AIR TRAFFIC AND NAVIGATION SERVICES SOC. LTD

REPUBLIC OF SOUTH AFRICA

Network Access Control Project

[ATNS/IT/RFP0018/2023/24/NAC]

TECHNICAL SPECIFICATION

Version 1.0

MARCH 2024

The information contained within this document is confidential to ATNS in all respects and it is hereby acknowledged that the information as provided shall only be used for the preparation of a response to this document. The information furnished will not be used for any other purpose than stated and that the information will not directly or indirectly, by agent, employee or representative, be disclosed either in whole or in part, to any other third party without the express written consent by the Company or its representative.

Table of Contents

1. Introduction

1.1 Project Purpose

Background

With the rise in cyber-attacks globally and with many organizations falling victim to hackers, ATNS needs to continuously improve its defence measures against Information Security threats. The Network Access Control (NAC) is a critical tool for any organisation to implement to significantly improve its security posture.

Gartner, which is one of the leading ICT research organisations, has highlighted the need for ICT networks to include a NAC solution due to its ability to enable organizations to implement policies for controlling access to corporate infrastructure by both user-oriented devices and Internet of Things (IoT) devices.

1.2 Scope of Work

The scope of work for the NAC project includes the following:

1.2.1. System Design

- Design the architecture and components of the NAC system.
- Defining where the integration points with existing network infrastructure.

1.2.2. Implementation

- Procuring and configuring hardware and software components for the NAC system.
- Developing custom scripts or integrations, where necessary.
- Testing and deploying the NAC system in a controlled manner.
- Policy Development for NAC system:

1.2.3. Access policy creation

- Defining compliance checks and security rules that are in line with ATNS's policies. Polices will include network access control, BYOD, Guest access, Posture assessment and TACACS+

1.2.4. User Training

- Service Provider to provide training sessions for network administrators and support staff on using the NAC system effectively.

1.2.5. Monitoring and Reporting

- Implementing real-time monitoring of network access attempts (Posture Assessment) and device compliance this will be monitored by the InfoSec team and they will log requests for assistance for desktop and server team if needed.
- Generating comprehensive reports for tracking access history and security incidents this will be reviewed regularly in weekly operations meeting for any remediations needed.

1.2.6. Maintenance and Support

- Establishing an ongoing maintenance plan for the NAC system with a service provider.
- Providing technical support for system users and administrators this will be done as and when needed but ATNS will take ownership of the system and do majority of the work so they able to use the system effectively in managing their environment.

2. Summary of requirements

2.1 The Environment

The NAC infrastructure will be capable of operating within the specified temperature range of 0°C to 35°C to ensure reliable performance under varying environmental conditions.

The hardware will comply with energy efficiency standards, such as Energy Star, to minimize power consumption and promote environmental sustainability.

Adequate ventilation and cooling measures will be provided in the server rooms to prevent overheating of devices.

2.2 The Project objective

The objective of the project is to implement a NAC system in order to enhance network security, improve compliance with organizational policies and regulations, streamline network management, and provide real-time visibility and reporting capabilities.

3. Systems Overview

The NAC solution needs to be based on the following:

3.1 Users’ devices and roles on the network, use of different levels of user licencing models for different user levels, i.e. Guest users and standard user licencing.

3.2 The solution needs to evaluate that user’s machines are compliant with ATNS’s security policies.

3.3 Enforce security polices by blocking, isolating, and repairing noncompliant machines.

3.4 Provide easy and secure guest access to vendors and dignitaries that visit the sites.

3.5 Audit and report who is on the ATNS the network.

3.6 Clustering based on virtual and physical servers.

4. Project Overview

The NAC project is a critical initiative aimed at enhancing the security and management of ATNS network. By implementing a robust NAC solution, the following objectives will be achieved:

4.1. Strengthening of network security by controlling and monitoring access to network resources.

4.2. Compliance with ATNS policies and relevant regulations.

4.3. Streamlining of network management through automation and policy enforcement.

4.4. Real-time visibility into network access and security posture.

4.5. Empowerment of network administrators and users with an intuitive and user-friendly system.

4.6. Native integration into ATNS existing network by use of physical and virtual clustering.

5. System Requirements for NAC System

5.1 Authentication Methods:

- Support for various authentication methods, including username/password, two-factor authentication (2FA), digital certificates, and integration with existing Azure into LDAP and Active Directory

5.2 Device Profiling and Authorization:

- Profiling and classification of devices based on attributes like device type, OS version, antivirus status, etc.
- Authorization of devices based on predefined policies and dynamic access control.

