Emppu Sieranen

Improving Remote User Environment Currently Provided for End Users and Service Providers

Metropolia University of Applied Sciences

Master’s Degree

Information Technology

Master’s Thesis

2 February 2020

Author Title Number of Pages Date	Emppu Sieranen Improving Remote User Environment Currently Provided for End Users and Services Providers 45 pages 2 February 2020
Degree	Master of Engineering
Degree Programme	Information Technology
Instructor	Janne Salonen, Principal Lecturer

This Master's Thesis was produced for Helsinki Region Environmental Services authority HSY. The thesis presents the current remote access system and a possible solution to how it can be improved. The thesis also discusses the benefits and issues of the solution to add a critical approach to it.

The company and working environment is described to establish the environment and who are the operators and stakeholders within it.

Guidelines from the security background are discussed as well as the technical structure of the remote access environment, piecing each component into an overview diagram. The business problem is explained together with the identity management process and how it positions in the technical environment.

The study provides an explanation about what the solution for improvement is and the available data is utilized to help establish the contents of the remote access environment. How the data can be organized in a way that supports the solution is explained. Reducing the number of identities present in the system is described. How the solution would impact the technical environment and the process of identity management of remote users is explained. The results are discussed together with further development possibilities.

The main goal of the study is, presenting the case situation and how it can be improved through changing the technical environment together with positive impacts on the remote user identity management process and reduction of costs. The thesis explains how the data contents can be organized in a way to achieve the desired resulting setup. The paper succeeds in laying the groundwork for the company to engage in a possible implementation project. The paper does not, however, present or suggest any specific technology platforms that should be used, achieving a neutral position in the presentation.

Keywords: Remoting, Access control, IAM, Process design

Contents

List of Abbreviations

NIST	The National Institute of Standards and Technology
VAHTI	Government Information Security Management Board
AAA	Accounting, Authentication, Authorization
VPN	Virtual Private Network
ACL	Access Control List
IPv4	Internet Protocol version 4
IAM	Identity Access Management
RBAC	Role-based Access Control
AD	Active Directory
LDAP	Lightweight Directory Access Protocol
API	Application Programming Interface
SD	ServiceDesk
CMDB	Configuration Management Database
SG	Security Groups. Can provide an efficient way to assign access to resources in a network.
TFA	Two-Factor Authentication. Adds another layer of security to a login process. For example, adding biometric verification and using a password.

1 Introduction

The thesis presents a solution and describes how the solution can be used to improve remote user access management and the process of identity management of remote users via changing the technical environment. As background information, related technologies and their functions are described and include selected security frameworks. The company's identity management process is described as well as the technical components to build an overview of the remote user system. The research question can be formed as:

"How to improve remote user identity management in remote user environment with multiple networks and access requirements for third-party service providers operating within those networks via changing the technical environment and through user configuration analysis?"

This study was commissioned by Helsinki Region Environmental Services Authority municipal organization, HSY. HSY produces waste management and water services, as well as provide information on the Helsinki Metropolitan Area and environment. HSY helps inhabitants to act for a better environment. [1]

Data analysis was performed against remote user configuration content and as such gives information which can be used in a separate implementation project. Processed data was organized into the structure presented. Impacts in reducing operational cost in identity management is discussed in the benefits section. The starting source data for the analysis was provided from the device receiving remote user connections. The data for analysis and process was exported and put into a work file, containing user and network access information. The thesis describes how this data was approached. The data structure design was assisted via adding metadata. This information was based on stakeholder discussions and different documentation sources. Organizational demands were considered together with stakeholders. The company's goal was to lay a groundwork in understanding the situation and the study presents a possible solution based on these demands together with used background resources.

The scope of the study does not include recommendations for any specific technology platforms but considers the current situation when mentioning specific technologies or products.

1.1 Organization and Values

Helsinki Region Environmental Services Authority or HSY produces water and waste -management services for citizens of Helsinki metropolitan area in Finland and environmental information to help act for a better environment.

Information Technology department (ICT) and their services is a part of HSY organization and responsible for managing IT information e.g. contracts, service provider coordination in various projects and participates in developing the ICT architecture, infrastructure and processes within. The ICT-department is also responsible for the company's information security. The department's goal is to provide a working ICT environment that supports different stakeholders in the company reach their goals efficiently, securely and to utilize new benefits of digitalization.

1.2 Environment and Users

The framework here is in the field of environmental services and as such the ICT-infrastructure can consist of multiple different systems. These systems can be operational systems that support the main business and operations of water and waste management and supportive systems such as finance management and human resources (HR) -systems.

The working environment consists of different service providers and company stakeholders that operate or are responsible for the systems. Stakeholders that use remote connections are the company's own stakeholders such as project managers, system owners, key users and end users. In addition to the company stakeholders there exists third-party service providers who also require the remote access environment provided by the company, because several of the destination systems are located within the company premises and operated networks. These systems are a combination of different networks, devices, applications and resources like documents. Third-party service providers can have administrative, development, research or user domain tasks they need to perform on the destination systems. To provide the remote access, a companywide infrastructure for remoting is provided by a third-party service provider. Granting remote access includes managing different identities in this environment, and this belongs into processes of the ServiceDesk (SD). The environment with different stakeholders and user categories is presented in Figure 1.

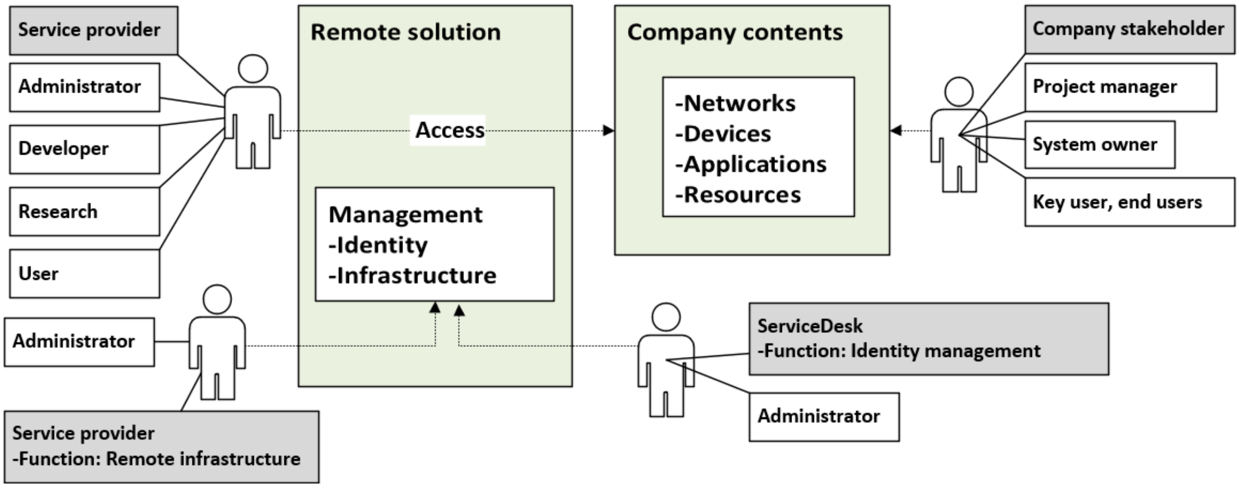

Figure 1 Stakeholders and Service providers

Figure 1 describes each stakeholder in relation to the remote environment and destination company owned contents. Third-party service providers use the remote solution. Management of the remote environment is split to identity and infrastructure management. Here the infrastructure is managed by the service provider, but identity management is done by both the service provider and company ServiceDesk, this is described with a notation called function. Stakeholder examples are noted on the right side of Figure 1.

1.3 Motivation

Being able to connect remotely increases flexibility and availability of human resources since not everything requires the person to be onsite to do a task. The remote use of different systems is growing even for systems that have existed for longer periods of time and because of it, the management should also be designed to support a comprehensive process. [2]

The motivation to engage in this the present study for the company lies in learning to understand what the current overall situation is as to the service provided for remote users. How their identities are currently being managed and how this could be improved. The motivation is to find out the composition of the remote user management process and how it can be improved. An important goal also is to reduce the amount of operational cost in the environment.

Another goal is to implement part of the identity management process into the service function provided by the SD, reducing the number of different operators that need information exchange to complete tasks.

After establishing basic information brief background information relating to information security is presented in Chapter 2. Chapter 3 presents the technologies that are utilized or present in the remote environment and describes the guidelines for select security framework sections. Chapter 4 describes the remote environments components and builds up into an overview diagram to be used later. The business problem and the current process for management operations is explained in Chapter 5 and Chapter 6 presents the solution with the data that was analysed to help find the solution and understand the structure of current user configuration. Chapter 7 describes the solution impacts and considers benefits and issues of the solution. Chapter 8 discusses the results, analysis reliability and further development options. The final thoughts are summarized in Chapter 9

2 ICT Security

For security background knowledge there exists a lot of different literature resources and guidelines. For this Thesis certain frameworks were selected to provide a security framework and support the study from the information security viewpoint. Sections from VAHTI were utilized, because of its relevance in conducting ICT security in Finland in the public sector and governmental organizations. NIST was also selected for it provides guidelines that have their background on several different security standards. The study also discusses managing identities and access rules so the framework for *Authentication, Authorization and Accounting (AAA)* was selected regarding *Authentication* and *Authorization*.

2.1 VAHTI

VAHTI, the Government Information Security Management Board is administrated and coordinated by the Ministry of Finance in Finland and works as a steering group to develop Finnish ICT security. VAHTI maintains and provides instructions and guidelines for information and technology security. Users for the instructions are Finnish public sector and government organizations but it can be utilized by other organizations to support their own security policy. VAHTI offers comprehensive instructions for a wide area on information security. [3] VAHTI is referred in this thesis to support the information security view since the case company is part of the public-sector service provider. Selected VAHTI guidelines are presented in the guidelines for the security section Chapter 4 “Technologies, concepts and security guidance”.

