. *Objectives:* The primary objectives of implementing Cisco SD-Access in our organization are to enhance network security, improve network agility and scalability, and simplify network management through automation.
2. *Infrastructure Modernization:* We aim to modernize our network infrastructure to support the growing number of devices and applications, reduce security risks, and streamline network operations.
3. *Alignment with Goals:* Cisco SD-Access aligns with our long-term IT and business goals by enabling a more flexible and secure network infrastructure that can adapt to changing business needs.
4. *Timeline:* We expect the implementation to be completed within a 12-month timeline, with phased deployments to minimize disruption.

Current Network Assessment: 5. *Current Infrastructure:* Our current network infrastructure consists of a combination of Catalyst switches, routers, and wireless access points with various configurations.

6. *Network Assessment:* We have conducted a network assessment to identify performance bottlenecks and vulnerabilities, including issues related to user access and network segmentation.
7. *Performance Issues:* Performance issues, such as network congestion and slow application response times, have been identified and need to be addressed.
8. *Critical Applications:* Critical applications include ERP systems, VoIP, video conferencing, and cloud-based services.

Infrastructure Requirements: 9. *Network Size:* Our network serves approximately 5,000 users across multiple office locations and data centers.

10. *Hardware Requirements:* We plan to deploy Cisco Catalyst 9300 switches for access and Cisco Nexus 9500 switches for the core network.
11. *Network Access Points:* We need to integrate both wired and wireless network access points into the SD-Access solution.

Security and Compliance: 13. *Security Requirements:* Our specific security requirements include network segmentation, access control, threat detection, and compliance with industry-specific regulations (e.g., HIPAA).

14. *Data Privacy:* We must comply with GDPR regulations, which require stringent data privacy and access control measures.
15. *Access Control:* Access control policies will be enforced through Cisco TrustSec to enhance network security.

Network Policies and Segmentation: 16. *Network Policies:* We have defined network access policies for different user roles and groups, including guest access, employees, and administrators.

17. *Segmentation:* Network segmentation will be implemented to isolate sensitive data and ensure that users have access only to authorized resources.
18. *User Roles:* User roles include standard users, power users, and network administrators with varying levels of access.

Integration with Existing Systems: 19. *Existing Tools:* We use Cisco Identity Services Engine (ISE) for user authentication and authorization, which will be integrated with SD-Access.

20. *Security Solutions:* Cisco Firepower Threat Defense (FTD) is currently in use for intrusion prevention, and it will be integrated into SD-Access for threat detection.
21. *Identity Providers:* Integration with Microsoft Active Directory is planned for centralized identity management.

User Training and Change Management: 22. *User Training:* We plan to provide training sessions for IT staff and end-users to familiarize them with the new network access procedures.

23. *Communication:* Regular communications will be sent to inform users about upcoming changes and provide guidance on using the new network.

Disaster Recovery and Redundancy: 24. *Disaster Recovery:* Our disaster recovery plan includes regular data backups, redundant network paths, and a failover strategy to ensure business continuity.

25. *Redundancy:* Critical network components will have redundant configurations to minimize downtime in case of hardware failures.

Budget and Resources: 26. *Budget Allocation:* A budget of $2 million has been allocated for the Cisco SD-Access implementation, covering hardware, software, professional services, and training.

27. *Internal Resources:* Our internal IT team will be actively involved, and we plan to hire Cisco-certified professionals for specific tasks.
28. *Cost Optimization:* We aim to optimize costs through efficient resource utilization and by exploring licensing options that align with our needs.

Testing and Validation: 29. *Validation Process:* A comprehensive testing plan has been developed to validate network functionality, security policies, and performance.

30. *Phased Deployment:* Testing will occur in phases, starting with non-critical areas and gradually extending to critical network segments.

Documentation and Knowledge Transfer: 31. *Documentation:* Detailed network documentation, including diagrams, configurations, and policies, will be updated and maintained.

32. *Knowledge Transfer:* IT staff will receive hands-on training, and comprehensive documentation will be provided for reference.

Support and Maintenance: 33. *Support Expectations:* We expect to have an SLA with Cisco for ongoing support and maintenance of SD-Access components.

34. *Updates and Patches:* Software updates, patches, and security updates will be regularly applied to keep the infrastructure secure and up-to-date.

Performance Metrics and KPIs: 35. *KPIs:* Key performance indicators include network latency, user authentication times, security incident response times, and network utilization.