RECOMMENDATIONS TO SECURE ADMINISTRATION OF IT SYSTEMS

ANSSI GUIDELINES

ANSSI-PA-022-EN
24/04/2018

TARGETED AUDIENCE:

Developers **Administrators** **IT security managers** **IT managers** Users

Information

Warning

This document, written by ANSSI, the French National Information Security Agency, presents the **"Recommendations to secure administration of IT Systems"**. It is freely available at www.ssi.gouv.fr/en/.
It is an original creation from ANSSI and it is placed under the "Open Licence v2.0" published by the Etalab mission [24].
According to the Open Licence v2.0, this guide can be freely reused, subject to mentionning its paternity (source and date of last update). Reuse means the right to communicate, distribute, redistribute, publish, transmit, reproduce, copy, adapt, modify, extract, transform and use, including for commercial purposes
These recommendations are provided as is and are related to threats known at the publication time. Considering the information systems diversity, ANSSI cannot guarantee direct application of these recommendations on targeted information systems. Applying the following recommendations shall be, at first, validated by IT administrators and/or IT security managers.
This document is a courtesy translation of the initial French document **"Recommandations relatives à l'administration sécurisée des systèmes d'information [16]"**, available at www.ssi.gouv.fr. In case of conflicts between these two documents, the latter is considered as the only reference.

Document changelog:

VERSION	DATE	CHANGELOG
1.0	20/02/2015	Initial
2.0	24/04/2018	Taking feedback into account, reorganisation of the chapters and graphical revamping

Contents

1
Preamble

Second version of the guide

The first version of this guide was published in February 2015 and received a lot of feedback, from the public as well as private sector.

Convinced that the administration of an IT system (IS) remains a critical activity that must be treated with the greatest attention, ANSSI is publishing an updated version with in particular:

- a reorganisation of the chapters which implies a new numbering of the recommendations as well as new recommendations (a list of the additions as well as a backwards compatibility matrix is supplied in appendix A);
- a chapter now devoted to remote administration in light of the generalisation of this practice (on-call, facilities management, etc.);
- a chapter providing details on common use cases including the use of a bastion, the architectural principles for mutualising certain administrative resources or the administration of a disconnected IS.

Objectives of the guide

First of all, it is reminded that the administration of an IS entails a set of technical and non-technical measures that among other things aim to keep the IS in operating and secure condition and to manage the minor changes or major developments.

This guide describes the security objectives and the principles for developing a secure technical architecture for administration. It proposes elements that are useful in assisting with the design. It presents a few concrete use cases but does not intend to be complete.

This document is intended for readers that have a minimum amount of knowledge to apprehend the security recommendations that are presented and the ability to adapt these recommendations to their specific context and needs. One must also refer to its organisation's IT system security policy and to the results of the risk analysis in order to determine the most pertinent recommendations to implement.

Convention for reading

For a few recommendations, several architecture solutions are proposed which are distinguished by their level of security. The reader therefore has the possibility of choosing a solution that is in line with his security needs.

Furthermore, in an iterative approach for securing the administration of an IS, these various levels of security proposed can make it possible to set an architecture target and identify the steps to achieve it.

As such, the recommendations are presented in the following way:

- R*x* constitutes a recommendation in the state of the art;
- R*x* - and R*x* - - constitute alternative recommendations to R*x*, with a lesser degree of security and respectively decreasing.

Moreover, in this guide, the use of the verb "*must*" is voluntarily more prescriptive than the formulation "*it is recommended*".

How to approach this guide ?

This guide attempts to cover all of the themes linked to the administration of an IS and lists the recommendations for which the implementation can be more or less complex according to the context of the organisation. A linear application of this guide will not be suitable for all contexts.

After a first read in order to become familiar with the concepts, it is recommended to assess the organisation's level of maturity on the subject of administering an IS using the list of recommendations (p. 55). For each recommendation, specify whether it is "*complied with*", "*partially complied with*" or "*not complied with*". Once summarised, this analysis can be the starting point for an action plan aiming to comply as completely as possible with the recommendations of the guide while still keeping a critical mind with regards to the application context.

2
Administrators, key stakeholders in the security of the IT system

This introductory chapter, devoted to the role of the administrator, aims to present a complete lexicon concerning the administration of the IS and therefore serves as a reference for the entire document. It is also a summary of the various themes addressed.

2.1 The administrators in the ecosystem of the organisation's IS

An administrator is not only an essential stakeholder in the IT system but also a major contributor for the security thereof. He may be an employee of the organisation (referred to as an *internal administrator*) or a subcontractor of the organisation (referred to as an *external administrator*), independently of the location of the activity. In addition, whether he is a technical administrator (network, system) or functional administrator, the needs for access and privileges are generally not uniform; administrators can be grouped into categories.

An administrator is a critical resource invested with technical capacities with access to the organisation's business information. Indeed, he is distinguished from the other users by the privileges that are granted to him on the IT system. He has *administration privileges* that are required for the proper execution of *administration actions*.

Administration actions

All of the installation, deletion, modification and consultation actions for the configuration of a system participating in the IS and likely to modify the operation or the security of the latter.

It is necessary to clearly dissociate the various roles of an administrator on the IS: on the one hand, the role of a standard user of the IS without special privileges and on the other hand one or more administrator roles. This among other things results in the creation of a standard user account in order to use the IS outside of administration and one or more *administration accounts* dedicated to administration actions. Identifying and authenticating administrators are the subjects of chapter 7.

A station used for administration actions, called an *administration station*, is a hardware terminal; it can be fixed or portable according to the needs. It is covered in chapter 4.

An administrator carries out actions using *administration tools*, which are generally software, made available on an administration station or dedicated servers. An SSH client, a centralised console for

directory management, a Web portal for firewall administration are examples of administration tools. Chapter 6 addresses this subject.

In case of remote access for an administrator (e.g., on-call at home, travel, service performed outside the premises of the organisation), this is referred to as *remote administration* in chapter 10.

An integral part of the organisation's IS in the broad sense, the *administration IT system* is the subject of this guide. It includes all of the *administration resources* required to administer the IS at hand including the *administration stations*, the *administration tool servers* and the *administration infrastructures* required for the proper operation thereof (directory servers, DNS, etc.).

These resources are connected to an *administration network*, a communications network that conveys the internal flows of the administration IS and the *administration flows* intended for administered resources. This network is mentioned in chapter 5.

Figure 2.1, as an example, is a summary in the form of a functional representation.

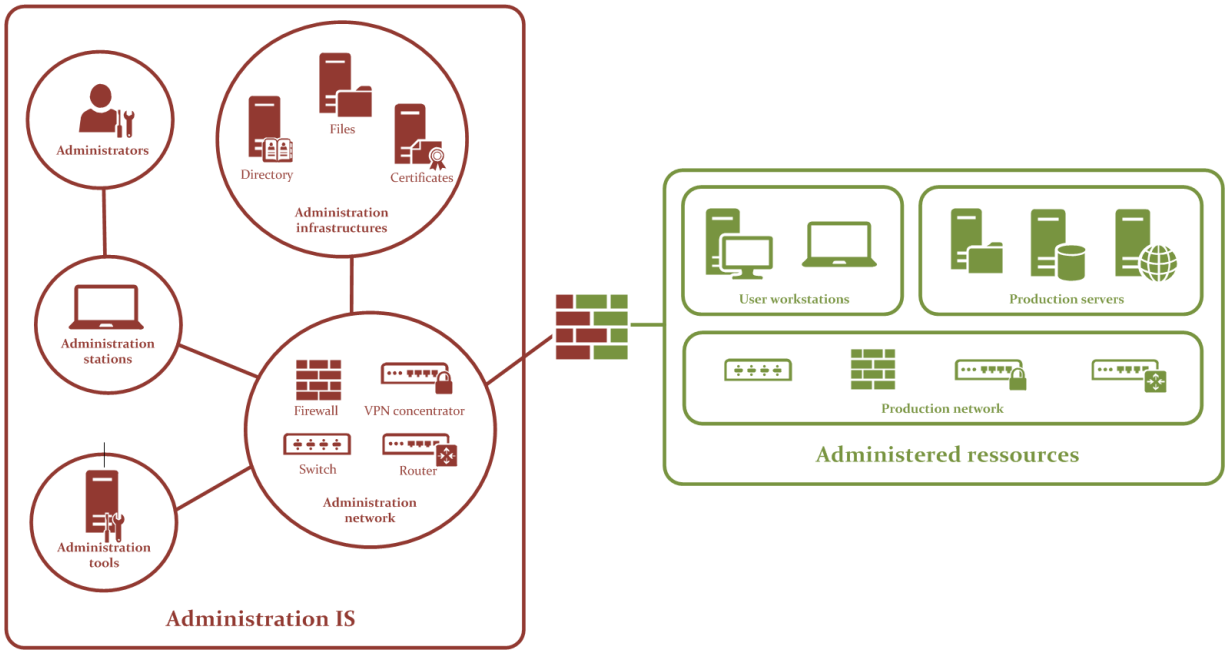

Figure 2.1: Functional representation of an administration IS and of administered resources

At the periphery of the administration IS, a secure exchange system, shown in figure 2.2 and presented in chapter 11, can be positioned for exchanges with other IS (e.g., an office environment IS connected to the Internet).

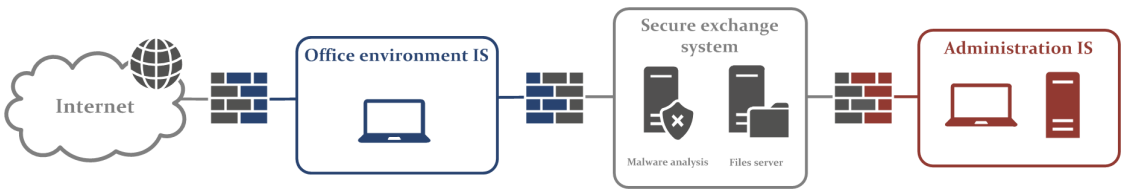

Figure 2.2: Functional representation of an administration IS and of a secure exchange system

2.2 Rights and duties of administrators

The functions of an administrator, which are complex, must be balanced between substantial powers and compliance with precise duties. In particular, an administrator of an IT system is bound to obligations of loyalty (compliance with ethical rules), transparency (compliance with the internal regulations and the IT charter) and confidentiality [1] (compliance with professional secrecy). Non-compliance with these duties can give rise to disciplinary sanctions, and even criminal sanctions. Appendix B covers the legal aspects in more detail, in particular the various rights and duties of administrators.

Firstly, the rights and duties of the employees, of which administrators are a part, regarding the use of the IT resources must be listed in an IT charter included with the internal regulations or the labour contract. The organisation can provide as a supplement a specific IT charter that applies to administrators. This charter must in particular instil vigilance among administrators with regards to the administration resources made available to them and on the instructions to follow in case of proven or suspected compromise, loss or theft. For any question pertaining to cybersecurity, an administrator must be able to refer to internal contacts of the organisation, who are clearly identified, whether or not they are technical personnels.

R1

Informing administrators of their rights and duties

An administrator must be informed of his rights and duties, in particular by referring to the organisation's IT charter.
It is recommended to develop a specific IT charter that applies to administrators.