2.2 NIST

The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce founded in 1901. NIST provided standards are utilized in a large range of technologies from smallest of technologies to the largest and most complex solutions. It is a non-regulatory government agency and focusing on U.S. -based organizations. NIST also provides guidance documents and recommendations through Special Publications (SP) 800-series. The offered standards are endorsed by the U.S. government, because they contain security best practice control in various industries like widely adopted NIST standard. It can be used by organizations that require stringent security measures. [4]

NIST SP 800-113 is selected to add support in the field of best practises when discussing different VPN solutions. NIST offers guidance and recommendations through its SP-800 series. From 800-113 the present study selected its supporting aspects seen relevant. As stated by the Federal Trade Commission there is no one-size-fits-all approach to managing cybersecurity and risks. Paper 800-113 and other guidelines by NIST should be used more as a consideration as they offer a compilation of best practices. [5]

2.3 Authentication, Authorization and Accounting (AAA)

Authentication, authorization and accounting (AAA) is a term for a security framework to provide control over access to computer resources, enforcing access and auditing policies. These processes as a combination provide an efficient network security and management. AAA security is meant to enable dynamic configuration of authorization level and authentication by creating a method list for different services. [6]

2.3.1 Authentication

Authentication is the first part of the process and describes the identity of an individual accessing certain applications or networks. This identity ensures whether the user is whom they claim to be. Before access is granted, the user enters a username and password. Each user must have unique identification information, this can be achieved via passwords, digital certificates, public key infrastructure or biometrics. [6]

2.3.2 Authorization

Authorization is the second part of the process that enforces policies for the authenticated user, determining which services and resources they can use. Authorization gives the user a set of attributes describing what actions individuals can perform. Different authorization levels can be assigned to different users, for example a user might be able to read content from a folder but cannot modify its contents. These authorization levels can be determined based on location, time of the day or frequency of logins for example. [6]

2.3.3 Accounting

Accounting is the process part which measures the authenticated user’s activities in the resources authorized for the individual. This can include various information such as session duration, how much data is being transmitted and resource utilization. Accounting information can be used to plan capacity and make trend analysis. Accounting can be used for auditing purposes, too. Accounting provides information about different systems and networks that enable administrators to review which resources are being used and by whom. [6]

3 Technologies, Concepts and Security Guidance

This chapter introduces the technologies, components, concepts and security guidance used in the remote user environment and in describing related processes. The security guidance section presents select guidelines from the NIST publication and VAHTI frameworks. Included are concepts relate to the remote user management process and the solution phase.

3.1 Virtual Private Network (VPN)

Virtual Private Network (VPN) creates a safe, encrypted connection over a less secure network like the public internet. Different protocols exist to encrypt data being transported. VPN creates a point-to-point connection to resources located in remote corporate networks. [7]

Remote users establish their connections using VPN when they use the remote access environment from outside the company to utilize resources inside the company network.

3.2 Internet Protocol v4 (IPv4)

Internet Protocol (IP) provides functions to deliver information from source to destination in system of networks. [8]

In the remote system environment clients that connect each have their own IP address assigned and each destination device and network being connected remotely have their own IP addresses.

3.3 Access Control List (ACL)

Access Control List (ACL) is a statement or rule configuration that denies or allows network traffic from source to destination. It is used to provide security in environments that use information networks. ACL enables network traffic control for IP addresses and different application protocols. [9]

ACL rules can be configured on devices that support it such as various firewall devices and must be configured in inbound direction although rules are applied bidirectionally. [10]

Each connecting external remote client has its own defined rules to allow use of different resources and applications through Access Control Lists (ACL). Figure 2 describes a setup for ACL.

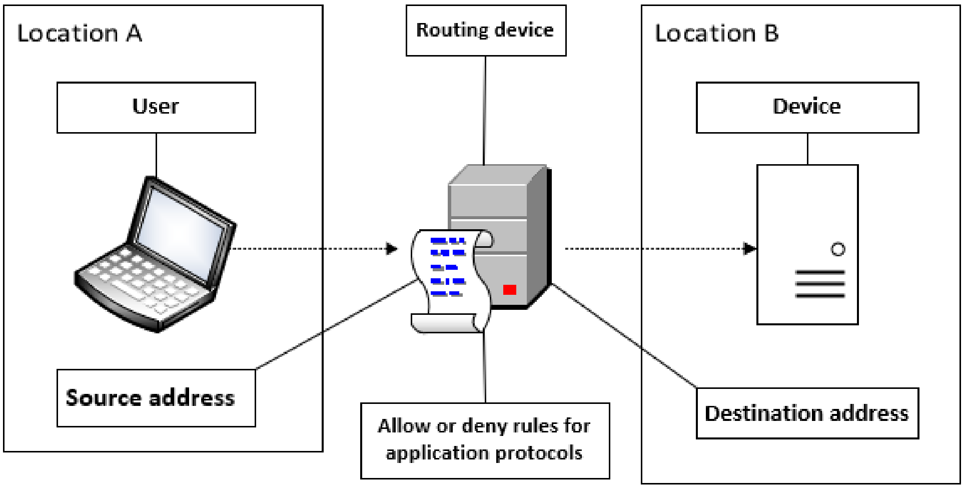

Figure 2 Access Control List

A routing device supporting ACL configuration statements has a rule entry for remote user in location A with a specific source address and destination addresses for destination location B. This rule can be an allow or deny rule for specific application protocols also.

3.4 Active Directory services (AD)

Active Directory (AD) is a Microsoft technology product that consist of several services running on Windows Server to manage permissions and access to networked resources. AD is used to store the user account information in the company along with group, computer and device information. AD and its functionalities are used to grant the *authorization* composition for each user within the company, be it an employee or a service provider. [11]

3.5 Security Groups (SG)

Security groups is a feature found in AD and can provide an efficient way to assign access to company resources within corporate network. By using security groups, it is possible to assign user rights to groups or assign resource permissions.

When assigning permissions, those should be assigned to groups rather than to individual users. The permissions are assigned once to the group, instead of several times to each individual user, reducing unnecessary work. Each account that is added into a group receives the rights that are assigned to that group in AD. User receives permissions stated in the security groups configuration.

In this thesis security groups located in directory services play an important role as to solution. Security groups in the solution are utilized to provide the VPN device the information so the device knows which ACL rules should be bound to arriving connection. This changes fundamentally how the remote system works and can be organized in the company’s case as explained in the solution section. [12]

3.6 Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) is an application protocol used to access and maintain directory services over network. LDAP stores objects such as usernames and passwords in directory services such as AD and shares that object data across the network. LDAP runs directly over TCP and through wide availability of TCP/IP means LDAP can run on most systems. [13]

LDAP Application Programming Interface (API) can be used to manage directory and browser applications but is not meant for creating directories or define how those services operate. [14]

3.7 Configuration Management Database (CMDB) and Service Requests

This is a database where enterprises and organisations store information about their IT assets and environment configuration. CMDB is used to record service requests in the identity management process and is a part of IT support operations.

These requests can have several different fields depending on which service they are categorized into. In this thesis, CMDB is referred to as a place where customer request information is stored and is not discussed further here. A request content used later include the customer field, IP addresses and protocols requested and the type of request. The types of customer requests when the context is the discussed remote user environment are create, delete and change requests. [15]

3.8 Identity Access Management (IAM)

Identity access management (IAM) in a company environment defines how role and access privileges are managed within a corporate environment in a given system and gives digital identity to individuals. With this identity and access privilege it is possible to utilize company resources and services.

IAM can be thought as a continuous development process for different system solutions in various lifecycle phases. Even older systems need to be changed so that they comply to rapidly changing security requirements of today and fit the company's IAM architecture. Continuous approach in IAM development can make management more secure and reduce unnecessary complexity while having a standard way to operate throughout the company. [16]

IAM as a concept and practice fits well within the scope of the present study, because the solution proposed will have an impact on the technical architecture of the VPN-environment and to the process related to how IAM can be done in this specific system and its business scenario. A comprehensive IAM structure and a continuous review and development on it should be a major consideration for different organizations.

3.9 Role-based Access Control (RBAC)

Role-based Access Control is used to restrict access into networks and resources based on individual user roles and responsibilities in a company. The tasks can be limited based on the roles such as read, create and modify rights of files. Using the RBAC approach can be beneficial in cutting down error potential when assigning permissions. Creating too many roles moves towards user-based control, defeating the purpose of RBAC. Figure 3 describes example roles and the systems and applications they are allowed operate on. [17]

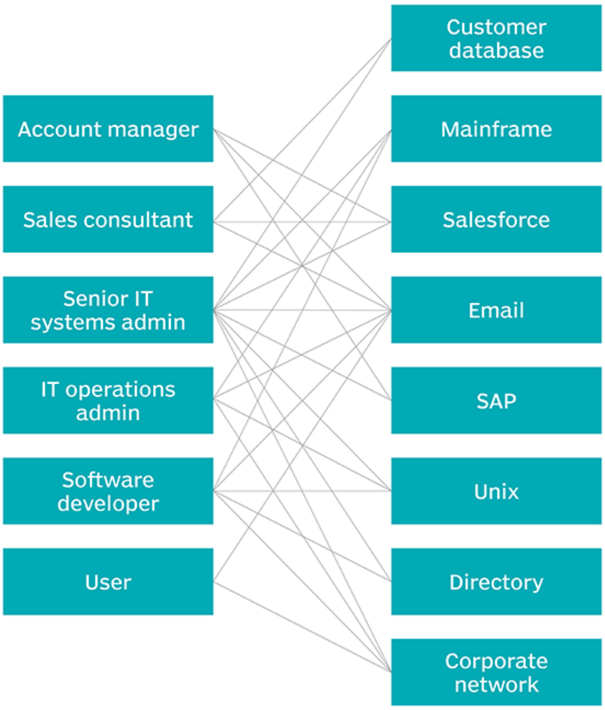

Figure 3 Role-based Access Control [17]

RBAC can be implemented after the organization has established their resources, personnel who need access and their possible roles. The RBAC approach is useful for growing companies, but also for organizations that control many users with different access requirements. RBAC can also be modified into more granular restrictions, after the baseline has been established. This gives RBAC flexibility to accommodate for changing security requirements. [18]

3.10 Special Publication 800-113 (Guide to SSL VPNs)

SP 800-113 is selected from NIST as security guideline. The publication is aimed to provide guidance on implementing SSL VPN and it is used as a general supportive background for VPN planning.

Organizations should determine what resources are accessed and by whom. After this a control policy should be designed. Organizations can utilize this guidance in combination with its own security policies or parts of it. Control policy can determine other characteristics such as authentication methods, client computer type, location and user identification. [19]

"VPN products vary in functionality, including protocol and application support. Each SSL VPN should be evaluated to ensure they provide the level of granularity needed for access controls" [19]

In the planning and implementation section of SP 800-113 it is stated in the identifying requirements section, that a company should recognize which resources and services need to be available for remote access and who should be allowed to access them. It is also important to identify other application-specific requirements to help plan for future requirements. A given system might change in a way that it needs to be accessed remotely. [19]

To begin the identification of access needs, a set of organizational requirements should be articulated. This does not have to be strictly technical but are steered by company needs. For example. [19]

- All users should be able to access certain applications like email and intranet servers

- A small group should be able to access a file share.