5.3 Policy Enforcement:

- Implementation of security policies to enforce role-based access controls, restricting users and devices to specific resources.
- Automated quarantine or blocking of non-compliant devices until they meet security standards.

5.4 Integration with the existing newly upgraded Infrastructure:

- Seamless integration with existing network infrastructure, i.e. switches, routers, firewalls, and authentication servers.
- The solution should also be able to integrate with the SIEM solution in order to perform post connect policies.

5.5 Scalability and Performance:

- Support for many concurrent users and devices without performance degradation.
- High availability and redundancy to ensure system reliability this will need to be spanned over two data centres at ATNS.

5.6 User-Friendly Interface for ATNS IT administrators:

- Intuitive web-based administration interface for configuration and management to be used for administrators.
- Self-service options for users to register and manage their devices (BYOD) this will help streamline the onboarding of devices and users on the network.

5.7 Comprehensive Monitoring and Reporting to be used by IT:

- Real-time monitoring of network access attempts, user activities, and device compliance status.
- Generation of detailed reports to track access history, compliance status, security incidents, and potential

threats.

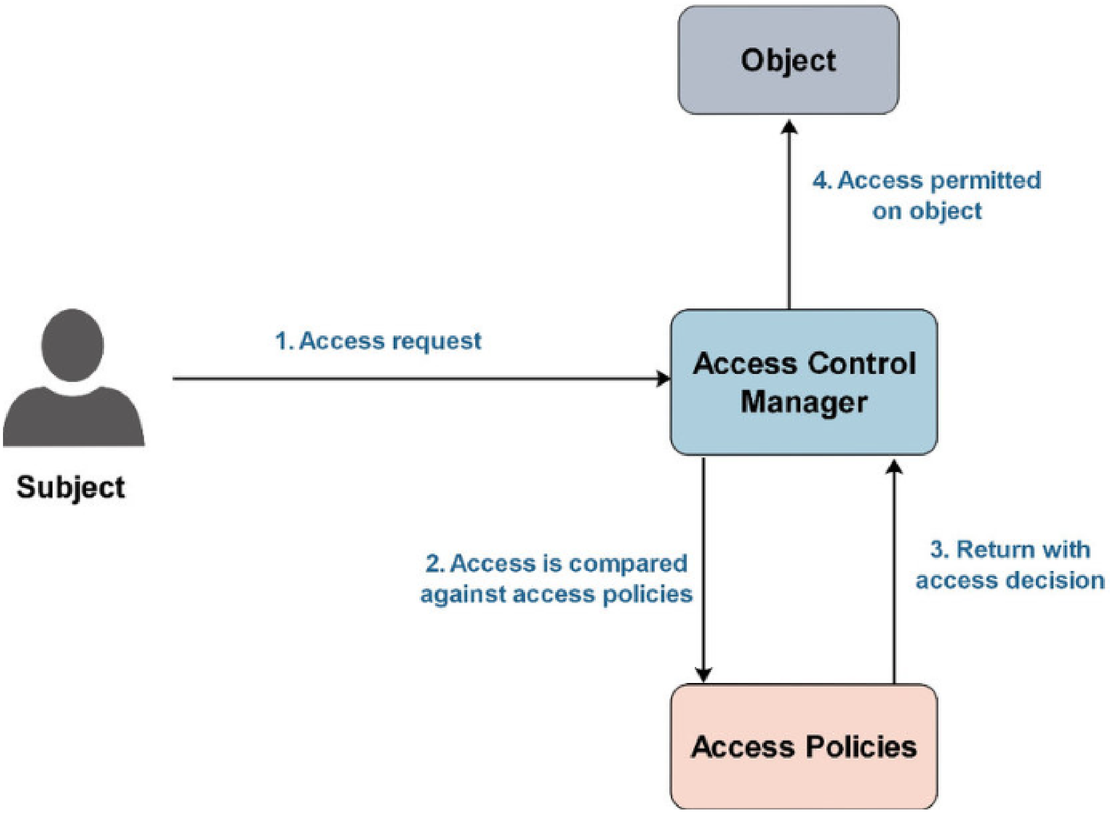
5.8 Native integration with ATNS Guest portal:

- The NAC will need to integrate with different levels of user licencing model's examples are the Guest user model and User licencing model.

6. System Architecture

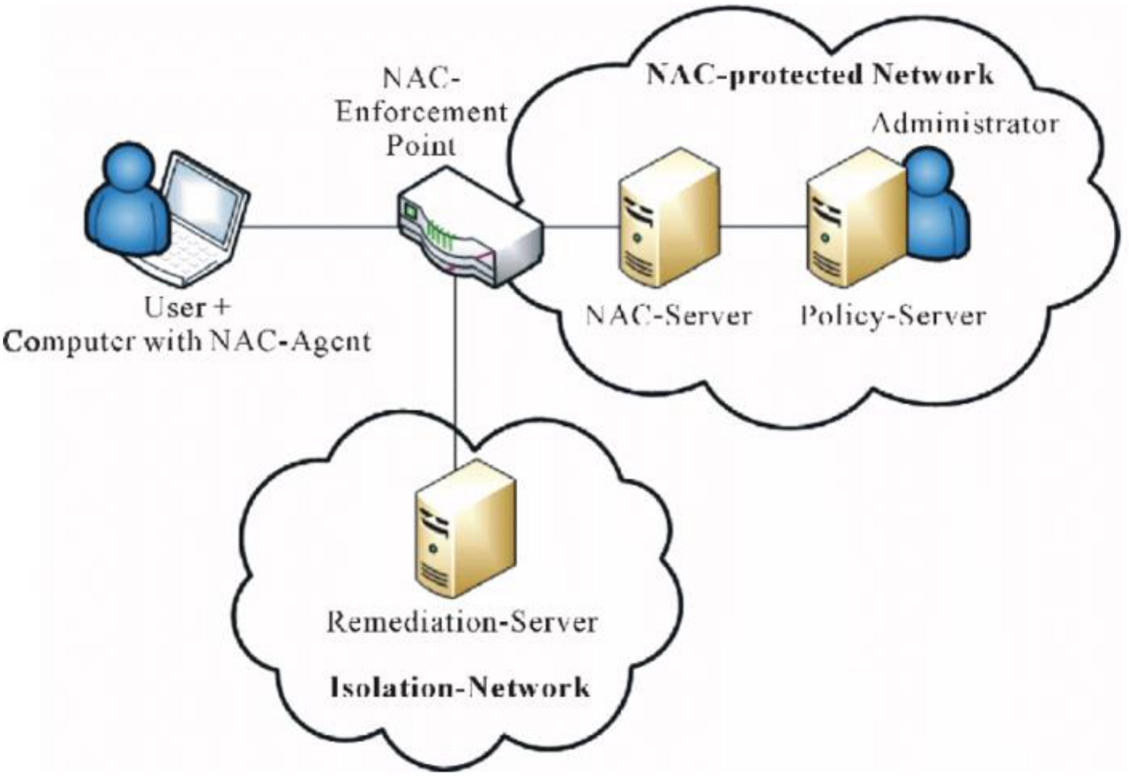
6.1. Access Management

The diagram below shows the flow of an access control policy. It shows the block diagram of how a user gets access based on an access request.