The role of the administrator not only requires a high level of trust from the organisation with regards to the criticality of his actions on the IS, but also a high level of technical skills. The initial and ongoing training of administrators is indispensable in guaranteeing control of all of the skills required to exercise their functions.

R2

Training administrators at the state of the art in terms of cybersecurity

As a critical human resource for the IS, an administrator must be trained at the state of the art, in its skill areas and in the security of IT systems (e.g., systems security, network security, public key infrastructure).
ANSSI's guideline for a healthy information system [10] must be mastered.

Regardless of how the organisation is organised and the sharing of responsibilities (between architects and administrators for example), it is essential to design and keep up to date the documentation for the ISs: architecture diagrams, IP address plans, inventory of the privileged accounts, etc.

1. Refer to the guide for employers and employees developed by CNIL [1] including in particular sheet no. 7 for administrators.

R3

Having up-to-date IS documentation available

Administrators must have documents available that accurately reflect the current state of the ISs that they administer, especially mappings of the IS (system, network applications) that in particular clearly show the interconnections with the exterior.

3
General points on the administration IT system

3.1 Risk analysis and security objectives

Administration resources are privileged targets for an attacker. Indeed the high rights required to perform the administration actions and the wide access that is generally granted expose these resources to a high threat. In many cases of compromise or intrusion on these devices, the attacker takes control of the entire IS.

Risk analysis

This guide does not intend to establish a complete analysis of the risks; this essential work, which is proper to each IT system, is the responsibility of the organisations that are in charge of it, in liaison with the Chief Information Security Officers (CISO). The risk analysis can be carried out with the EBIOS method [19] for example.

As such, the architectures of the administration IS can vary according to the criticality of the administered IS or of the uses by various populations of administrators, with each one not having the same level of trust, for example between internal and external administrators.

R4

Carrying out a risk analysis on the administration IS and its ecosystem

Before any study on the technical measures to implement, a risk analysis must be conducted giving special attention to the security needs of the administration IS and its interconnections.
In a continuous improvement approach, it is recommended that the risk analysis and the implementation of the measures induced be reviewed at least once a year.

Security objectives

The first security objective of the recommendations of this guide is to protect the administration IS from any attempt of a compromise. Indeed, the most common compromise scenario is the execution of malware on the administration station – or on a station to which an administrator has connected with his administrator privileges. This malware can be introduced through Web browsing, by opening an attachment in a booby-trapped email or from a removable device.

Information

Malware can take advantage of the high privileges of an administrator session to execute actions such as:

- theft of password hashes on the station, for example via a memory copy (e.g., *Pass The Hash* attack which allows these hashes to be used again to access, without knowing the password and therefore without having to retrieve it, the resources of the IT system);
- installation of spyware (e.g., Trojan, keylogger);
- access to a command-and-control server[a];
- distribution of a worm.

The second security objective is to protect the administered IS from intrusions and compromise for which the administration IS would be an attack vector. In this case, it is sought to minimise the consequences on the administered IS of a compromise of the administration IS. Due to the high privileges of the administration IS on the administered IS, a malicious action is still possible but suitable partitioning of the administration IS must make it possible to prevent a complete compromise of the administered IS.

3.2 Trust zones and administration zones

In order to reduce the attack surface to IT attacks and the consequences in case of compromise, it is necessary to divide the administered IS into homogeneous zones called *trust zones* then to deduce *administration zones* therefrom within the administration IS.

Trust zone

A trust zone comprises exclusively homogeneous resources; it is administered by administrators of the same level of trust.

Breaking the administered zone down into trust zones can be determined by the combination of several homogeneity criteria, among which:

- business criticality (e.g., high, medium, low);
- organisational (e.g., internal or outsourced administration);
- exposure (e.g., to Internet, to suppliers, exclusively internal);
- regulatory (e.g., health data, personal data, data concerning national defence secrecy);
- geographical (e.g., breakdown by country).

By default, an administration zone corresponds to a trust zone. Cases of mutualisation are discussed in paragraph 12.2.

This dividing of the administered IS (and the consequences on the administration IS for the defining of the administration zones) must be carried out in the initial design phase as well as before

a. A command-and-control server (C&C) is a computer which gives orders to devices infected by malware and which receives information from these devices.

any significant change in the administered IS. It makes it possible indeed to feed the architectural work in order that all of the administration needs be processed with continuity.

Technical mechanisms for partitioning are then implemented in order to materialise the administration zones: filtering, encryption, authentication, etc. As such, by complying with the least privilege principle, a given administrator has access only to the administrative zones for which he has a real operational need, without it being technically possible to access another zone.

R5

Defining the trust zones of the administered IS and deducing the administration zones

Before any study of the architecture of the administration IS, the administered IS must be broken down into trust zones. This work makes it possible to deduce a dividing of the administration IS into administration zones.

3.3 Products qualified by ANSSI

Qualification [23] pronounced by ANSSI makes it possible to certify a certain level of security and of trust in the products [2] and the service providers. This process makes it possible to ensure in particular that the products fulfil the security objectives defined in the security targets that were approved beforehand.

It is recommended to use qualified products for the protection of the administration IS even if the organisation is not subjected to any regulatory text. Special attention will be given to the security target that specifies the qualified perimeter of the product (e.g., the dynamic filtering of the IP flows at layers 3 and 4 for a firewall) as well as the assumptions for the environment.

R6

Favouring the use of products qualified by ANSSI

Generally, it is recommended that the hardware and software used to protect the administration IS be qualified by ANSSI at the level required by the security needs. Otherwise, it is recommended that they have another security visa delivered by ANSSI [a].

Warning

It is recommended to always pay attention to the hardware and software versions to which they apply as well as the definition of the security target.

2. ANSSI qualified products include three levels: basic, standard and reinforced.
a. Refer to https://www.ssi.gouv.fr/en/security-visa.

3.4 Trust in the partitioning of virtualised environments

The use of virtualisation technologies is now common in order to mutualise resources, simplify operating tasks and reduce costs. However, trust in a virtualisation solution depends primarily on the trust given to the partitioning mechanisms that allow for several environments running on the same hardware to coexist. From a security standpoint, these mechanisms must guarantee a seal that is equivalent to that of physically separate environments.

In practice, the qualification process mentioned in paragraph 3.3 is difficult to apply to virtualisation technologies in light of the complexity of the design and developments as well as the multiples cases of integration.

Consequently, the precautionary principle must prevail: by default, it is therefore assumed that the partitioning between two virtualised environments, hosted on the same hardware, does not guarantee a sufficient level of trust from a security standpoint. This observation applies to any type of resource that can be virtualised, not only servers but also network devices (routers, switches…), security devices (firewalls, VPN concentrators…) or others.

Therefore, virtualisation on the same hardware can be used only for having instances of the same trust zone coexist, that have among others:

- the same security needs (confidentiality, integrity, availability);
- the same level of exposure, i.e. accessible from zones and by people from a trust level and with homogeneous privileges.

In the case at hand, the precautionary principle therefore consists in dedicating virtualisation hardware for the administration IS.

For example, a tool server and a directory server of the administration IS, if they are virtualised, can be hosted on the same hardware with the condition that the latter is dedicated to them and that it is for example different from the one used for business applications (cf. figure 3.1). In another technical area, virtualised devices for routing and filtering for the flows internal to the administration IS must also not be mutualised on the same hardware as virtualised devices that enable access to the production services.

R7

Dedicating hardware in case of virtualisation of administration infrastructures

In case of virtualisation of administration infrastructures, the corresponding virtual instances must be deployed on dedicated hardware that is not mutualised with other virtualised infrastructures.

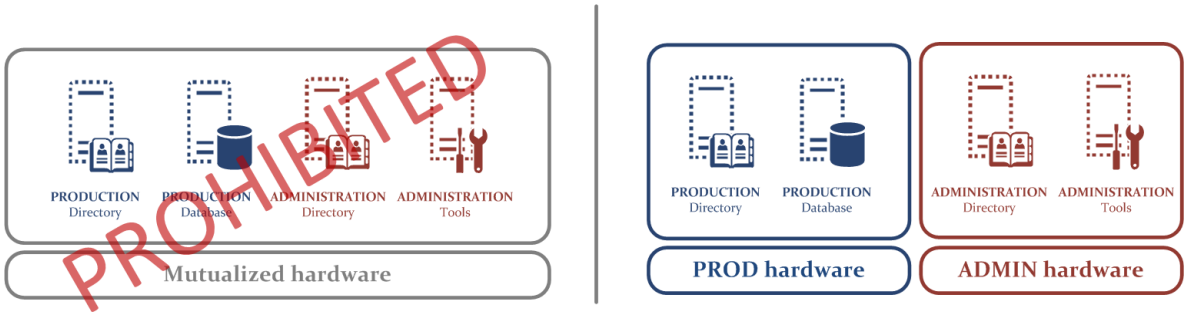

Figure 3.1: Partitioning virtualisation hardware for servers

Warning

Generally, virtualisation products are complex and require perfect control in order to guarantee secure usage: configuration of the internal network, knowledge of the information flows between the virtual machines, targeted set up of authenticated encryption, etc.

4
Administration station

4.1 Managing the administration station

As an entry point of the administration IS, the administrator's workstation is a critical component by nature as it has extended access and privileges. Furthermore, it generally processes sensitive information for the IT system (configurations, architecture dossiers, software versions deployed, passwords, etc.) and the technical capacity to access business information. It must therefore be subject to hardware and software securing in order to restrict as best as possible the risks of a compromise.

Firstly, it is indispensable for the organisation to keep control of the administration station made available to administrators, whether the latter are internal or external. Any practice such as "Bring Your Own Device" (BYOD), which is not in general recommended, is to be prohibited for an administration station.

R8

Managing and configuring the administration station

The administration station has to be managed by the organisation – or otherwise a mandated service provider. *Under no circumstances* is the use of a personal device to be tolerated for the administration of an IS.

Warning

Entailing a risk of hardware entrapment, beyond controlling the procurement process and in particular the security conditions thereof, administrators need to have their awareness heightened as to the physical protection of their administration station.

4.2 Architecture of the administration station

In order to respond to the duality of the needs of administrators (performing administration actions from a secure environment on the one hand and access to an office environment IS[3] as a user on the other hand), three architecture solutions can be considered. They are presented in decreasing order of security with regards to the security objectives that are set:

- a dedicated administration station;
- a multi-level administration station;
- an administration station with remote access to an office environment IS.

3. The office environment IS is spoken of in a broad sense, i.e. everything that is not the administration IS.

A dedicated administration station

The solution that provides the best guarantee from a security standpoint consists in using two physically separate stations (cf. figure 4.1), respectively for the administration actions and for the other uses (e.g., access to office services, access to the Internet).

R9

Using a dedicated administration station

The main measure of security consists in dedicating a physical workstation to the administration actions. This station has to be separate from the station that allows access to the conventional resources that can be accessed on the organisation's IS (business resources, internal mail system, document management, Internet, etc.).