- Third-party companies should be able to access administrative servers.

Further going into the design phase SP 800-113 and selecting access control and its suggested steps to help form a structured approach in the thesis. The presented steps are [19]

- List the resources that will be accessed remotely
- List the users or groups
- List the conditions under which the resources should be accessible
- List how the remote environment should be used to access the resources

3.11 Security of End Devices and 2013 VAHTI instructions

In the *“Päätelaitteiden tietoturvaohje” (5/2013 VAHTI) Summary* section it is recommending that policy guidelines should be considered when acquiring new end devices or services related to them in government organizations. [20]

It can be stated that the remote access environment and any suggestion to change the technical environment is a workstation related feature. This specific guideline is written from the viewpoint of confidential material, but it does not state it could not be applied into other systems, too.

When different end devices are connecting into company resources it is good practice to investigate and recognize, what kind of strength and weaknesses they might have. Work that happens remotely must be considered because the device is not in a physically known location and connecting happens most likely through internet or another untrusted network. In these situations, administrative and operations tasks that always connect remotely must be arranged through VPN-connections. The same rules should apply here like they do when connecting to resources in a secure corporate network. [20]

It is not feasible to extend company security policies onto service providers and their processes to full extent as this can critically constrain operations at the destination. One reason why security is a concern to the company in those places where it can be influenced. Features that can improve the situation should be investigated when possible.

4 Remote Access Environment

This chapter explains how identity is discussed and referred to in the study’s context, because in the company case the current identity for accessing company resources remotely is a combination of multiple different technical environments. The identity of an individual is assembled from several pieces and for that reason technical environment description starts from describing each part separately and builds into an overview diagram.

Before moving into the business problem, describing the solution and method used to form it, it is necessary to describe the company remote access setup in a general sense. Each subcomponent is explained before building up to the overall remote system environment diagram.

4.1 Identity A

Identity A is described in Figure 4 being the first component of the remote environment setup. Identity A is what the remote user first gets when entering remotely. Individual remote users are assigned Identity A as a is given a username and an ACL rule statement or a list of ACLs. Each ACL rule determines if a specific user is granted access to the destination resource along with the allowed applications.

Identity A is created and stored at the network perimeter device that marks the border between untrusted networks like the internet and corporate network and its contents. Identity A is assigned either to service providers personnel from a third-party company or HSY own employee. Users who require remote access to different networks and resources can only be accessed through the discussed environment.

The user is identified at the VPN-gateway device with a user account name and password.

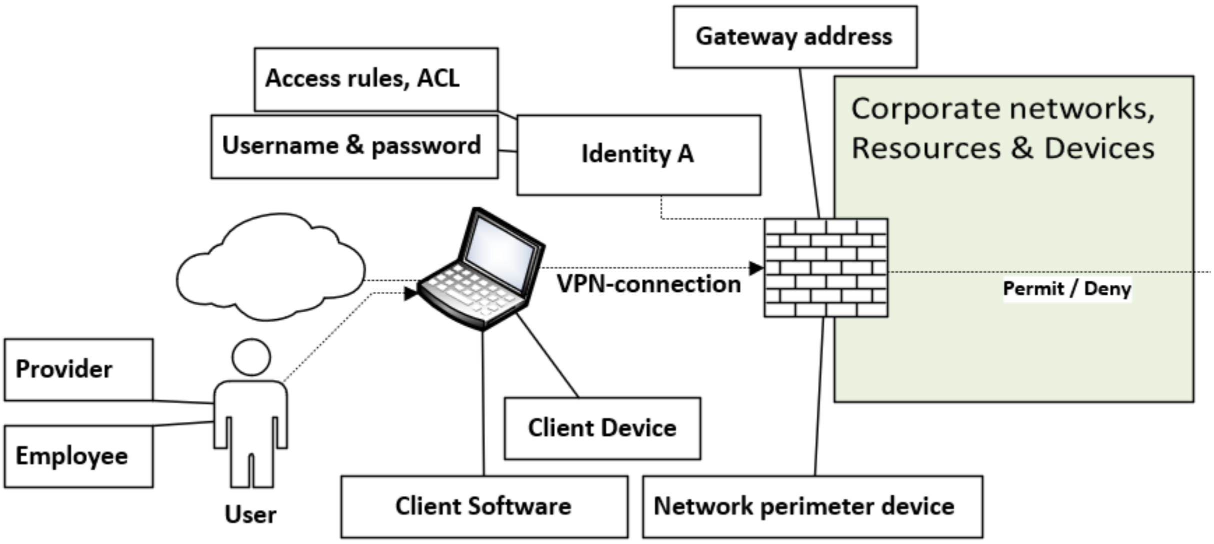

Figure 4 identity A

For a remote user a client device and client software are required to establish a VPN-connection and authenticate at the gateway address assigned to the perimeter device. Based on the given credential information, the connection is either *authorized* or prevented. The user for Identity A can have various responsibilities at the destination such as system maintenance, research and/or development.

4.2 Identity B

Identity B in the remote access environment is the second *authenticating* user account contributing to authentication chain. This identity is a user account stored in the company's directory services in AD and is unique for each authenticating user, just like Identity A. The user gets a second username and password pair from this environment component. Figure 5 describes identity B.

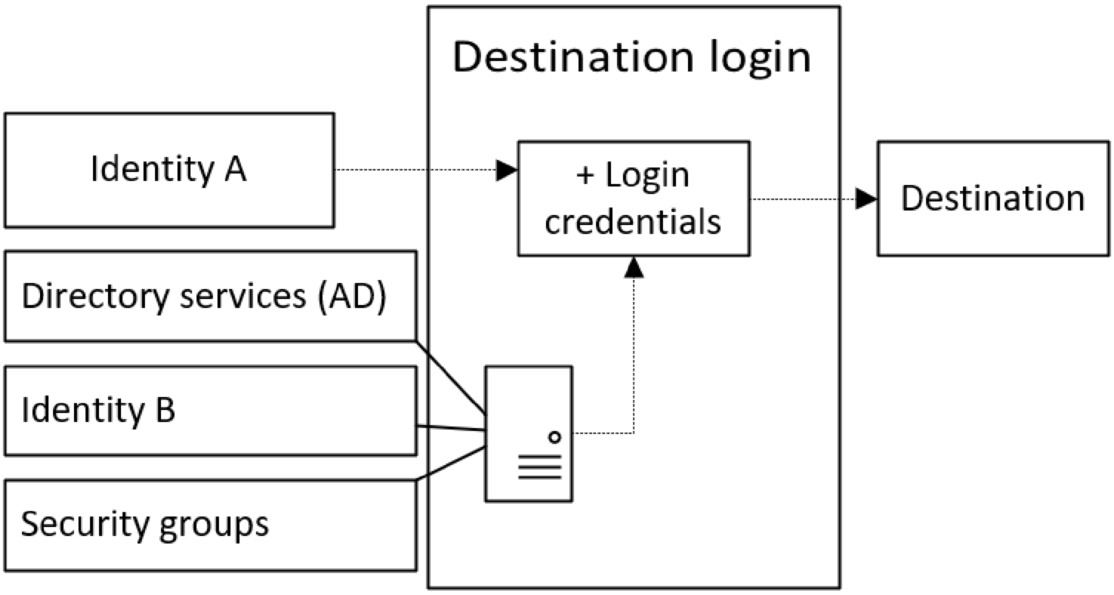

Figure 5 Identity B

This separate login information is given before individuals move forward and in to the final login phase. At this phase directory services can act as another layer of *authorization*, granting different privileges through security groups. After passing this phase the remote user arrives at the destination.

4.3 User Access and Destinations Requirements

Destination devices and applications being accessed by the remote users are in different IP networks. These networks can contain multiple systems, another option is that a certain system is split between different network segments. The most typical scenario is that one system is in one network segment.

When working with ACL rules issued to each user this creates different access needs that can vary a lot between different users. Different levels of *authorization* may also be granted between users.

Different types of access requirements are described in Figure 6 as X and Y -category user requirements defining the user type and attributes for identity. X and Y have characteristics that are described as follows:

User X requires access to only one network containing one system with many devices and environments.

- **User:** Admins that deliver continuous management for a certain system.
- **Attribute:** Little or no change to ACL rules during identity lifecycle.

User Y requires access to multiple networks and into specific destination.

- **User:** Development and research type of usage
- **Attribute:** Access is granted for temporary duration
- **Attribute:** ACL settings typically change over identity lifecycle

User N in Figure 6 is just to illustrate that there is no limit for the number of remote users and that the total number of remote users does not stay static.

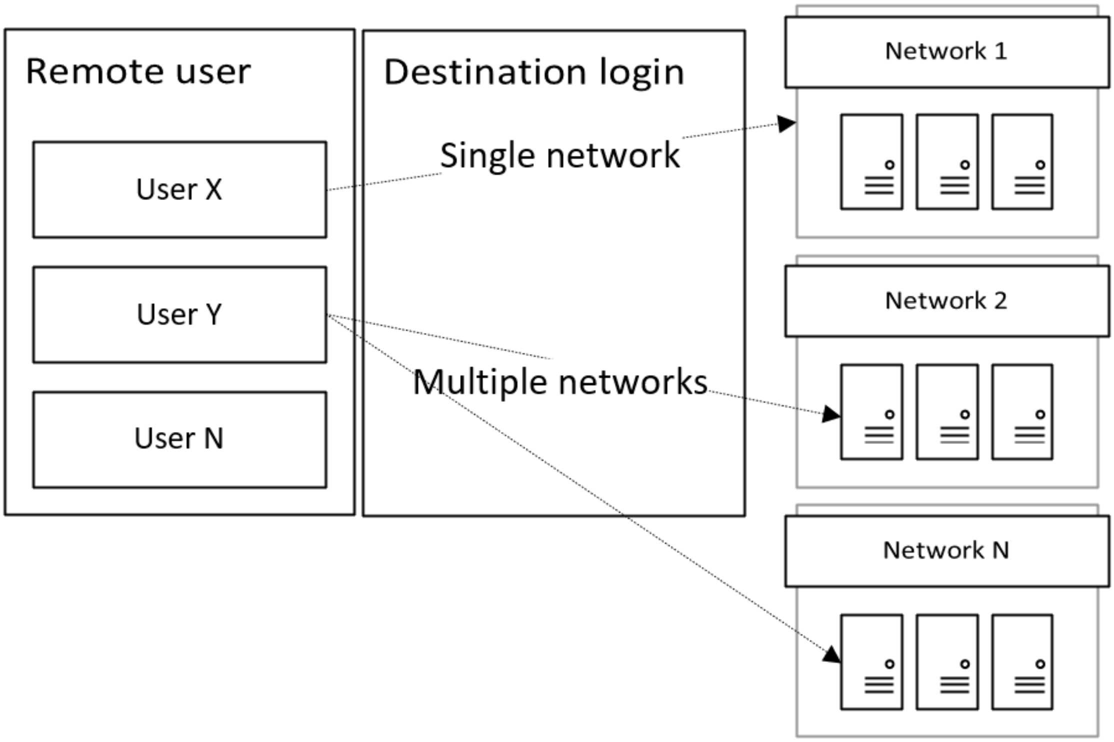

Figure 6 Access requirement types X and Y.