Object
4. Access permitted on object
1. Access request
Access Control Manager
Subject
2. Access is compared against access policies
3. Return with access decision
Access Policies

6.2. Logical Architecture

Figure below is the NAC solution overview to be used to dynamically provision each user and endpoint device. This will entail authentication, endpoint compliance, remediation, and policy enforcement functions in the process of validating user identity and security posture of host devices before allowing access to the ATNS network.



6.3. Redundancy and High Availability:

Redundancy will be built in at Bruma and OR Tambo (Data centers) with one physical device and one virtual device respectively at the two hub sites. The solution will have 2 devices at the two main sites. The physical will be for administration and policy management and virtual will be for monitoring.

High availability will be managed also by splitting the solution between the two sites to manage the user loads for pre and post administration.

7. Specification

ATNS will be looking at a hybrid NAC solution for its two main sites:

7.1. ATNS Bruma: 2 appliances

7.1.1 Administration and policy appliance: physical appliance

7.1.2 Monitoring appliance: Virtual Appliance

7.2 ATNS O R Tambo: 2 appliances

7.2.1. Administration and policy appliance: physical appliance

7.2.2. Monitoring appliance: Virtual Appliance

8. Hardware Specifications

8.1 Physical appliances

The physical appliances shall meet the minimum specification below.

- Designed for medium deployments.
- Processor: Intel, 2.1GHz or equivalent
- Memory: 32GB (2 x 16GB)
- Hard disk: 1 x 600 GB, 12Gb SAS 10K RPM SFF HDD
- Hardware RAID: Level 0
- Network interfaces: 2 x 10Gbase-T, 4 X 10GE SFP

8.2 Virtual appliances

- The virtual appliance shall operate on VMWare ESXI 7.x with recommended 16vCPU and 32GB memory.

9. Software Performance Requirements

9.1 Ensure the NAC equipment is equipped with the latest stable and secure firmware or operating system from the respective vendor.

9.2 Ensure that one or more nodes are connected in a cluster (distributed system). This will support failover for administration and monitoring activities and for processing to be distributed across the policy nodes.

9.3 ATNS will require a small to medium deployment for load sharing purposes.

9.4 The appointed service provider will need to provide the software licences.

10. System Features

ATNS requires two fundamental NAC methods, i.e. pre-admission and post-admission.

10.1. Pre-admission: It occurs before network access is given when a user or endpoint device begins a request for network access. A pre-admission network control assesses the access request and only permits network access if the requesting device or user can demonstrate compliance with corporate security policy and authorization to enter the network.

10.2. Post-admission: Post-admission network access control occurs when a user or device attempts to enter a different portion of the network. If the pre-admission network access control fails, the post-admission network access control may restrict lateral movement inside the network and reduce cyber-attack damage. Upon each request to transfer to a new network segment, a user or device must re-authenticate.

10.3. Provide policy-based automation to deliver services to the network based on ATNS's business priority and to simplify device deployment. Zero-touch device provisioning and software image management features to reduce device installation or upgrade time.

11. Scalability Requirements

11.1 The NAC deployment will need to support 5000 minimum concurrent active sessions with up to 15 000 concurrent connections.

11.2 The request for a hybrid, clustered solution will allow for future growth if needed but with the current specifications we will manage the growth for the next 5 to 8 years.

12. Environmental Conditions

The equipment will be operational only in the data centres (Bruma and FAOR)

- The systems shall be able to operate properly under the following temperature and relative humidity:
- Temperature: -5 ^{o}C to +30 ^{o}C
- Relative Humidity: up to 60%

13. Technical Training

13.1 The technical training shall be provided for 5 Technical resources.
13.2 The following technical training should be included over the shoulder training.

14. Warranty

The service provider shall provide a 5-Year next business day OEM Warranty as part of the solution to cover hardware related failures.

15. Environmental Sustainability requirements

Disposal and data destruction will be in accordance with ATNS's procedures. This will include the destruction and removal of ATNS passwords, configurations, and IP addresses.