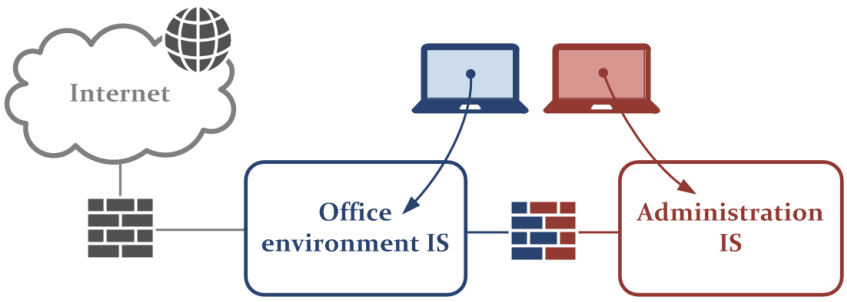

Figure 4.1: Dedicated administration station

A multi-level administration station

The principle of a multi-level station consists in having several software environments (two in general) on the same physical station by using virtualisation or containerisation technologies.

Mechanisms for hardening the core and partitioning make it possible to isolate these environments in order to reduce the risks of a compromise at a high sensitivity level or information leak from the high sensitivity level (here the administration IS) to the low sensitivity level (here the office environment IS).

This solution (cf. figure 4.2) offers a lesser level of security than a physical separation. In this exclusive case of the administrative station derogating from R7, it must absolutely undergo an evaluation of the trust of the isolation and partitioning mechanisms. Indeed, using this solution, if it is not trustworthy, can give a false sense of security. It is moreover preferable that these mechanisms be managed at the level of the system, not by a user application (cf. figures 4.3 and 4.4).

R9 -

Using a multi-level administration station

If there is no physically dedicated administration station, using virtualisation or containerisation technologies in order to obtain a multi-level system can be considered, if the partitioning of the environments is carried out with mechanisms that are evaluated as being trustworthy at the system level.

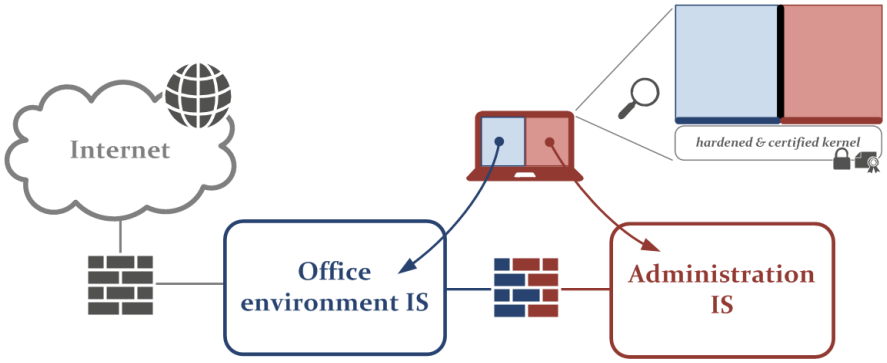

Figure 4.2: Multi-level administration station

Figure 4.3: Administration station hosting an office environment virtual machine

Figure 4.4: Office environment station hosting a virtual administration machine

An administration station with remote access to the office environment IS

A last solution, with a lesser degree of security, consists in using on a daily basis a hardware administration station that allows for access to the office environment IS via remote access (cf. figure 4.5).

In this architecture, the attack surface of the administration IS is indeed increased through the use of a remote access client running on the administration station. In the event the remote access server located in the office environment IS is compromised, an attacker could then run back through the established communication channel in order to compromise the administration station.

In any case this practice requires stronger mastery of the interconnection between the two ISs.

Warning

Note that the reverse solution, which consists in accessing from an office environment station to an administration station via remote access, is to be prohibited (cf. figure 4.6).
Indeed, as the office workstation potentially has access to the Internet, the compromise of it could allow an attacker to spy on the actions performed from the station (keys struck, screen copies), especially the connections initiated to the administration station (e.g., IP address, password).
An attacker could then replay these connections and, via bouncing, access the administration tools then the administered IS.

In addition, using remote access software requires configuration precautions that aim to reduce the exchange functions between the local system (administration) and the remote system (office environment). Lacking an evaluation on the date this document was written, the exchange mechanisms of remote access software cannot, *a priori*, be considered as being trustworthy. In a non-exhaustive manner, the information exchange functions to be deactivated are:

- the advanced cut/paste functions;
- screen sharing;
- the peripheral device handling function (USB, printers, etc.);
- network sharing.

Therefore, setting up a secure exchange system, as detailed in chapter 11, may be required.

In this derogatory case for architecture, it is imperative that:

- a filtering of the remote access flows to the office environment network be carried out by a firewall;
- authentication on the administration station be carried out using the directory of the administration IS;
- authentication on the office environment be carried out using the directory of the office environment IS.

R9 --

Using an administration station with remote access to the office environment IS

If there is no administration station that is physically separated from the office environment station nor a trustworthy multi-level system, a solution with a lesser degree of security can consist in the administrators:

- using their station for administration actions;
- accessing, via remote access only, to their office environment (physical or virtual, for example: *Virtual Desktop Infrastructure*) from this administration station.

In this case, the functions that allow for exchanging information between the two environments must be deactivated.

Warning

Note that this solution is not recommended for administering critical infrastructures (e.g., hypervisors, directories).
Moreover, in order to be able to react in a timely manner in the event of a crisis, it is recommended to have a procedure for deactivating remote access to the office environment IS from the administration stations.

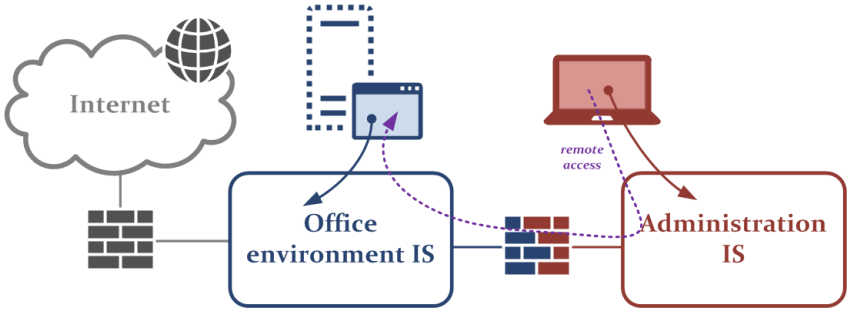

Figure 4.5: Physical administration station with remote access to a virtualised office environment

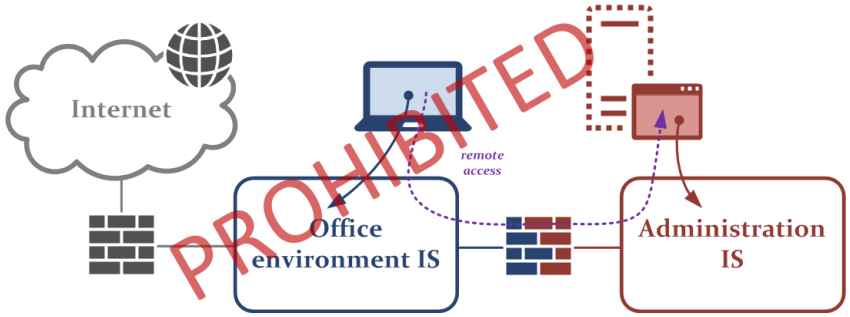

Figure 4.6: Physical office environment station with remote access to a virtualised administration environment

Information

As a supplement to the presentation of these three architecture solutions of the administration station, paragraph 12.3 covers the coexistence of several solutions.

4.3 Measures for securing the administration station

Information

All of the following recommendations apply regardless of the architecture solution chosen beforehand for the administration station.

Access to the Internet

Access to the Internet significantly increases the attack surface for IT attacks and favours a large number of attack vectors: Web browsing, email, opening files or running downloaded programs, etc. As such, it is very difficult to guarantee the integrity of a station that has access to the Internet.

R10

Blocking all access to the Internet from or to the administration station

The administration station must not *under any circumstances* have access to the Internet.
This recommendation in particular includes Web browsing and the use of electronic mail connected to Internet, even if these services are filtered by secure gateways for Internet access.

Consequently, access to the Internet and to electronic mail accounts can be authorised only from office environments, which themselves are subjected to filtering through the organisation's Internet access gateways.

Regarding the retrieval from the Internet of security updates for the station, details on the implementation of relay servers is provided in chapter 8. Other exchanges from or to the Internet are addressed in chapter 11 on exchange systems.

Securing software

In order to reduce the risks of compromising the administration station, the controlling and the hardening of its software and of its configuration are imperative.

Configuration actions must be conducted for the security of the operating system. For this, it is recommended to refer to the security guidelines proposed by the manufacturers. The latter describe configurations that are suited to their solutions and form a first step in securing the system. ANSSI also published guidelines for this purpose, for example on Linux [3], Applocker [8] or Windows 10 [7] [6].

R11

Hardening the operating system of the administration station

The guidelines of the manufacturers for securing the systems of the manufacturers must be applied. At least the following points must be addressed:

- deactivating unnecessary services;
- applying restricted rights according to the real operational need;
- activating and configuring the local firewall in order to prohibit any incoming connection and limit outgoing flows according to the real operational need;
- hardening the system configurations (for example for Windows: GPO, Applocker, SRP or, for Linux: SELinux, AppArmor, kernel hardening);
- activating all of the update mechanisms in compliance with the recommendations in chapter 8 dedicated to security maintenance.

Administrators must not be able to modify the configuration of the administration station. For this, they must not be integrated into the local "Administrators" group of the station. Most of the administration actions are generally done using Web browsers, tools of the thin client type or through the command lines (e.g., `ssh`) and therefore do not require particular privileges on the station.

This measure fulfils a double objective: preventing human error which would result in a drop in the level of security of the station and limiting the consequences of the execution of malware.

R12

Limiting administration privileges on the administration station

By default, administrators must not have administration privileges on their administration workstations. These privileges must be granted solely to administrators who are in charge of administering administration stations.

So as to significantly limit the attack surface of the system, only software – as well as updates to it – that has been validated beforehand according to a defined control process should be used. For this, cumulative verifications on the binary or configuration files to be installed can be:

- technical: virus scanning, sandbox scanning, digital signature verification, traceability using a hash, etc.;
- organisational: checking the source of the download, of the sender, etc.

Making tools available to administrators can be done using "remote distribution" (or "remote deployment") tools, a Website or through dedicated network sharing, with the latter being accessible only on the administration IS.

R13

Limiting the software installed on the administration station

It is recommended to install on the administration station only software and tools that are useful for administration actions. To do this, it is necessary to:

- draw up and maintain the list of useful administration tools;
- implement a process for validating and distributing administration tools according to technical and organisational criteria.

Encryption

The hard drive on the administration station can contain sensitive data, useful for accessing the IT system. Loss or theft of the station is detrimental as it could lead to a compromise of this data.

R14

Encrypting all of the storage devices used for administration

It is recommended to carry out full encryption of all of the storage devices (hard drives, removable storage devices, etc.) used for administration actions.

Warning

Laptop computers are in particular exposed to the risks of loss or theft. In the framework of digital nomadism (cf. chapter 10), this recommendation is of an indispensable nature.

The encryption systems used must guarantee a certain level of robustness and be adapted to the sensitivity of the data to be protected. Such systems are in the catalogue of products that have been qualified by ANSSI.