There are several different application protocols on top of destination IP addresses depending on the system being accessed, this is also shown in the ACL statements found from the configuration data analysed in the present study.

4.4 Security Features

Individuals that access these different systems have multiple identities they need to handle. On top of these identities there can exist other mechanisms to provide extra security. Each complete chain should use some form of two-factor authentication to keep user accounts safe during times where digital frauds and hacking incidents is increasing, weak passwords being one of the highest causes of a security breach. Because of this a final layer before a successful login is described. This layer in the login phase can provide additional *authorization* or *accounting* functions that are different between different systems and is present in the final login phase before the destination is reached. This is presented in Figure 7. [21]

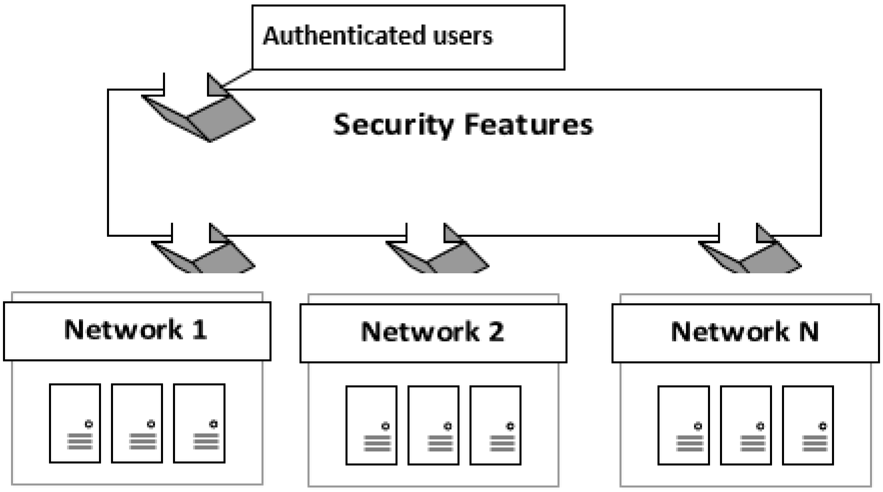

Figure 7 Security features layer

Features in Figure 7 describe a layer that can consist for example of the following features:

- Multi-Factor Authentication (MFA)
  - In online environments this means passing several different security measures to access a system. [22]

- Two factor authentication (2FA)
  - If a system requires only one extra security check before login it is called two-factor authentication. [22]

- One Time Password (OTP)

  - At login event a password that is valid only once is called OTP. These one-use passwords can be sent to the user with SMS text message, or by a phone application. Physical handheld device called security token can deliver OTP as well. [22]

- USB Security
  - Security key is a hardware device that uses USB to connect to a computer or other device, allowing access. [23]
- Logging
  - A separate logging system for auditing purposes.

This layer in the final overview diagram is described to further understand the scope. The exact technical contents of this layer are not described as they vary depending on the destination system. Another reason for this is to steer the study's focus on the actual VPN service and the identity stores within this specific environment.

4.5 Overview

Chapters 4.1 – 4.4 describe the different components present in the remote access environment. The sections contribute to a remote access architecture where a user logs in at the gateway, this is where *authentication* happens. Then *authorization* is given based on ACL rules defined for each user, granting access to different resources in different networks.

Different identities have different tasks they perform at each resource. Users perform additional authentication in those systems that have directory services enabled. Depending on the system there exists the security layer which can provide authorization or account functions, or both. This is described in Figure 8 *Remote system overview* and will be referred to in the solution section.

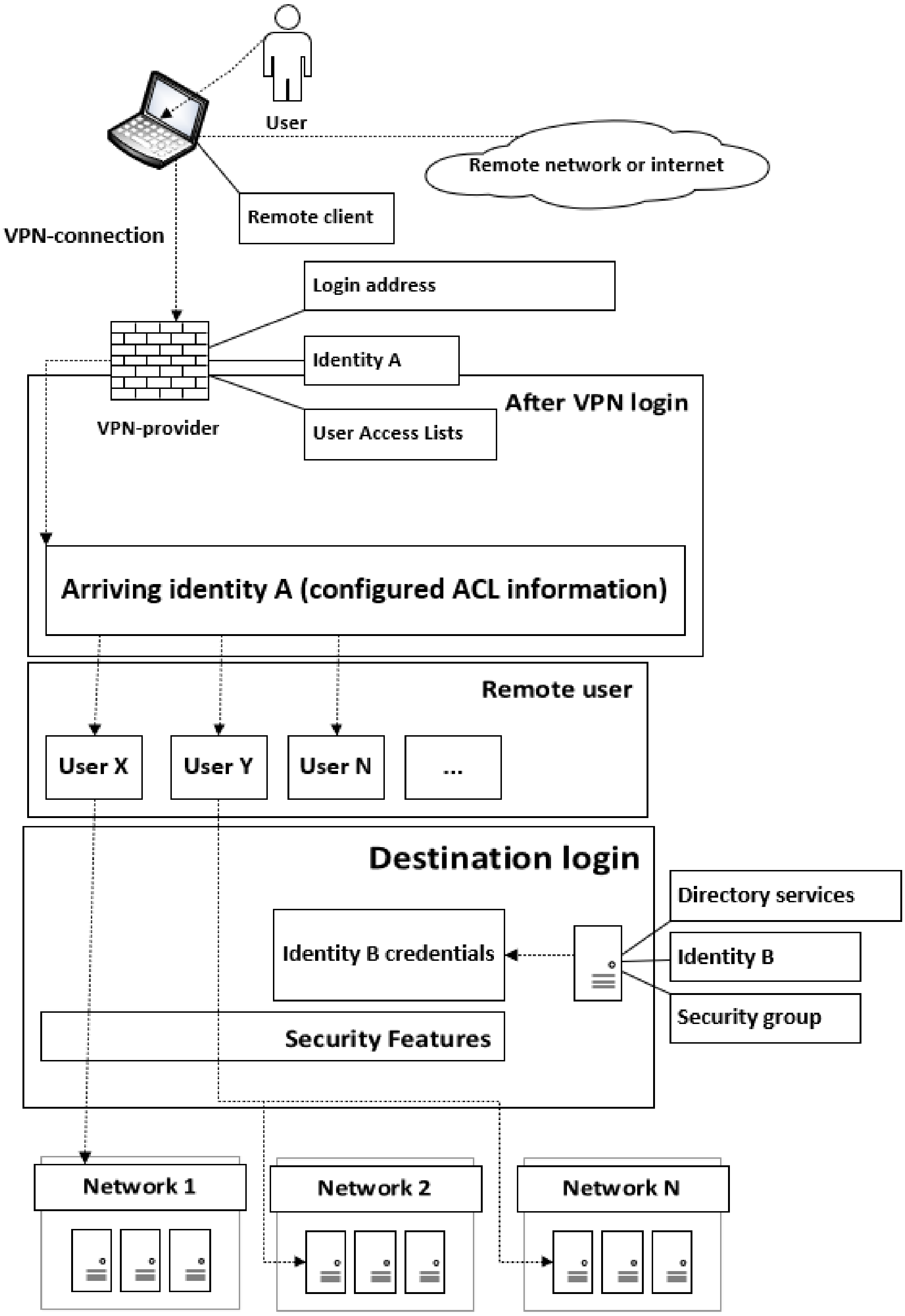

Figure 8 Remote system overview

Figure 8 is described with following steps

- User logs in at the perimeter address with a username and password.
- VPN device lets the user through based on specific ACL rule statements.

- User with specific access requirements continues to the destination and depending on the destination system a second username and password is required. This is noted as Identity B and provided by Directory Services.

- Before destination login happens, select additional security features or mechanisms exists depending on the destination system.

Figure 8 has all the previously explained subcomponents and from it, it is possible to easily understand how different identities and their storing environments are situated in different locations and services.

5 Problem Description and Remote Access IAM Process

Currently in the setup described in Chapter 4 users authenticate themselves at the VPN perimeter device. After the authentication is complete in all the necessary steps, the user has established connection to the company network environment. The user gets an allocated client address and is *authorized* to destination hosts based on their ACL rules. The starting point and attention is focused on the client VPN user accounts. The scope of the present study does not include various other services offered from the same perimeter environment for example VPN-tunnels that offer business to business connection. Problem description and data analysis focus on user accounts which contribute to identities used to remotely access systems by those service providers that operate on systems located inside the corporate network. Different access requirements exist for these third-party providers as discussed above.

Systems that can be and are operated via remote access can roughly be categorized into systems that are connected to the company's office network and systems that are operated in isolated network VLAN locations.

The problem with the current setup is that VPN client accounts, Identity A is needed to establish remote connection and that their configuration information ACL rules have stacked over time and lived through several system lifecycles and organization changes while at the same time need for remote access grows and systems become manageable through remote technologies like VPN. Also *authorizing* ACL rules exist on the perimeter device, outside of company's AD services. While this is happening, and new systems are being built a controlled IAM must be maintained also due to today's security requirements and changes in identity collection that can and are changing faster when certain workloads become more temporary since access identities and systems lifecycle become shorter.

Why this is seen as an actual problem the process for controlling the VPN identities is described and a proposed change to that process is presented in the solution section. It is also explained why this would make managing easier and operational costs lower. Impacts of this process change have been discussed together with the company's stakeholders.

5.1 Create, Remove and Change Requests for Access Identities A and B

A need for a stakeholder's remote access can be initiated for example from a project that needs more developers or a new person starting a job at service function that delivers different administrative tasks for the company. A request for remote access is done by project manager or service manager to the company's IT department operated and owned support function in ServiceDesk (SD)

SD then records the request as a service request ticket into Configuration Management Database (CMDB) with necessary information such as related systems and/or software. If the requester, or customer, is not the company's own worker, the request is recorded for the project or business owner of the company side and additional approval check is triggered. The content of the requests is checked for destination IP addresses and necessary application protocols and then forwarded to the VPN-provider side where Identity A is created. Identity A location is at the VPN-provider side as described earlier and SD personnel has no direct access to it.