In addition, using encryption implies developing a process linked to the life cycle of the secrets (e.g., initialisation, storage, retrieval in case of loss).

5
Administration network

The administration network is defined as the communications network over which travel the flows internal to the administration IS and the administration flows intended for administered resources. This network must be the object of specific measures for securing in phase with the risk analysis and the security objectives described in paragraph 3.1.

5.1 Protecting administration resources

Just as with the recommendation on administration stations, implementing an administration network that is physically dedicated to administration resources offer the highest level of security against a compromise of the administration IS and guarantees strong partitioning with any other network that may potentially be connected to the Internet.

In order to prevent connecting undesirable devices to this dedicated administration network (e.g., office workstations, personal stations), network authentication is recommended as a supplement, for example via the implementation of the 802.1x protocol.

R15

Connecting the administration resources on a dedicated physical network

The administration resources (e.g., administration stations, tools servers) must be deployed on a network that is physically dedicated for this purpose.
Where applicable, it is recommended that the administration stations authenticate in order to access the administration network.

If the strict application of this recommendation is technically impossible (e.g., over an extended network) or is disproportionate with respect to the security needs, an alternative with a lesser degree of security can be considered based on a dedicated software network.

R15 -

Connecting the administration resources on a dedicated IPsec VPN network

If there is no physically dedicated network, the administration resources must be deployed on a software network dedicated for this purpose by implementing network encryption and authentication mechanisms, namely the IPsec protocol. As a supplement, software segmentation mechanisms (VLAN) and network filtering are recommended in order to limit exposure of the IPsec VPN concentrator to the administration stations only.
For the implementation of the IPsec protocol, the recommendations in ANSSI's guide [13] must be applied.

Grouping administration resources by trust zone makes it possible to set up pertinent partitioning and the adequate network filtering measures within the administration IS. Furthermore, in order to guarantee the partitioning of the administration IS with respect to the outside, perimeter filtering must also be provided. In the framework of security maintenance, the latter must be the object of a regularly revised procedure. In this way, obsolete, unnecessary or excessively permissive filtering is deleted or, otherwise, deactivated.

R16

Applying an internal and perimeter filtering to the administration IS

Regardless of the network solution retained, network filtering between the trust zones must be implemented within the administration IS. Moreover, all of the interconnections with the administration IS must be identified and filtered. A flow matrix, limited to the real operational need, must be developed and reviewed on a regular basis in order to ensure the traceability and the monitoring of the filtering rules.

Information

ANSSI publishes recommendations for defining a network filtering policy of a firewall [12] and for the cleaning thereof [14].

Figure 5.1 shows recommendations R16 and R15 (diagram on the left), R16 and R15- (diagram on the right). The illustration of R15- , on the right, represents only administration stations connected with IPsec VPN (conventional case when deploying a VPN client). However, it is entirely possible to consider connecting other administration resources in the same way.

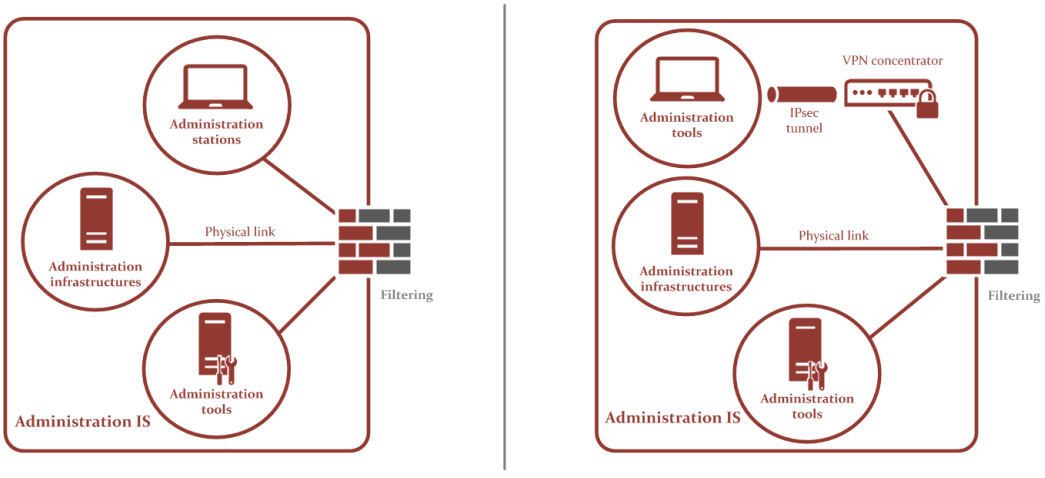

Figure 5.1: Administration networks with filtering function

5.2 Access to administered resources

Access to the administered resources must be controlled, not only at the local level using application configurations on these resources, but also at the network level via additional measures for network blocking or filtering in a defence-in-depth approach.

Local securing of access to the administered resources

In order to filter as close as possible access to an administered resource, it is recommended to implement local filtering, for example using an application firewall with a flow matrix that is limited to strict operational needs. In particular, only the identified administration resources can access the administration services. For example, the production service of a Web server can be accessed on port TCP/443 (HTTPS) by all of its legitimate clients and its administration service can be accessed on port TCP/22 (SSH) by the administration resources that are identified for this purpose.

R17

Applying a local filtering on the administered resources

In order to control access as close as possible to the administered resources, it is recommended to apply a local filtering to them that corresponds to strict operational needs.

Information

Some systems, for example content management systems or Microsoft Active Directory service, do not distinguish the listening port of the production and administration services (same TCP port). In this case, applying R17 is always necessary but is not sufficient. The security of the administration at the administered resource level in the end relies on the application configuration of the service (e.g., access control, rights management) and its robustness; attention must therefore be given to this but that is not the purpose of this guide.

Implementing a dedicated administration interface

As soon as it can be carried out technically on an administered resource, the segregation of production and administration interfaces is recommended. This measure not only guarantees a local filtering that is more specific (e.g., an administration service is allowed only on the administration interface) but also increases availability of the administered resource in case of denial of service on the production interface.

Separating into physical network interfaces offers a maximum level of security and as such makes it possible to dissociate network filtering devices respectively on the production and administration networks. Otherwise, a separation into virtual network interfaces is recommended.

If this separation cannot be carried out from a technical standpoint on a system, then the application of local measures, including recommendation R17, must be all the more so strict.

R18

Dedicating an administration physical network interface

It is recommended to dedicate a physical administration network interface on the administered resources by ensuring the following prerequisites:

- the software services that allow for the execution of administration actions must listen only on the administration network interface provided for this purpose;
- the internal functions of the operating system must not allow for the routing of information from the production network interfaces to the administration network interface of the same resource. They must be deactivated (e.g., deactivating *IPForwarding*).

R18 -

Dedicating a virtual administration network interface

If there is no physical administration network interface, it is recommended to dedicate a virtual administration network interface on the administered resources. The same prerequisites as R18 apply.

Information

Some manufacturers offer remote management interfaces (e.g., Cisco IMC, Dell RAC, HP iLO) that provide access to the low layer of the device. Therefore, if they are used, they must be considered as specific administration network interfaces and connected to the administration network. According to the risk analysis and the organisation of the administration teams, these interfaces can be connected in a different zone of the administration of the higher layers.

It is necessary to ensure that it is not possible for an attacker, who has taken control of an administered resource, to use the administration network interface to bounce to the administration resources. Consequently, only the flows initiated from the administration stations or servers to the administered resources must be authorised by default. The rolling up of event logs from the administered resources (e.g., client syslog) to the administration IS can form an exception.

R19

Applying a filtering between administration resources and administered resources

Recommendation R16 must be rigorously applied between the administration resources and the administered resources.

Likewise, it is necessary to ensure that it is not possible for an attacker, who has taken control of an administered resource, to use the administration network interface to bounce to the other administered resources. Consequently, all communication between the administered resources must be prohibited through the administration network. In this framework, it is possible to have recourse to:

- a network filtering based on a "micro-segmentation" (an administered resource = a sub-network), this practice can however represent a certain operational complexity;
- the use of the Private VLAN (PVLAN) functionality on the switches (cf. the ANSSI guide [5]).

R20

Blocking all connections between administered resources through the administration network

A measure for network blocking or filtering must be implemented between administered resources in order to prohibit any attempt of a compromise via bouncing through the administration network interfaces.

Case with a wide area network

In the case of multi-site architectures or wide area networks, the administration resources can be distant from the administered resources. The administration flows then potentially transit via a third-party transport network [4]. In this case, it is necessary to protect the administration flows for confidentiality, integrity and authenticity.

R21

Protecting the administration flows transiting over a third-party network

If the administration flows travel through a third-party network or outside of the premises with a suitable level of physical security (e.g., portion of dark fibre passing through the public space), the latter must be encrypted and authenticated from end-to-end until reaching another zone of the administration IS or another resource to administer. In this case, an IPsec tunnel must be established.
For the implementation of the IPsec protocol, the recommendations in ANSSI's guide [13] must be applied.

Figures 5.2 and 5.3 respectively illustrate access to the administered resources in the case of a local network and a wide area network.

4. A transport network is said to be third-party when it is not controlled by the organisation (e.g., Internet or a telecom operator's network).

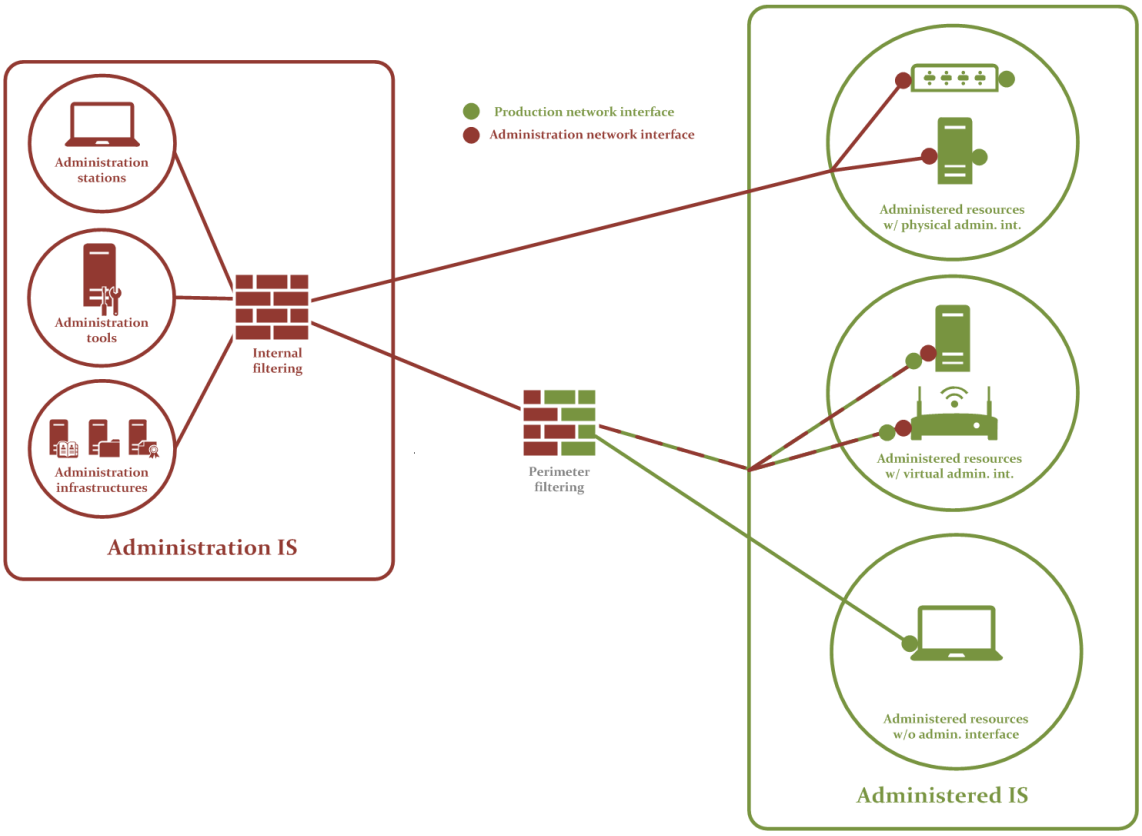

Figure 5.2: Administration, over a local network, through dedicated administration interfaces (physical or virtual) or a production interface