Optionally if the target system is using AD to *authorize* its local login and as uses AD as its IAM, then SD creates also AD-user account or Identity B and forwards the account information to the customer along with necessary use instructions.

At the VPN-provider side. Identity A or VPN client account is created with a certain naming convention with additional information such as company and phone number when applicable. A set of ACL rules is placed on this account and the account gets an IP address. The login information along with instructions to using the VPN-gateway address and suitable VPN-client connection software manual is sent directly to the user and company IT support is notified that Identity A is created. All information related to and the use of Identity A is handled at the VPN-provider side.

A request for deletion is also originated from the customer just like the create request. This is once again recorded by the SD into the CMDB and request is forwarded to VPN-provider where identity A is deleted. The same applies to deletion as creation, further approval is required if the requester does not have approval directly attached to the request.

At each of these steps where the process task is given to SD or forwarded to the VPN-provider side, an operational cost is generated. Additionally, the operational cost is larger in the VPN-provider side as configuration requires additional knowledge in operating a network perimeter device and its user database configuration.

Identities A and B lifecycle processes are managed separately, contributing into a process diagram which leads to additional information exchange between different operators. Because Identity A is stored in an outside system in relation to SD operations adds up the information exchange required and time consumption. The current process is described in Figure 9 where each operator has its own track, crossing a track creates information exchange and operational cost (OC). Generated OC is marked on each step that has it. The steps are numbered to illustrate the amount of information exchange taking place.

In a situation where the destination system is using AD as identity B to *authenticate*, additional OC is generated at step 3, this is a separate process requiring possibly different or additional administrative rights and as such having its own operational cost. Creating Identity B does not apply to systems that are not using AD for authentication. The process for create request is described in Figure 9.

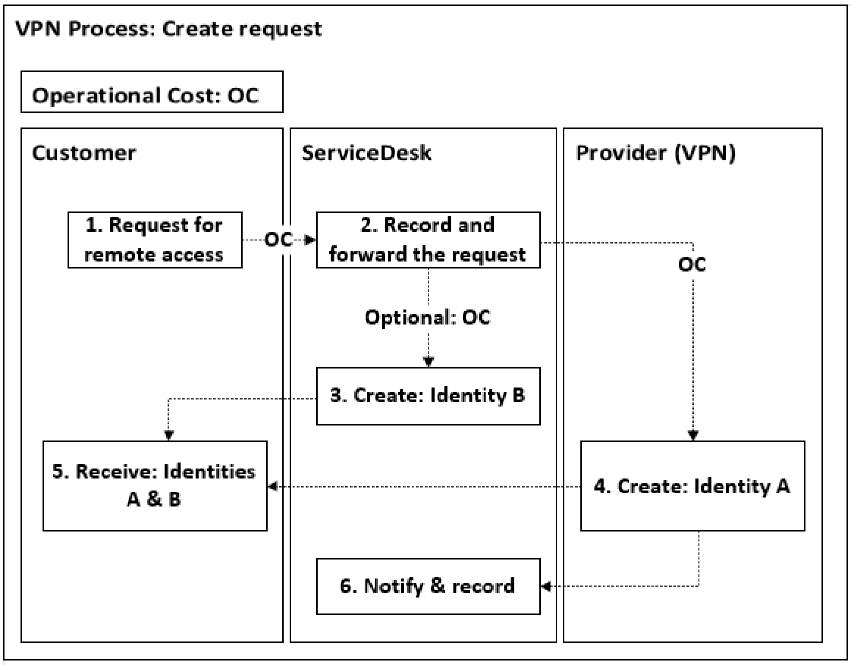

Figure 9 Process create

Figure 9 illustrates the functions and operators that exist within a service request explained earlier in detail. To summarize, the customer sends a request across to SD which then records the necessary information and passes it to the VPN-provider who creates Identity A, finally passing this information back to the customer and notifying SD about it. If identity B is needed, SD creates it.

The process for deletion is described in Figure 10.

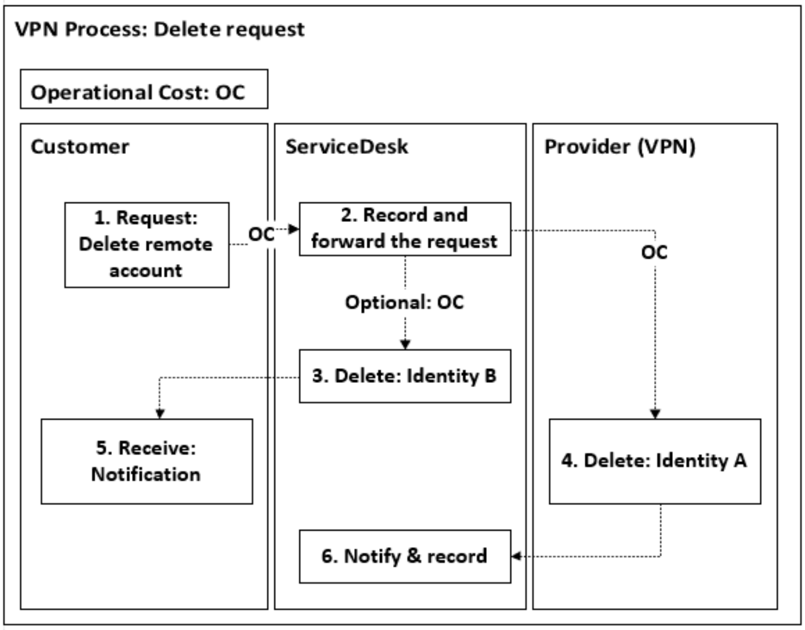

Figure 10 Request delete

Following the same structure as in create request in Figure 9. Delete request in Figure 10 is initiated by the stakeholder customer, then recorded at the SD function and then passed on to the VPN-provider for deletion. Part of the business problem is the lifecycle process of the remote identities where each user account is operated separately.

Request for change is described in Figure 11.

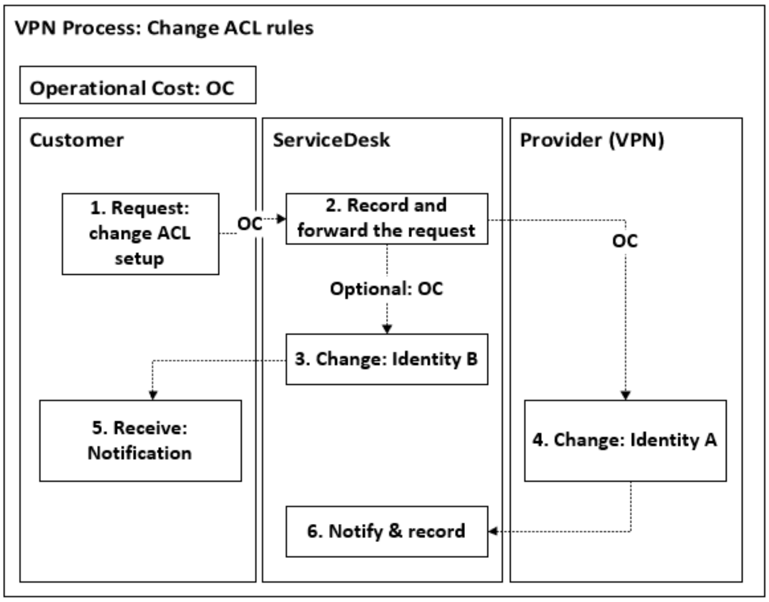

Figure 11 Request change

Change request follows the same structure as Create and Delete, but the contents differ in step 3 and 4 specifically. In Figure 11 step 3 requires SD to make changes for a possible identity B within the organization directory services. At step 4 the service provider needs to configure each VPN account or identity A's ACL rule statements separately.

6 Solution and Data Analysis

Chapter 6 describes how to the process described in chapter 5 can be improved, how approaching a solution was started, what was done and what is the result. The solution proposes that the identity provided by and located in the VPN perimeter device should be changed. The proposition for change is that the identity and defined ACL rule information is provided centrally from directory services. The solution discusses how this can be achieved with LDAP. LDAP is used to query AD for each remote user and their *authorizing* ACL rules and mapping security groups located in the AD into specific ACL rules in the network perimeter device. Chapter 6 also presents the initial data and its preprocessing and how it was organized to move closer to simpler IAM and group-based management conforming RBAC principles.

6.1 VPN with LDAP Binding

LDAP is one of the methods in which a VPN solution or product can query the contents of AD. In the proposed solution LDAP query is used get the authenticated user account and to bind incoming remote users to group information located in AD and groups assigned ACL information. Based on the queried group information a user gets *authorized* access to defined applications and destination addresses.

LDAP can be used to query the contents of AD and it being widely supported across different platforms is selected to enable the perimeter VPN device to perform queries against AD. There are various vendors and platforms that enable the use of LDAP such as:

- OpenVPN [24]
- VMware Workspace ONE UEM [25]
- Paloalto [26]
- Cisco [27]

An LDAP enabled VPN perimeter device can be translated into a change described in Figure 12. when considering the current situation presented in the previous technical overview diagram.

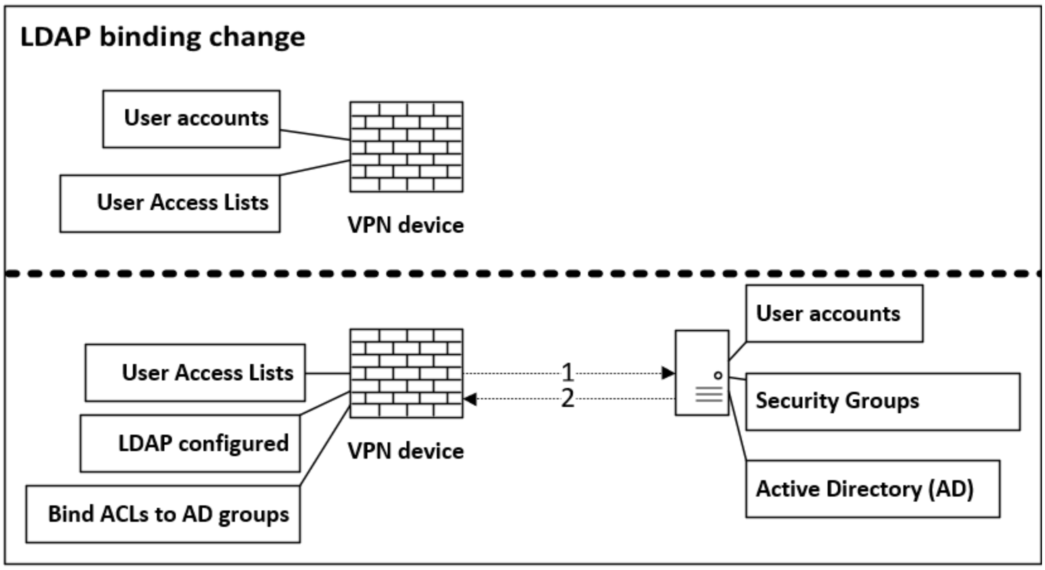

Figure 12 Perimeter device, LDAP enabled

Before utilizing LDAP, the VPN device has user accounts and ACL rules stored in that environment. After enabling LDAP and configuring necessary information about the AD services it can be used to query AD and its user account and security group information (step 1, Figure 12). The query then sends back information about the authenticated user's account information and its group information (step 2, Figure 12). The group has the attached ACL configuration defined at the VPN device.

6.2 Starting Point, Current VPN User Data

Remote user accounts and ACL rules exist in the VPN perimeter device initially. To understand what kind of network level *authorization* these users have and what the current situation is a file export of the current client configuration is generated. This information forms identity A described earlier and is given to individuals at the network level *authentication* phase. This user data was then analysed and organized.

Different systems exist in different lifecycles, some systems have their setup changed over the years and across organizational changes and mergers. This means that some destination addresses might have changed or have been re-used for other purposes. Some networks defined in the ACL rules have turned obsolete.

Provider or third-party companies operating in these systems also in some parts have gone through organizational changes as well over time, affecting their roles and needs inside *authorization* context. For these reasons the data needs to be pre-processed in such a way that destination addresses, and user accounts are verified that they are valid.

Analysis is done by looking at the users ACL information, which destination addresses are being used and which application protocols are permitted. Information surrounding these destination environments is further collected from different stakeholders. Different stakeholders were described in Chapter 1.2. The discussions helped to establish the company needs, following the description in the supporting guidelines mentioned in NIST SP 800-113.

Various sources to establish stakeholder needs were used, i.e. the following resources and tools:

- Discussions held with different stakeholders like system owners, project managers, key users and the ICT department

- Documentation provided by the company

- Network tools such as ping command and DNS records for verification purposes.

Using these resources and tools, additional descriptive metadata was formed to supplement the source data.

Adding metadata and filling out missing information helped to avoid a situation where work with invalid information would have been conducted and adds to the quality of the data.

The original data was stored as a backup in a separate file and a separate working file was created. New information and corrections were performed on the working file. It is worth to note that during the study, the actual remote process was going on in the production as usual. This was realized and understood that taking a configuration information at a specific time changes over time and that results need to consider these changes with a final sync up of the data.

6.3 Initial Data Content

A VPN provider delivered a configuration export file as discussed in Chapter 6.2. The original data contained the following information

- Client IP address assigned to a user.
- Client accounts login name.
- ACL -rule statements for each user. Defining allowed resources and applications.

The number of client connections analysed was 300 that needed remote access to various destination systems and applications.

6.4 Work File with Status and Meta Information

Metadata was used to supplement the existing initial data to help recognize access needs and to find criteria by which a rule group can be formed. The working file's function was to improve source data and to track each client or clients pre-processing *status* filled as a separate attribute. The *status* attribute was indicated as following:

- 1) Was the client account verified or marked as obsolete?
- 2) Were there any necessary changes required in specific ACL rules?
- 3) What company documentation was needed for verification?
- 4) Which stakeholders could provide necessary information about a user?

Status attribute values 1) and 2) were used to also trigger service requests to the VPN-provider side to change the configuration as work continued during the ongoing VPN management. Based on the value of *status* attribute, specific clients were analysed further, and the following additional metadata was added:

- Service provider company
- System or systems that were present in the ACL rules
- Application allowed for each system
- Identity B authentication method at the destination. AD information if applicable

When this information gathering was completed it was used to plan the security group solution and structure.

6.5 Tool Selection

Microsoft Office Excel workbook file was used to handle the data in table format with each remote client present on its own row and each column containing information mentioned in Chapters 6.3 and 6.4. Workbook had different sheet for ACL rules. For around 300 users, each client containing one or more rules the amount of ACL rule statements ended up in around 3200 making over 10 rule statements on average. The original state of information was kept in their own data sheets as source data and different sheets were generated and used in the working phase.

Active Directory tools were used to find the entries that had presence in both the directory services and the VPN perimeter device. AD user groups were investigated to understand which *authorization* setups were used there to give information about the destination systems.

6.6 Security Group Design and Findings

After the data was cleaned at the pre-processing stage, organized and filled with the described information, the next step was to assemble remote client accounts into groups and design a way that supports the desired *authorization* levels which support a RBAC-styled approach. This furthers the idea that only the necessary *authorization* level is distributed for each user. Because in the solution these security groups co-exist with other policy groups in AD if an actual implementation project is engaged, this should be considered, and they should be distinguishable from each other at a service level.

To distinguish VPN access groups from other security groups a *root level* is defined to know which service it is related for example *root* could be named as VPN or VPN-service, or similar. After establishing the *root level* to be VPN-service it was decided to use the company information as the second level for identifying *authorization* level of an *authenticated* user.

From the data it was discovered that most systems and most of each system accessing clients belonged from one to a few different service provider companies. After this was established it was further discovered that inside a certain company there exists different ACL statements between the same third-party company's employees. Some providers have only one individual. A situation with multiple company employees were distinguished from each other with a role -level after the company level. A sub role level the first one is reserved to allow flexibility in a situation that even more granularity will be needed in the future. The following setup was established:

- **VPN/Root** ← The root level. Determines what system this container security groups operate.
    - **Company/Service providers** ← Groups individual remote clients based on their third-party company information. Determines a baseline destination address setup and application protocols.
        - **Role/Tools** ← Determines additional destinations and application protocols. Expands service providers *authorization* level when necessary. Additional approval is required to gain this role.
            - **Sub role** ← Left for expanding possibilities. If further granularity is needed. Allowing flexibility.

From the data it was discovered that around 40 different service provider companies and their operators require remote access to company resources with various needs. With around 300 remote users this averages in about 7 to 8 individual users. Some environments were larger and had more members at the company level than others while other environments used more well-defined granularity at the *authorization* level, resulting in more roles and sub-roles to be created. A few systems were accessed by only one or two operators in the smallest setup.

7 Solution Impact and Considerations

Chapter 6 described a way to use Active Directory as the source for remote users ACL rules and authenticating remote users. Chapter 7 continues to describe how engaging in an implementation project, choosing presented solution would impact the remote system environment setup from a technical point of view and the impacts to the VPN IAM process. Chapter 7 provides a critical approach in this and considers the benefits and possible issues with the solution.

7.1 Impact on VPN Environment Setup When Using LDAP

If an implementation plan for LDAP binding between VPN perimeter device and AD directory services is created, it removes identity A from the *authentication* process chain that each remote user must go through. Physical locations of account information are reduced to one and *authorization* is queried by the VPN perimeter device from AD instead of VPN device distributing ACL rules directly to the remote user. Mapping information to bind ACL rules to AD group information is still stored at the VPN device it being responsible for network level routing decision for incoming clients. This is described in Figure 11.

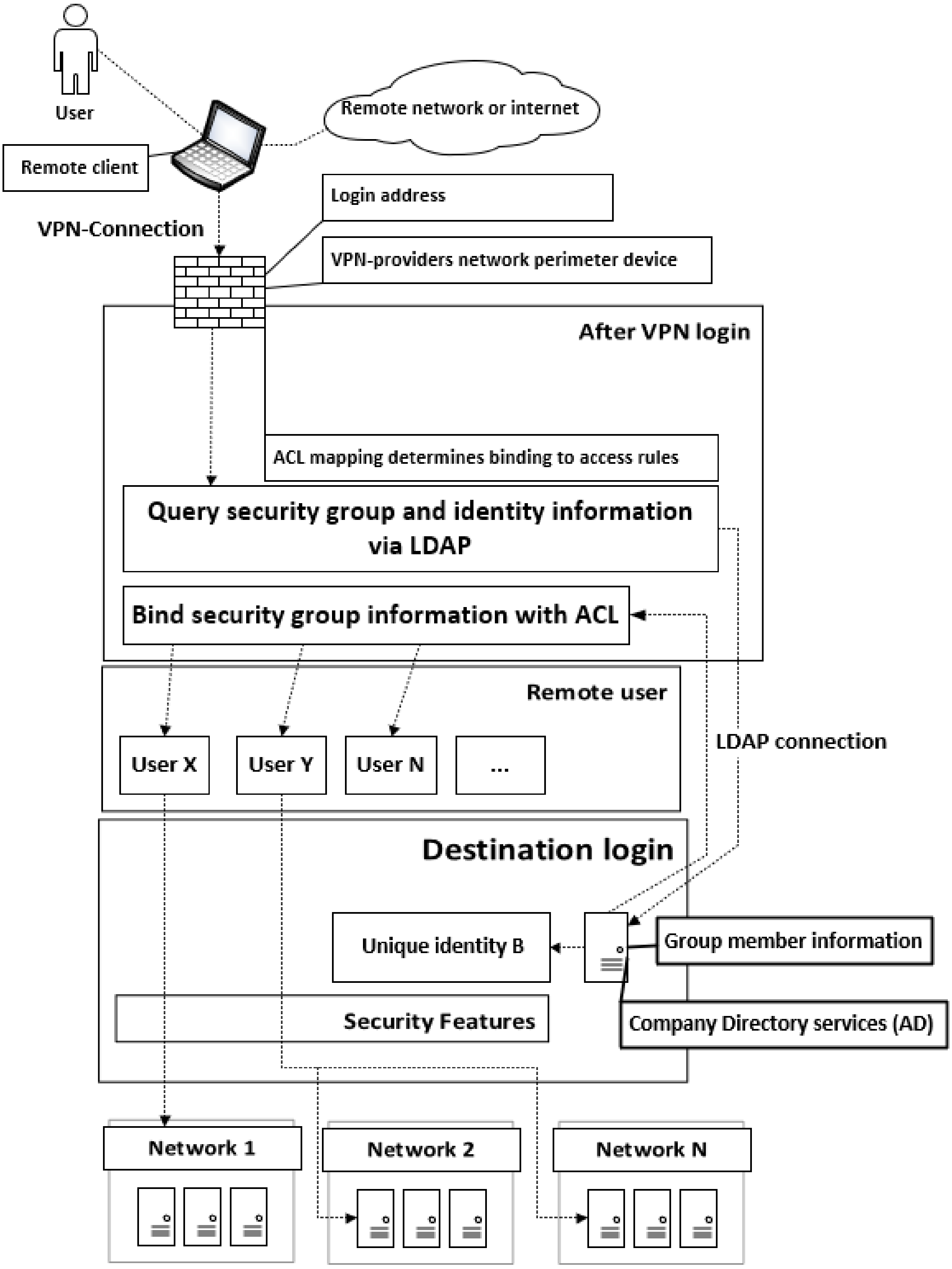
User
Remote client
Remote network or internet
Login address
VPN-Connection
VPN-providers network perimeter device
After VPN login
ACL mapping determines binding to access rules
Query security group and identity information via LDAP
Bind security group information with ACL
Remote user
User X
User Y
User N
...
LDAP connection
Destination login
Unique identity B
Group member information
Security Features
Company Directory services (AD)
Network 1
Network 2
Network N