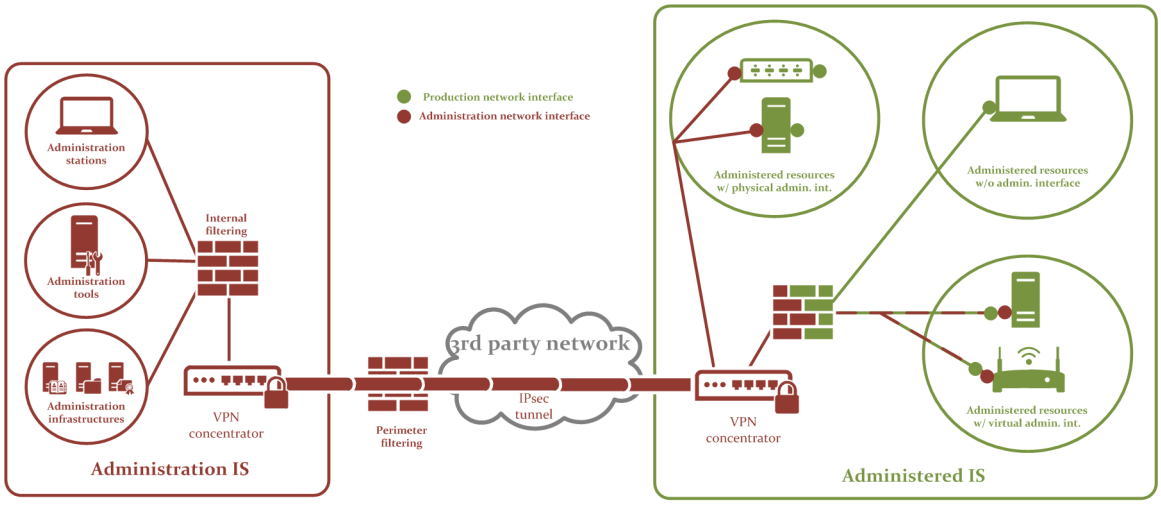

Figure 5.3: Administration, over a wide area network, through dedicated administration interfaces (physical or virtual) or a production interface

6
Administration tools

Administration tools, software that allows for the carrying out of administration actions, are made available to administrators, either locally on their administration station or in an offset manner and centralised on servers. Specific measures for protecting them from compromise attempts or illicit use must be implemented.

6.1 Partitioning the administration tools

In the continuity of the principles for reducing the attack surface described in paragraph 3.2, the main measure aims to segregate the administration tools by administration zone. Recall that one or several trust zones of the administered IS correspond to an administration zone of the administration IS.

Local administration tools

In the case of local administration tools at the administration station, partitioning by administration zone is difficult to apply. Recall that these tools must be deployed according to strict operational needs in accordance with R13.

Centralised administration tools

In the case of centralised administration tools, implementing dedicated servers by administration zone allows for implementing the partitioning sought and facilitates updating tools.

R22

Deploying the administration tools on dedicated and secure servers by administration zone

Administration tools must be deployed by administration zones according to the real operational need. This measure can result in implementing dedicated tools servers, integrating for example administration tools proposed by software or hardware vendors (e.g., thin client or Web service that interacts with the administered resources). The recommendations for securing software on administration stations (R10, R11, R12, R13, R14) must be applied, as soon as possible, to the administration tools servers.

As a supplement, implementing mechanisms for physical network partitioning or logical network segmentation (e.g., VLAN) and filtering (e.g., firewall) must guarantee only legitimate connections from the administration stations to the administration tool servers.

This practice contributes, furthermore to limiting the risks of a compromise, via bouncing, from one zone to another.

R23

Applying a filtering between the administration stations and the administration tools servers

Recommendation R16 must be rigorously applied between the administration stations and the administration tools servers by authorising only flows at the initiative of the administration stations.

6.2 Securing the administration flows

Whatever partitioning measures are retained, the administration flows require protocols that use encryption and authentication mechanisms (e.g., SSH, HTTPS, SFTP). The objective consists in reinforcing the confidentiality, integrity and authenticity of the administration flows.

R24

Using secure protocols for administration flows

It is recommended to systematically use, when they exist, administration protocols and tools that use robust authentication and encryption mechanisms (cf. *RGS* [20]), giving preference to standardised and proven secure protocols (e.g., TLS or SSH). Where applicable, non-secure protocols must be explicitly deactivated or blocked.

Warning

Some tools may flaunt the use of security mechanisms but their implementation may not be compliant with the state of the art. It is therefore necessary to provide for example any traces generated by these tools (e.g., password hash) and to check the encryption of all of the information.

Some protocols or administration tools are obsolete and do not implement these encryption mechanisms. In this case, the use of IPsec VPN, from the tools server or administration station to the nearest administered resource, can make it possible to overcome these shortcomings.

R24 -

Protecting where applicable the administration flows in an IPsec VPN tunnel

If there are no dedicated administration interfaces or administration tools that allow for end-to-end encryption and authentication, the administration flows must be protected by implementing an IPsec VPN tunnel, with mutual authentication via certificates, from the tools server or the administration station to the administered resources. This IPsec VPN tunnel must be established as close as possible to the administration resource and the administered resource.

6.3 Break or continuity in the administration flows

According to the security needs expressed in the framework of the risk analysis, it may be desired to either provide a break in the exchanges between the administration station and the administered resource, or to guarantee the end-to-end establishment of an authentication then a session. The following paragraphs illustrate the two cases of use: with or without a protocol break.

Figure 6.1 shows the use case of implementing bouncing in an administration zone that makes it possible to apply a certain quantity of processing such as filtering connections, authentication of administrators on a front gateway, access control or the logging of the actions performed and the commands executed by the administrators.

R25

Favouring a protocol break for traceability needs

A protocol break must be favoured if access traceability is needed.

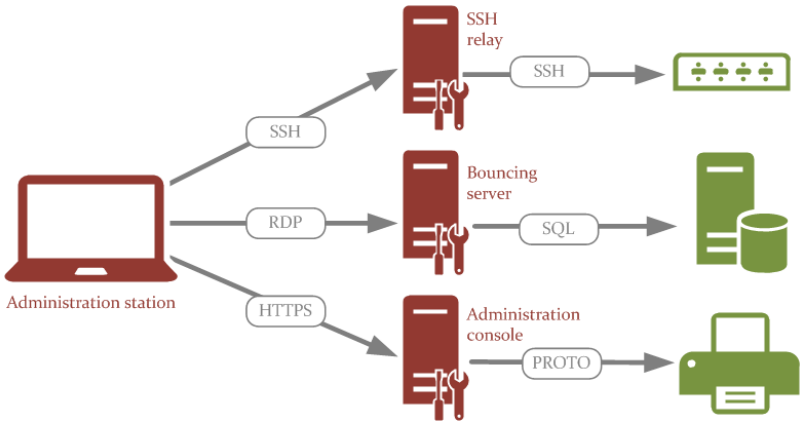

Figure 6.1: Administration with protocol break

Information

Paragraph 12.1 provides more details on the architectural issues linked to administration bastions.

For the other use case, without a protocol break, the objective consists in not interrupting the secure session, based on trusted encryption mechanisms (cf. figure 6.2).

In this case, it is still possible to implement a protocol interception mechanism in order to provide traceability for administration actions. This practice of intercepting flows is however to be considered with precaution and is not desirable in certain cases; ANSSI publishes a guide [15] that addresses the technical and legal aspects linked to these uses for the HTTPS protocol.

R26

Renouncing a protocol break for confidentiality needs

The absence of a protocol break must be favoured if confidentiality in the administration flows is needed.

> Where applicable, the protocols used must all the more so be secure and configured in the state of the art in accordance with R24.

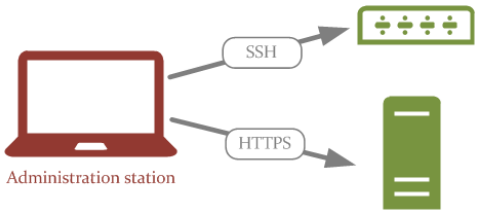

Figure 6.2: Administration without protocol break

7
Identification, authentication and administration privileges

7.1 Identification

It is indispensable to dissociate the roles on the IS, in particular for an administrator: simple user or administrator with privileged rights granted over the administered resources. In addition, an administrator can intervene over several technical areas. Consequently, separate accounts must be created and used according to the role (user or administrator) as well as separate administration accounts per technical area.

Logically, and in order to prevent any replay of a potentially compromised secret, the associated secrets (e.g., PIN code, password, private key) must be different between accounts.

R27

Using dedicated administration accounts

The administrator must have one or more dedicated administrator accounts, separate from his user account. Authentication secrets must be different according to the account used.

The identifiers and secrets associated with the administration accounts are part of the first targets in an IT attack. Stealing this information greatly simplifies the compromise of an IT system and makes it more silent. The directories that participate in identifying and authenticating administrators on the administered resources are critical elements. An attacker that gains control of them indeed makes it possible to have all of the privileges over the administered IS.

R28

Protecting access to the directories of the administration accounts

The directory or directories that contain the administration accounts have to be protected for confidentiality and integrity and must not be exposed to environments of lesser trust (e.g., office environment IS).
It is recommended to deploy a directory that is dedicated to the administration IS as an administration infrastructure. The latter manages the administration accounts and access control to the administered resources.

Additional technical measures that restrict the use of administration accounts on the workstations must be implemented.

R29

Reserving administration accounts only for administration actions

Administration accounts must be used *exclusively* for administration actions. In particular, no administration account must be used for office environment actions or for opening work sessions on stations others than those reserved for administration actions.

By default, the built-in administration accounts (e.g., root, admin), present on the devices during installation must not be used. The use thereof must remain exceptional and restricted to a highly limited number of administrators. Indeed, these accounts do not make it possible to account precisely for the actions performed on the devices. This also makes it impossible to implement pertinent access control to the administration tools and the segregation of rights. Only creating individual administration accounts can meet these needs.

R30

Using by default individual administration accounts

Individual administration accounts must be assigned to each administrator.
The built-in administration accounts must not be used for current administration actions and the associated secrets must be accessible to only a highly restricted number of people.