Figure 13 Environment overview without Identity A

Like Figure 8, Figure 13 can also be expressed with a series of steps, fundamental change happens at Steps 1 and 2 marked as NEW:

- 1) User logs in at the perimeter address with a username and password.
    - NEW: VPN perimeter device gets the user identity from directory services contributing to identity B.
- 2) VPN device lets the user through based on specific ACL rule statements.
    - NEW: ACL rules setting is based on what the LDAP query returns as the user’s security group information. Mapping of ACL rules to groups happens at the perimeter device.
- 3) User with specific access requirements continues to the destination and depending on the destination system a second username and password is required. This is noted as Identity B and provided by Directory Services.
- 4) Before destination login happens, select additional security features or mechanisms exists depending on the destination system.

Figure 13 uses Figure 8 as its base and illustrates the fundamental change happening at the VPN-perimeter device. In the setup it can be argued that VPN device does the *authentication* and *authorization* but only under directory services supervision and information queried from it via LDAP.

7.2 Impact on VPN Identity Management Processes

This chapter describes how changing the technical environment into using LDAP query impacts the Identity management process when handling VPN users. Figure 14 describes the management process for the requests create and delete when using LDAP in the solution listed below. Creating and deleting remote user accounts is removed from the VPN-service provider side and can be handled from a single location together with the rest of the identities.

- Request: Create

  1) Customer sends a service request to company’s ServiceDesk (SD)

  2) Request is recorded to CMDB. VPN user is created (Identity B)

  2B) Identity B is added into appropriate AD security groups to grant the ACL rules defined at the VPN perimeter device

  3) Account information is sent to the customer

- Request: Delete

  1) Customer sends a service request to company’s SD

  2) Request is recorded to CMDB. VPN user is deleted (Identity B)

  3) Customer gets notification of the request being complete

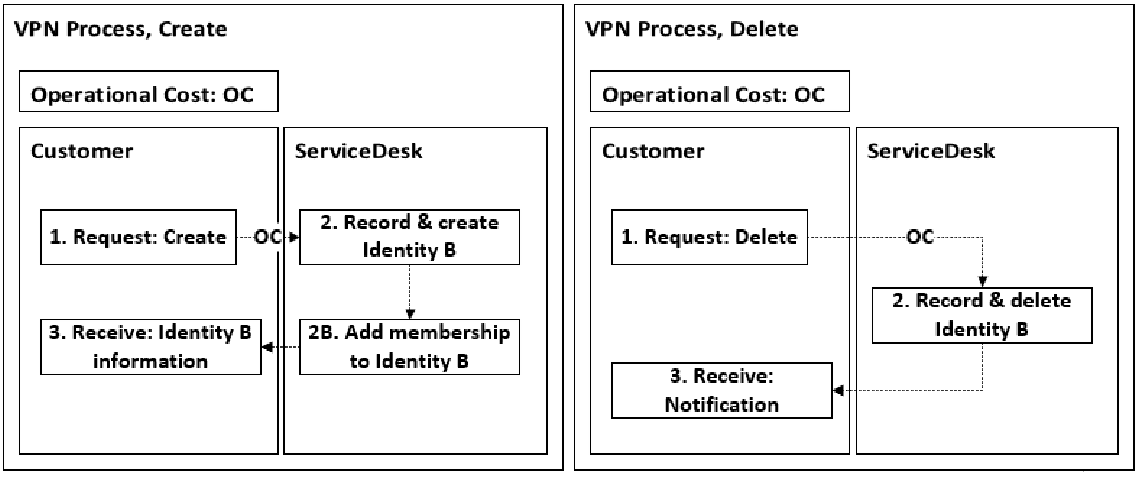

Figure 14 Create & Delete requests. After process change

Figure 15 describes a scenario where the user or users require changes to their ACL setup with a more suitable *authorization* level. This can be due to a change in job description that requires a change in the role level from the *authorization* tree presented in the solutions security group structure.

To accomplish this, first a request to SD for role change is made by the customer. The request is then recorded in CMDB and the user's account is modified by changing the group membership information of Identity B which is used for remote access. The customer receives a notification when the request is completed, a new set of ACL rules is activated to grant role-based access.

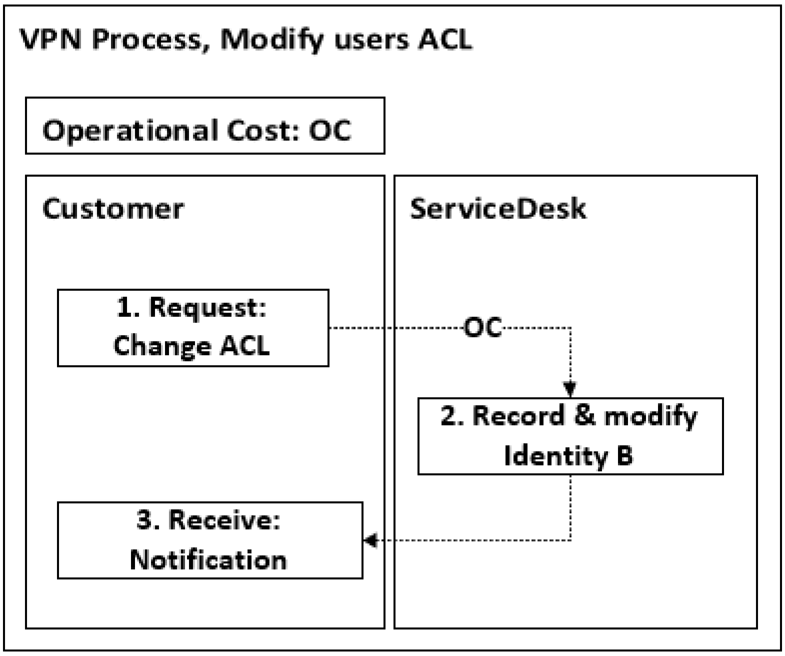

Figure 15 Single user ACL change request. After process change

Figure 16 describes the steps present in a request for new ACL group as follows.

1) Customer sends a service request to company's SD

2) Request is recorded to CMDB.

3) A new group is created into AD. New AD group information is sent to VPN provider. (This is marked as a separate step, because it requires collaboration as to how the ACL content will be defined and for what reason. This is documented separately)

4) VPN-provider creates the ACL statements at the VPN device and queries company AD with LDAP for group information. Group is then attached appropriate ACL rules at the VPN perimeter device.

5) Identity B is added into appropriate AD security groups by company SD. Like in the create request step 2B.

6) Customer gets notification of the request being complete

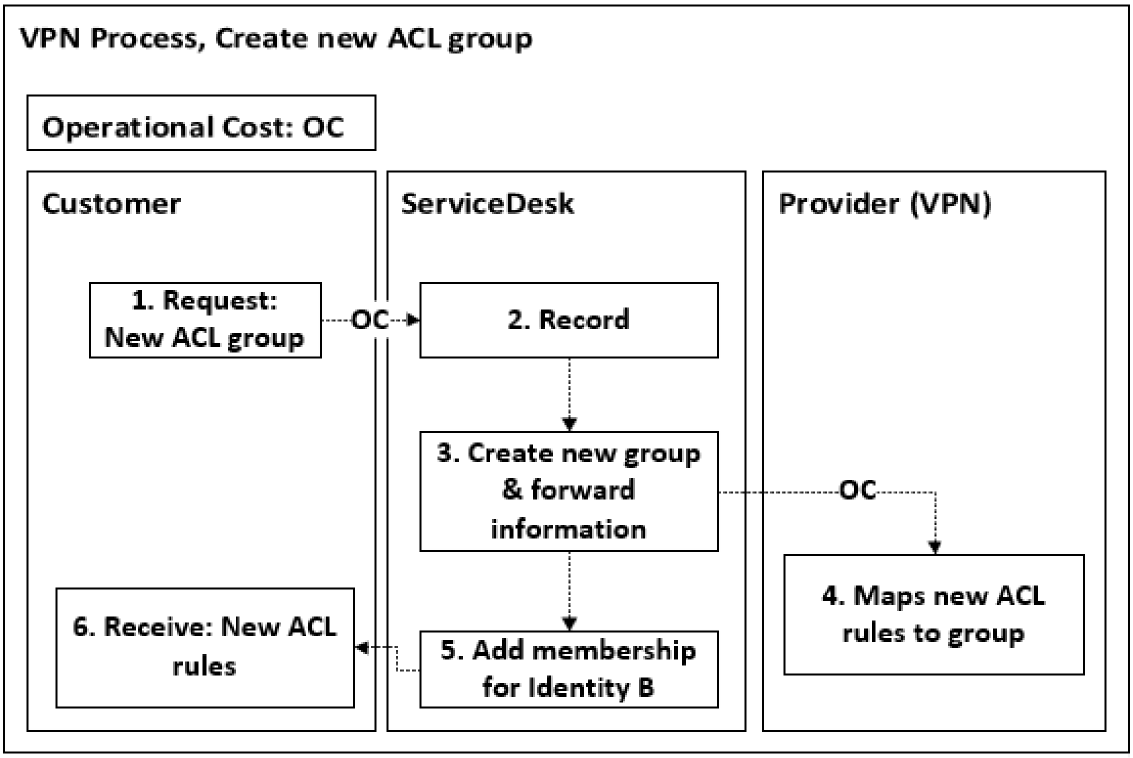
VPN Process, Create new ACL group
Operational Cost: OC
Customer
ServiceDesk
Provider (VPN)
1. Request: New ACL group
OC
2. Record
3. Create new group & forward information
OC
4. Maps new ACL rules to group
5. Add membership for Identity B
6. Receive: New ACL rules

Figure 16 New group with new ACL rules request. After process change

Possible situations where an ACL group creation or modification is required at the VPN-provider side include the following scenarios:

- New service provider company starts operations in company environment.