Information

Assigning individual accounts is usually the object of a naming convention. If, for example, Jo Smith has the identifier `jsmith` for user account, two possible options for the identifier of administrator account are:

- an identifier that is derived directly from the user account: `adm-jsmith`;
- an anonymised identifier (but still individual): `adm-0x2a`.

This second method, which is more restrictive from an operational standpoint because it requires keeping a table of correspondence up to date, makes it complicated for attackers to target the identification of the administrators (e.g., phishing efforts, attack on the user account).

In order to detect as early as possible the signs of a possible compromise and apply the precautionary and corrective measures, it is imperative to audit the use of administration accounts. Appendix A of the guide [11] describes the elements to be audited. Logging and the supervision of security are covered in paragraph 9.2.

R31

Logging events linked to administration accounts

The mechanisms for event auditing concerning administration accounts must be implemented. In particular, the following logs must be activated:

- session openings/closings;
- account locking;
- account management;
- security group management.

The administration accounts must be monitored rigorously over time: creation, deletion or modification. The associated privileges must be adjusted as many times as necessary.

R32

Providing an administration account management process

An organisational and technical process for managing administration accounts and the associate privileges must be implemented and be part of a procedure for control and revision on a regular basis.
Concerning the organisational aspect, this process must be resilient enough to overcome the absence of one or several stakeholders.
Operational organisations must be associated in the design phase and are then responsible for the application thereof.

7.2 Authentication

Authentication makes it possible to ensure the identity of an administrator or of an administration service account before granting access to the administered resources. In order to define the type of authentication to implement, the *Référentiel Général de Sécurité* (*RGS*), and in particular appendices B1, B2 and B3, provide more details on the encryption and authentication mechanisms.

R33

Referring to the RGS in order to choose the authentication mechanism

In the design or revision phase of the administration architectures, reference should be made to appendices B1, B2 and B3 of the *RGS* [20] in order to use the authentication mechanism in compliance.

The built-in administration accounts (e.g., root, admin) generally have a default password, that can be consulted on hardcopy documentation or on the Internet. They therefore need to be modified right from installation.

R34

Modifying the default passwords of built-in accounts

The default passwords for built-in administration accounts must be modified at the time the device or service is installed. Preferably, the new passwords are different per device and are sequestered.

Administrators may be forced to use a large number of secrets, which makes the compliance with good practices (e.g., complexity, length, renewal – cf. guide [2] for example) difficult to maintain over time. Despite the implementation of a centralised authentication directory, the number of residual passwords may remain high due to devices or softwares that are incompatible with these authentication solutions. Storing them in a file, as clear text or with weak encryption, must however be proscribed.

R35

Storing passwords in a password safe

It is recommended to use a password safe that has a security visa [a] in order to securely store passwords on the IS administration.

Various factors contribute to the authentication robustness. They are to be taken into account when choosing authentication mechanisms and can be distinguished as follows:

- what I know (e.g., a password, a PIN code);
- what I have (e.g., a fingerprint, an iris);
- what I possess (e.g., a smart card);
- what I know how to do (e.g., handwritten signature).

An authentication is said to be multi-factor when at least two different factors are used. In IT, it is common to combine the ”what I know” and ”what I possess” factors.

Warning

Multi-factor authentication provides real security only if, in a cumulative way:

- authentication via a simple password is rendered impossible;
- the factors stem from independent channels (e.g., certificate stored on a smart card and a memorised PIN code).

R36

Favouring double-factor authentication for administration actions

For administration actions, it is recommended to use authentication that includes at least two factors.

For the ”what I possess” factor, the use of authentication hardware of the smart card or USB token type is common and recommended. This hardware carries a portion of the secret elements which contributes to the authentication process. The other factor can be for example a PIN code.

Authentication elements are in general digital certificates of the x.509 type. This technology requires the generation of certificates and induces the notion of trust in the certification chain and into the public key infrastructure (PKI). Indeed, although the use of certificates appears to be more robust than the password, its robustness is mostly based on the trust in the life cycle of certification (generation, signature, storage, revocation) and, consequently, in the service provider who is providing these services.

R37

Using trusted digital certificates for authentication

The use of digital certificates as an element that contributes to authentication is recommended.
These certificates should be acquired from an ANSSI-qualified digital certification services provider or to deploy a public key infrastructure that is compliant with the requirements of the *RGS* [20] that supervises this area.

a. Refer to `https://www.ssi.gouv.fr/en/security-visa`.

Authentication for administrators can be local or centralised. Except for special cases, using a centralised authentication server is recommended. Indeed, this solution makes it possible to prevent "sedimentation" of accounts created over time, favours better monitoring of accounts and compliance with the security policy (e.g., renewing authentication secrets, locking). Several technologies make it possible to respond to this type of architecture: Kerberos, RADIUS, etc.

R38

Favouring centralised authentication

It is recommended to favour a centralised authentication architecture instead of local management directly on the administered devices.
Where applicable, using multi-factor authentication is a high priority as it provides additional trust in the system and resists brute force attacks better.

7.3 Administration/root privileges

The administration accounts directory is used in particular to configure the privileges in order to restrict access to the administration of administered resources or to administration tools. An administrator must be able to access and administer only the resources that he is authorised to access and administer. In addition, this directory must itself be protected from any untimely modification and from any uncontrolled access on critical attributes, such as fields of the *password* type.

R39

Respecting the least privilege principle in granting administration privileges

Administration privileges must be implemented in the administration account directory while respecting the least privilege principle.
In the specific case for the most privileged rights on the directory itself, only administrators of the administration IS can have them.

In order to facilitate the management of administration privileges (adding, modifying and deleting), it is recommended to create groups. A group contains, according to the strict operational needs, all of the administration accounts that must have homogeneous administration privileges over one or several administered resources. The privileges on these resources are as such granted to the groups, not to the accounts.

R40

Granting administration privileges to groups

Administration privileges must preferably be granted to groups of administration accounts rather than unitarily to administration accounts.

In addition, security policies are to be defined and deployed in order to ensure access control to administration tools. This consists in controlling the access of different categories of administrators through administration account profiles. Among the elements to be defined, at least the following should be provided:

- account privileges: the various accounts (administrators, services, systems) must be granted the privileges that are strictly necessary to perform the administration actions on the devices or services identified;

- access authorisation to the tools: access control rules must be defined so as to specify the particulars for accessing administration tools such as times, the type of authentication, authorised and/or prohibited actions, etc.;
- when applicable, the password policy: minimum and maximum length, modification period, number of login attempts before the account is locked, history, etc.

R41

Deploying security policies

It is recommended to deploy security policies for the purpose of defining the privileges of each administration account, controlling the access to administration tools according to the real operational need and reinforcing authentication.

8
Security maintenance

Due to its critical nature, an administration IS must in particular comply with the principle of security maintenance. The latter consists in implementing all of the measures, whether or not technical, that aim to maintain or even increase the level of security of an administration IS all throughout its service life.

R42

Carrying out the security maintenance of the administration IS

The security maintenance for all of the elements that compose the administration IS must be provided periodically and within a reasonable period of time, in particular through applying security updates. For this purpose, it is recommended to conduct technology watch.

Updates must be possible only through depository relays that are internal to the organisation (cf. figure 8.1):

- dedicated to the administration IS;
- isolated from the Internet via a gateway of the DMZ [5] type;
- implementing filtering via a white list (exclusive list of Websites that correspond to authorised manufacturer sites);
- checking, wherever possible, the integrity and the authenticity of the files that are downloaded.

R43

Setting up relay servers for retrieving updates

For retrieving updates (e.g., security patches or anti-virus signatures), relay servers dedicated to the administration IS must be implemented within a DMZ.
Only the flows initiated from these relay depositories to Internet can allow for the downloading of updates. Filtering mechanisms via a white list make it possible to limit access to only official sources.

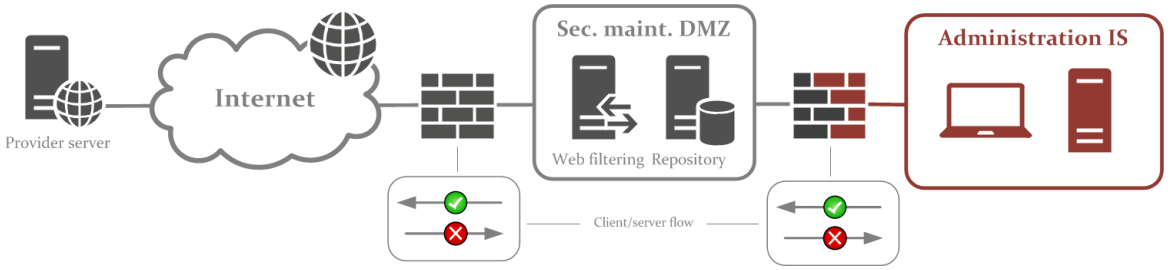

Figure 8.1: Retrieval architecture and making updates available

5. DMZ : refer to the glossary in appendix C.

Finally, in order to prevent any service regression following the implementation of a technical or security patch, the correct operation should therefore be validated beforehand. Procedures for deployment as well as going back must be developed. This practice generally requires having a qualification platform.

R44

Validating the security patches before generalising them

It is recommended that the administrators qualify security patches before they are put into production and generalised.
An emergency procedure must also be provided in order to react in case of a crisis that requires applying a security patch as quickly as possible.

9
Backing up, logging and supervising security

9.1 Backing up

As with any IS, it is essential to define a backup policy for the administration IS, in order to be able to re-establish service after an incident or compromise. For this, the elements to be backed up, the location of the backup and the access rights associated with it must be identified clearly. Backups must be made on a regular basis. Finally, the procedures for restoration must be documented and tested.

R45

Defining a backup policy for the administration IS

In order to overcome corruption or the unavailability of data caused by an incident or compromise, a backup policy must be defined and applied for the administration IS.
For the most critical elements, an off-line backup is recommended.

9.2 Logging and supervising security

Logging technical events, including those linked to security, and analysing them on a regular basis make it possible to detect any compromise of the IS. Archiving this information allows for digital forensics in order to understand how an intrusion was possible.

The logging needs for the administered IS and for the administration IS must therefore be taken into account in designing the administration IS. An administration zone must be dedicated to the logging services (cf. figure 9.1). Indeed, in order to ensure a relevant analysis of the event logs, integrity must therefore be guaranteed from when they are created until their place of storage. In case of intrusion, the attackers will want to delete or modify the traces generated so that their presence goes undetected. In order to cover this risk, beyond partitioning the logging services, it is necessary to limit access to this information to only those who need to know it.

R46

Dedicating an administration zone to logging

It is recommended to dedicate an administration zone to the logging of the administered IS and the administration IS. Where applicable, specific access control must be set up.

Creating an administration zone dedicated to logging imposes naturally that all of the logs roll up in a centralised manner (cf. figure 9.1). Moreover this participates in making the correlation of the logs more effective.

R47

Centralising the collecting of event logs

The architecture must provide for the transmission of the event logs in a centralised manner, from the devices to the logging services.

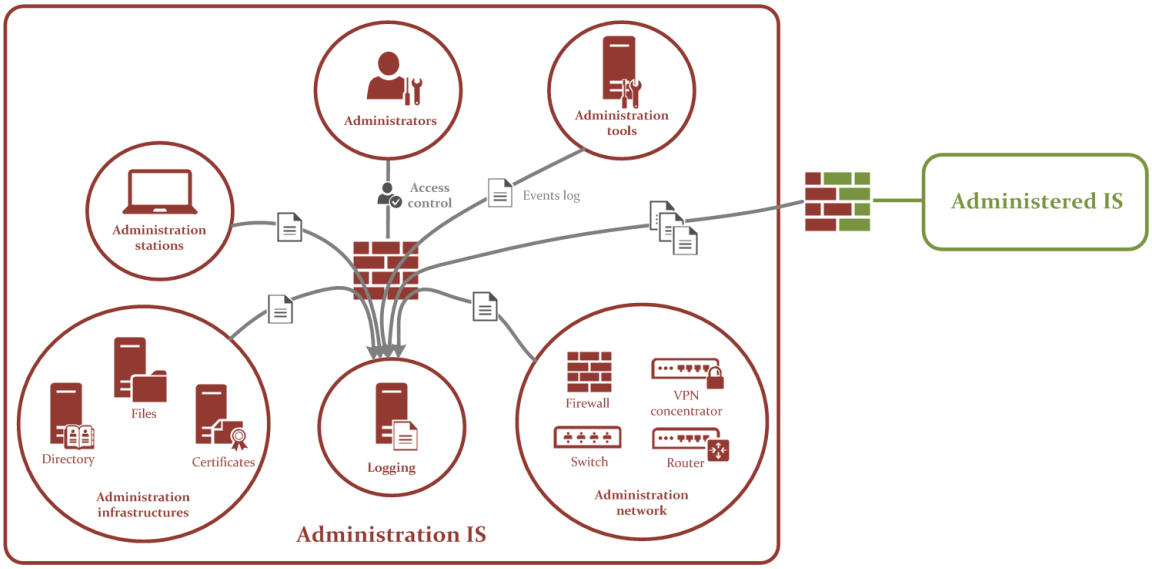

Figure 9.1: Functional representation of logging within the administration IS

Information

As a complement, it is recommended to make use of the related guide from ANSSI [11] and to apply the principles and recommendations of it.
To go further with rolling up event logs and supervising security, the requirements reference document for security incident detection service provider [22] is a guide of good practices.

10
Remote administration and digital nomadism

For various reasons (operational, budgetary, etc.), organisations set up mobile access for their administrators or outsource outside of their premises certain administration perimeters to outsourcing companies. On this subject, the ANSSI publishes a guide [9] concerning outsourcing and managing the associated risks.

It is suitable in this guide to speak of *digital nomadism* for the use of an administration station in a location outside the professional sphere (public place, residence) and of *remote administration* more generally for any access to the IS outside of the organisation's local network. Thus remote administration covers not only digital nomadism but also the use of an administration station from the premises of a service provider for example.

In order to avoid weakening the level of security of the administration IS, a means of a secure connection has to be provided to these administrators (internal or external) who act outside the organisation's geographical perimeter.

Warning

Implementing remote administration requires stronger control of the administration station and the configuration thereof. Indeed this practice substantially increases the risks of a compromise of the IS, in particular in case of theft or loss of the station. The security measures described in paragraph 4.3 must therefore be *fully* implemented on the administration station used in the framework of remote administration, including the encryption of the storage devices.

In the framework of digital nomadism, the administration station can be the object of indiscretion and the information displayed on the screen can be read unbeknownst to the administrator. In addition to the vigilance of the administrator who makes sure that he uses his administration station in a safe environment, the administrator must use a confidentiality filter screen.

R48

Installing a confidentiality filter on the mobile administration station

The mobile administration station must be equipped with a confidentiality filter screen in order to limit the scope of the information displayed.

In light of the current attack techniques and communication protocols, using IP encryption and complying with mutual authentication principles are recommended. IPsec VPN technology covers this need. In comparison with SSL/TLS technology, for which some implementations also propose

establishing a VPN, the attack surface of IPsec solutions is smaller and the exchanges for renewing keys is more robust.

R49

Using an IPsec VPN for the remote connection of the administration station

An IPsec VPN tunnel must be implemented between the mobile administration station, or the remote site, and the administration IS.
All of the incoming and outgoing flows must transit through this tunnel. Any split tunnelling[a] configuration is strictly prohibited.
For the implementation of the IPsec protocol, the recommendations in ANSSI's guide [13] must be applied.

Warning

In the case of a mobile administration station, access to the IPsec VPN concentrator via Internet constitutes the only exception to recommendation R10 and requires strict local filtering in accordance with R11. In addition, the VPN profile has to be configured with the IP address of the concentrator (and that of its optional backup instance) in order to prevent any opening of public DNS flows to the Internet.

In the framework of the use of a software IPsec VPN client, users of the administration station must not be able to modify the network configuration or, *a fortiori*, disengage the remote access mechanisms via VPN. This makes it possible to ensure that no usage error or malicious action will result in diverting the use of the administration station in order to directly access a network (e.g., Internet) other than that of the organisation.

R50

Preventing any modification of the VPN configuration of the administration station

The user of the administration station must not be able to change its network configuration in order to disengage or divert the remote access mechanisms via VPN.

Information

In this specific case, using a captive portal to benefit from an Internet connection can be a problem. As this case of remote administration, probably from a public place, should theoretically be exceptional, it is recommended to use the Internet connection of a trusted mobile phone with tethering feature available.

Moreover, it is recommended to dedicate a VPN concentrator for remote access to the administration IS, separate from the one used for remote access for users to the other ISs. In order to obtain a sufficient level of trust, this VPN concentrator must be physically dedicated.

Finally, according to the level of trust granted to the various categories of administrators (e.g., internal/external, critical/non-critical IS), it is recommended to dedicate a VPN concentrator per

a. Split tunnelling is an IT network concept consisting of providing simultaneous access to two networks (e.g., local network and remote network via an IPsec tunnel).

category of administrators. This measure must be coherent with the internal partitioning of the administration zones to which these VPN concentrators are connected.

R51

Dedicating a physical IPsec VPN concentrator for remote administration

For remote administration, a physically dedicated IPsec VPN concentrator must be deployed at the periphery of the administration IS, at the front of the non-controlled network (e.g., Internet, partners).

Warning

It is important to ensure compliance with recommendation R21 if administration flows pass through a third-party network at the outlet of the dedicated VPN concentrator for remote access.

Figure 10.1 represents the cases of remote administration including digital nomadism.

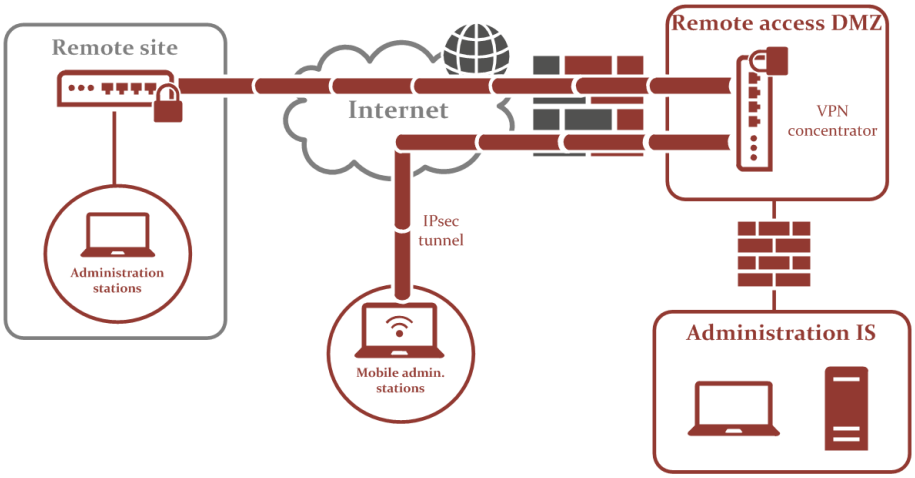

Figure 10.1: Remote administration and digital nomadism

11
Secure exchange systems

In order to overcome the risks linked to the use of removable devices (e.g., USB key) on the administration station, secure exchange systems must be set up. In order to distinguish the security requirements according to the uses, it is suitable to speak in terms of:

- *internal exchange system* for exchanges within the administration IS;
- *external exchange system* for exchanges between the administration IS and an office environment IS (which may be connected to the Internet).

In any case, it is essential that these devices do not weaken the means of protection of the administration IS and are integrated into the risk analysis perimeter. It is also necessary to establish a precise list of the needs in terms of exchange (type of information, volume, frequency).

R52

Deploying secure exchange systems

In order to meet the function needs for internal and external exchanges of the administration IS, it is necessary to set up secure exchange systems.

11.1 Exchanges within the administration IS

As soon as administrators wish to share information with each other linked to this role (e.g., configurations, screenshots), dedicated means should be made available within the administration IS, as administration infrastructures.

For example, a message system dedicated to the administration IS, asynchronous or instantaneous, can be set up with the condition that it does not have, in accordance with recommendation R10, any direct or indirect interconnection with Internet. This can more basically be a file server.

R53

Dedicating the internal exchange system to the administration IS

The internal exchange system for the administration IS must be deployed within administration infrastructures of the administration IS without any interconnection with other ISs.

11.2 Exchanges outside the administration IS

Despite the ban on accessing the Internet from administration stations prescribed by recommendation R10, administrators may need to exchange information (e.g., sending logs, retrieving patches) with outside correspondents (e.g., software and hardware vendors).

An external exchange system (cf. figure 11.1) must then be set up and for example comprise a firewall and client/server services (e.g., SCP, SFTP) with one or several interconnections. In this case, the flows must be authorised in the following way:

- from an administration station (client) to the external exchange system (server);
- from an office environment station (client) to the external exchange system (server).

This as such guarantees that no direct flow is authorised between the office IS and the administration IS.

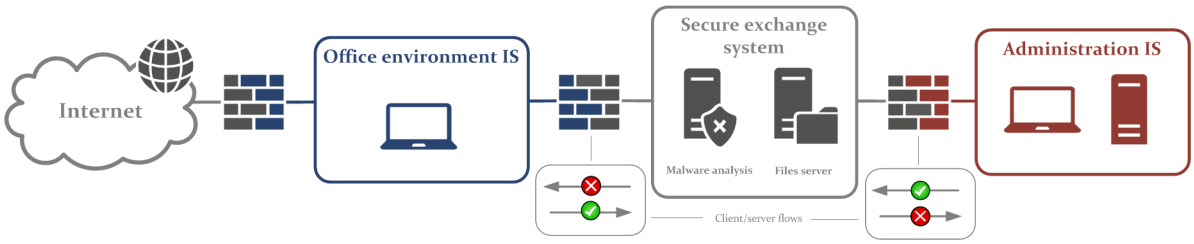

Figure 11.1: Functional representation of an external exchange system

Moreover the external exchange system must authorise only data transfer protocols and prohibit any possibility of opening work sessions. For example, with the SSH service, the latter must be configured to authorise only file transfer commands of the SCP (*Secure Copy*) or SFTP (*SSH File Transfer Protocol*) type. The recommendations in ANSSI's related guide [4] apply.