- More granularity to *authorization* levels is required that does not exist already. New sub-roles need to be created in AD and in mappings done at the VPN-provider.

- A provider company starts operations inside an environment they did not need to before. This requires changes to existing ACL mapping information at the VPN-provider

Based on Figures 14,15 and 16 it can be stated that the VPN-provider is only needed to control the ACL mapping configuration at the VPN-device. The VPN-provider is not needed to create or delete new remote user accounts or control if changes happen at roles that already are available through AD security groups. Chapters 8.1 and 8.2 explain the benefits and possible issues in the solution.

7.3 Benefits

The modification of the current VPN remote user environment removes operational costs from various positions in the VPN IAM process. *Authorization* for individual users in respect to network level access moves to the same place where destination login *authorization* is also controlled by company SD. For each identity, creation and delete operations, the VPN-provider is not needed, this reduces the amount of back and forth information exchange to achieve a working remote connection.

With physical locations and number of identities, or accounts with password being reduced if this change is implemented connects the IAM of a single user to uniform exit process. This affects the users so that they do not need to manage separate passwords, making the remote environment easier to operate.

7.4 Issues

The presented solution is not without flaws in a case where a change request for the ACL group mapping is made. A mistakenly configured ACL rule change in the worst case scenario can mean that users are able to access destinations they are not supposed to.

When security group design is concerned and approaching the situation with RBAC in mind. It might become unnecessary to use too many roles, defeating the purpose of operating in a group-based manner. In a very complex situation where roles are harder to find this might propose a problem. Complexity can arise from security specifications that set highly restricted rules for each user.

It can also be argued that when the identity for remote use is provided only by AD services in an outage situation it cannot provide the VPN perimeter device identity for *authentication* and group information to perform *authorization* ACL rules on the client connection. This makes the service dependent on a single point of failure, so it becomes necessary to carefully consider what options exist for different high availability solutions. To counter this argument, there could exist a disaster process that allows local accounts to be created if *authentication* and *authorization* via querying AD becomes unavailable.

8 Results

Data analysis via stakeholder discussions, documentation review and the use of tools revealed inconsistencies in the configuration that were fixed during the data pre-processing phase, resulting in more accurate data.

It was necessary to consider the changes happening in the remote environment production management, while working with the data requiring additional coordination.

As a result, the VPN user database content is prepared and structured so that it is possible to convert it into information that can be used to setup security groups in a case that company decides to engage an implementation project for an LDAP enabled VPN solution.

The solution describes the current process and impacts if this change is implemented, providing beforehand information to help the company in decision making. Instructions for the SD function could also be formed with the help of the detailed description provided here.

From the process diagrams and the explanation given it is easy to understand how the steps currently contribute to higher operational costs, raising awareness and help understand this specific environment and its expenditure implications in the ICT budget. In comparison, it can be understood which parts of the operational costs are removed if it is decided to implement the solution.

The study shows a case example on how implementing existing information as metadata to the ACL rules and user accounts can help in defining a stakeholder access need and how the roles can be created based on this.

The study is written in a way that it does not review a specific vendors or platforms solution, but looks on a specific company case, what problems are present and how it could be improved along with a description of a possible solution approach and background information to support it.

8.1 Analysis and Solution Reliability

Analysis of the data and solution review were carried out during the study. The author gave presentations as status reports to the company.

The selected solution is more like a market place of ACL rule groups, a user is put into an existing group preferably. Different solutions might exist, but the idea of using sub roles gives flexibility for more granular access design.

Another solution could have been presented if the study was purchased from outside the company. The study was done by consulting colleagues in the ICT department and stakeholders in different operative departments.

8.2 Further Development

In a general sense it could be asked if this type of analysis and solution could be scaled into more larger environments. In a much more complex case and with more users it could be possible to create a few different types of grouping methods and compare each different grouping as an operational cost analysis. Meaning the company could analyze how much cost is generated in IAM operations if the grouping used wide network level permit rules or more narrow rules. Narrow rules could mean more change operators at the group level but going into this would be another topic for research.

Another path of development more from the case company perspective could be an actual implementation project and selecting specific technologies, like for example which network perimeter device would suit the needs best, could cloud technologies be utilized.

Also, different features could be built on top of the solution and after implementation. From AAA, *accounting* was not touched upon but could be a development branch or focus for another study. Features such as centralized logging or connection recording for employee training purposes could be investigated. Also, expanding security features and investigating further into these is a possibility, like a password management system or a self-service portal.

9 Conclusions

It is necessary for different companies and organizations to recognize technologies and components that contribute to IAM and its complexity as more complexity usually involves more operators and increased cost. Also, occasions for errors increase when updates or changes are done in any of those components and within destination systems.

In the company scenario in the current setup there it is possible to increase control over which systems are being accessed along with simplified lifecycle management for the remote users.

The current remote environment setup is tedious to maintain because of the separation and use of multiple identities. This increasingly results in misconfiguration and obsolete information to accumulate over time, for the destination systems have their own separate lifecycles.

During the making of the study the company concluded that in today’s security becoming more important it is useful to bring components of IAM closer to SD operations and standard operations rather than having a separate system for this, also due to administrative resources being limited.

The study offers a ready to use solution proposal for how to prepare the company AD for an integrated VPN solution.

The presented solution and its different aspects describe only one scenario of a company which operates in the environmental field with various access needs. The working environment consists of common office systems to different automation systems.

References

1 Helsingin Seudun Ympäristöpalvelut <https://www.hsy.fi>. Accessed 18 January 2020

2 ITarian, Remote Access A Computer. Internet article <https://www.itarian.com/remote-access-a-computer.php>. Accessed 18 January 2020

3 VAHTI, The Government Information Security Management Board. Documentation <https://www.vahtiohje.fi/web/guest/home>. Accessed 18 January 2020

4 NIST, The National Institute of Standards and Technology. About NIST <https://www.nist.gov/about-nist>. Accessed 18 January 2020

5 NIST, Federal Perspectives. Internet Article <https://www.nist.gov/cyberframework/federal-perspectives>. Accessed 18 January 2020

6 Codebots, what is AAA? Internet Article (Serena Reece, Nov 27th, 2018) <https://codebots.com/application-security/aaa-security-an-introduction-to-authentication-authorisation-accounting>. Accessed 18 January 2020

7 Techtarget, Virtual Private Network. Internet Article (Margaret Rouse, August 2019) <https://searchnetworking.techtarget.com/definition/virtual-private-network>. Accessed 18 January 2020

8 RFC760, Internet Protocol. Documentation (Marina del Rey, January 1980) <https://tools.ietf.org/html/rfc760>. Accessed 18 January 2020

9 Ittsystems, ACL. Internet Article (James Cox, Editor. June 5, 2019) <https://www.ittsystems.com/access-control-list-acl/>. Accessed 18 January 2020

10 Cisco, VPN filter Example. Configuration Manual (July 6, 2016) <https://www.cisco.com/c/en/us/support/docs/security/pix-500-series-security-appliances/99103-pix-asa-vpn-filter.html>. Accessed 18 January 2020

11 Techtarget, Active Directory. Ignite 2018 Conference coverage (Posted by Margaret Rouse, June 2018) <https://searchwindowsserver.techtarget.com/definition/Active-Directory>. Accessed 18 January 2020

12 Microsoft, Active Directory Security Groups. Documentation (Apri 19, 2017) <https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups>. Accessed 18 January 2020

13 Timothy A. Howes, LDAP - Key Advantages. Technical Report (July 27, 1995) <http://www.openldap.org/pub/umich/ldap.pdf> Accessed 18 January 2020

14 Microsoft, LDAP. Documentation (May 31, 2018) <https://docs.microsoft.com/fi-fi/previous-versions/windows/desktop/ldap/lightweight-directory-access-protocol-ldap-api?redirectedfrom=MSDN>. Accessed 18 January 2020

15 Servicenow, Configuration Management Database. Product description <https://www.servicenow.com/products/servicenow-platform/configuration-management-database.html>. Accessed 18 January 2020

16 CSO, What is IAM? Internet Article (James A. Martin & John K. Waters) <https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html>. Accessed 18 January 2020

17 Techtarget, Role-based Access Control (Posted by Margaret Rouse. Contributor Linda Rosencrance (September 2018) <https://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC>. Accessed 18 January 2020

18 Okta, Benefits of an intelligent RBAC strategy. Web article <https://www.okta.com/identity-101/what-is-role-based-access-control-rbac/>. Accessed 18 January 2020

19 NIST, Special Publication 800-113 (Guide to SSL VPNs). Publication (Sheila Frankel et al) <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152086>. Accessed 18 January 2020

20 VAHTI, Päätelaitteiden tietoturvaohje 5/2013 (The Government Information Security Management Board) <https://www.vahtiohje.fi/c/document_library/get_file?uuid=b1064d7a-83e5-4246-be9a-a8a84c8caaa0&groupId=10229>. Accessed 18 January 2020

21 Hackernoon, What is 2-Factor Authentication and Why Should You Care? Web article (Nitin Sharma. October 3, 2018) <https://hackernoon.com/what-is-2-factor-authentication-and-why-you-should-care-e8af5808d499>. Accessed 18 January 2020

22 Explainthatstuff, Two-Factor authentication. Web article (Chris Woodford. October 13, 2018) <https://www.explainthatstuff.com/how-security-tokens-work.html>. Accessed 18 January 2020

23 USDigitalMedia, USB Security and Two Factor Authentication. Web Blog (August 22, 2019) <https://www.premiumusb.com/blog/usb-security-and-two-factor-authentication>. Accessed 18 January 2020

24 OpenVPN, How To Authenticate Users With Active Directory. Configuration guide <https://openvpn.net/vpn-server-resources/how-to-authenticate-users-with-active-directory/>. Accessed 18 January 2020

25 OpenVPN, How To Authenticate Users With Active Directory. Configuration guide <https://openvpn.net/vpn-server-resources/how-to-authenticate-users-with-active-directory/>. Accessed 18 January 2020

26 Paloalto, Set Up LDAP authentication. Web Documentation (September 20, 2019) <https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/authentication/set-up-external-authentication/set-up-ldap-authentication>. Accessed 18 January 2020

27 Cisco, Configuring Dynamic Access Policies -Chapter 6. Web Documentation <https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/vpn/asdm_71_vpn_config/vpn_asdm_dap.pdf>. Accessed 18 January 2020