R54

Authorising only transfer protocols to the external exchange system

Only the protocol services that allow for data transfer must be authorised *to* the external exchange system; the flows must always be at the initiative of the clients located outside of the exchange system. *Under no circumstances*, should it be possible to access a work session through the external exchange system.

Access to an external exchange system from the office environment IS must be strictly reserved for the users that need to transfer information to the administration IS. This reduces the likelihood that another machine, which is more exposed and potentially compromised, can deposit malicious files on the external exchange system. This restriction can be fulfilled by implementing a filtering and access control to the external exchange system.

R55

Limiting access to the external exchange system to strict operational needs

It is recommended to limit access to the external exchange system of the administration IS only to the stations and to the users that need it.

In order not to compromise one's administration account or accounts, it is essential that an administrator authenticates on the external exchange system with an account listed in a dedicated directory or positioned in the office environment IS and *under no circumstances* with an account listed in a directory of the administration IS.

R56

Do not authenticate with an administration account on the external exchange system

Administrators must not authenticate with an administration account on the external exchange system considered to be less trustworthy with respect to the administration IS.

In order to limit the risks of leaks or compromises concerning the data exchanged, an external exchange system must not store the transferred files for long.

R57

Do not permanently store data in an external exchange system

The data exchanged must not be permanently stored on an external exchange system. As soon as the transfer is complete or otherwise within a reasonable amount of time, they must be deleted.

Finally, the content filtering mechanisms and protecting mechanisms against malware must be deployed systematically. This measure aims to protect the administration resources from the risks of a compromise through the execution of malware, which may have been conveyed through files or binary files of which the origin is not trustworthy.

R58

Analysing the content of the data exchanged via the external exchange system

All of the data transiting through the external exchange system must systematically undergo a content scan in order to detect malware.

12
Special cases for administration IS architectures

Inspired from actual cases encountered on a regular basis, this chapter suggests indications for implementation that stem from the recommendations of this guide; it also warns about practices that are not desirable.

12.1 Using a Privileged Access Management solution (aka bastion)

There are products on the market called administration bastions or more simply bastions. This is a breakdown of bouncing, such as introduced in paragraph 6.3. These devices generally concentrate several security functions, such as for example the centralised management of authentication, traceability, automatic renewal of secrets.

Warning

As with any security product, in addition with commercial name that can procure a security sense, should it be chosen, one must be cautious of deploying and using it.

Deploying a bastion for the administrative actions is obviously not a substitute for all of the recommendations in this document, especially the partitioning of the administration IS and the securing of the administration workstation described in chapter 4. Indeed, the bastion forms a critical administration resource in that it potentially concentrates at one time authentication secrets for administration accounts or logs linked to administrative actions. It must not be accessible from an IS with a lower level of trust, an office environment IS for example.

When the level of trust in the various functions of the device is satisfactory – through an ANSSI qualification process for example – and a bouncing device is deemed pertinent in the architecture of the administration IS, the latter has to be deployed within the administration IS, in the administration infrastructures zone (cf. figure 12.1).

Warning

The solution that would consist in deploying a bastion as a means for interconnecting an office environment IS and an administration IS is to be banned (cf. figure 12.1). This would provide a false sense of security because in reality the bastion, the single entry point to the administration IS, would constitute a substantial opportunity for

attacks from an office environment workstation that has access to the Internet.

Figure 12.1: Integration of a bastion into an administration IS

12.2 Possible mutualisation of the administration station

For budgetary or operational reasons, it may be desired to mutualise an administration station for different administration zones and as such administer different trust zones and even different ISs of the same organisation, for example: firewalls for an internal zone and firewalls of a zone exposed to the Internet, network devices (network administration) and hypervisors (system administration), a hosting zone with an Unprotected level and a hosting zone with a "*Diffusion Restreinte*" level in terms of II 901 [18].

Information

The principles proposed for mutualising the administration station can be applied in the context of the same end organisation but this is not suitable in an outsourced multi-client context. In addition, they are not complete and must be in phase with the analysis of the risks carried out in accordance with R4.

Warning

Mutualising the administration station must not weaken the partitioning, physical or logical, implemented between the trust zones within the administered IS or ISs.

Recall that (cf. chapter 6) an administration station can have administration tools installed locally or, non-exclusively, access administration tools servers.

An administrator can have a single administration station for administering different trust zones, with the following conditions:

- securing the administration station must be in phase with the security needs of the most demanding trust zone administered (e.g., a physically dedicated administration station in accordance with R9 for administering a critical IS can be used for the administration of a standard IS);
- the administration station can be used for the administration of trust zones with different sensitivities (e.g., non-sensitive and sensitive, even non-sensitive and *Diffusion Restreinte* in terms of II 901 [18]) but under no circumstances ISs of different classifications in terms of IGI 1300 [17];

- the tools servers that can be accessed from the administration station must not be mutualised for the administration of two separate trust zones (in other words, a tool server remains dedicated to a single trust zone and partitioned in an administration zone);
- any local tools at the administration station that provide direct access to the administered resources must be partitioned in order to prevent any bouncing between two administered resources of two separate trust zones through the administration station (in other words, on a mutualised administration station, the environments for running local administration tools of two separate trust zones must be separate, for example through the use of containerisation);
- access to the various trust zones from the administration IS must comply with the partitioning, hardware or software, between trust zones (in other words, two hardware firewalls or a firewall configured with two DMZ are deployed at the periphery of the administration IS, in order to comply with the partitioning of the trust zones).

Figures 12.2 and 12.3 show the case of mutualisation of an administration station of two separate trust zones, respectively of a homogeneous or heterogeneous level of trust.

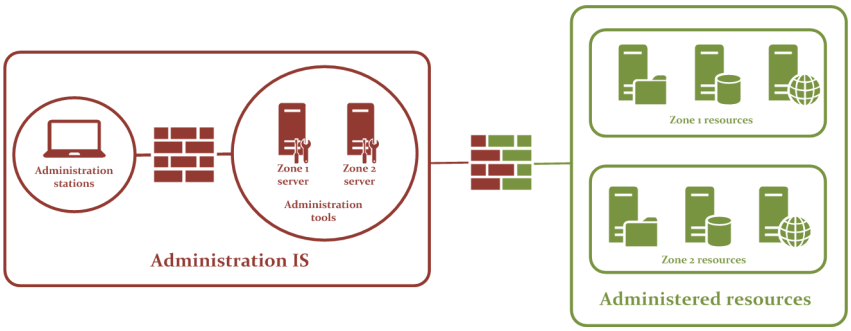

Figure 12.2: Mutualisation of the administration station for two homogeneous trust zones

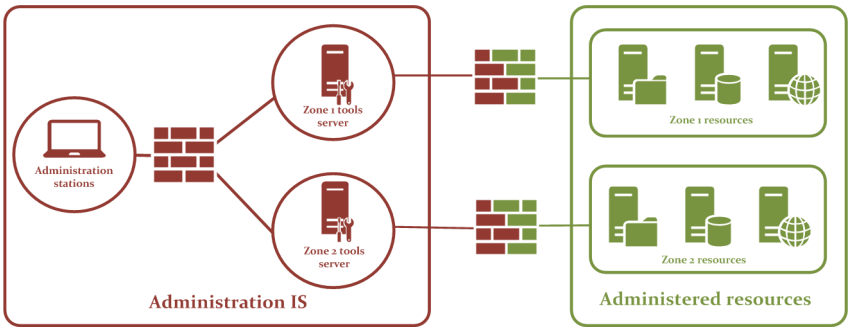

Figure 12.3: Mutualisation of the administration station for two heterogeneous trust zones

12.3 One or several administration station solutions?

The administration station is a key point in the architecture of the administration IS. Three solutions with a decreasing level of security are proposed in chapter 4. For operational reasons, it may seem preferable to retain only one of these solutions.

However, for certain organisations, a single solution, lowering the standard from a security standpoint, can meet all of the functional needs but may not be enough to cover the risks of the administration of the most critical devices or ISs.

On the contrary, a single solution that raises the standard can be disproportioned for less sensitive ISs or not suitable for highly complex ISs.

In this case, it is desirable to have two solutions that coexist (e.g., a dedicated station in accordance with R9 and a station with remote access to the office environment IS in accordance with R9–). In order to simplify maintenance, the administration stations can then benefit from a common hardening system and remote access to the office environment IS is reserves, optionally, to some of them (cf. figure 12.4).

Warning

The following constraint should be complied with: *in fine* an administration tool can be used, or resources can be administered, only by a single type of administration station.

Therefore, it is necessary to construct two separate access chains of the administration IS and ensure a software or physical partitioning between the latter. For example, for a software partitioning, it is recommended:

- in the case of a physical administration network, to use a separate VLAN per type of administration station;
- in the case of a software administration network based on IPsec VPN, to deploy a separate VPN profile per type of administration station.

As such, filtering based on a firewall then makes it possible to restrict access to the tools servers or to the administered resources in accordance with the warning message *supra*, while still allowing for shared access to certain administration infrastructures (e.g., directory, update servers).

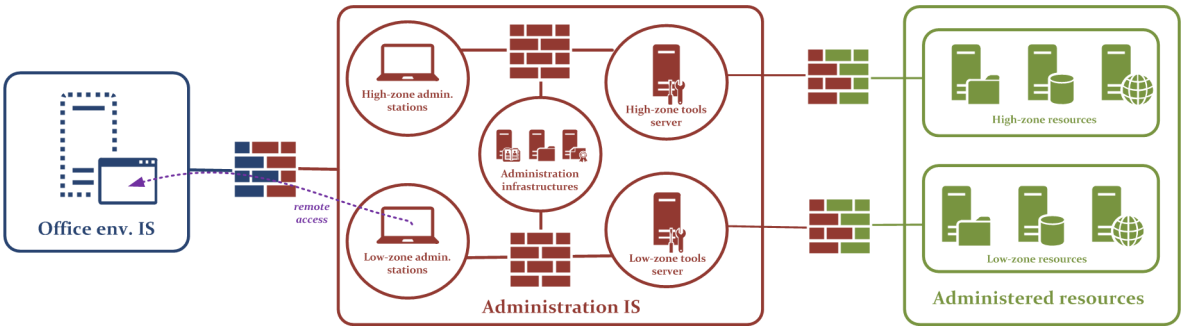

Figure 12.4: Administration IS integrating two administration station solutions

12.4 Administration of administration resources

Regardless of the measures taken to secure the administration of an IS, the question of the administration of the administration resources cannot be avoided. It is important that these resources (e.g., administration stations, administration tool servers) are themselves securely administered.

For this, it is recommended:

- to either carry out local administration in the case of a ”small” administration IS that has only a few administration resources;
- or to deploy an administration zone in the case of larger administration ISs, by implementing adequate partitioning and filtering measures.

In this use case, the administration stations used must have a level of security that is at least equivalent to those used for current administration. They are capable of using the shared administration infrastructures (e.g., a directory for authentication) but access, as soon as possible, dedicated interfaces for the administration of the resources of the administration IS in accordance with R18 or R18- (cf. figure 12.5).

Moreover, it is recommended to strictly apply the least privilege principle to the administration accounts of the administrators of the administration IS.

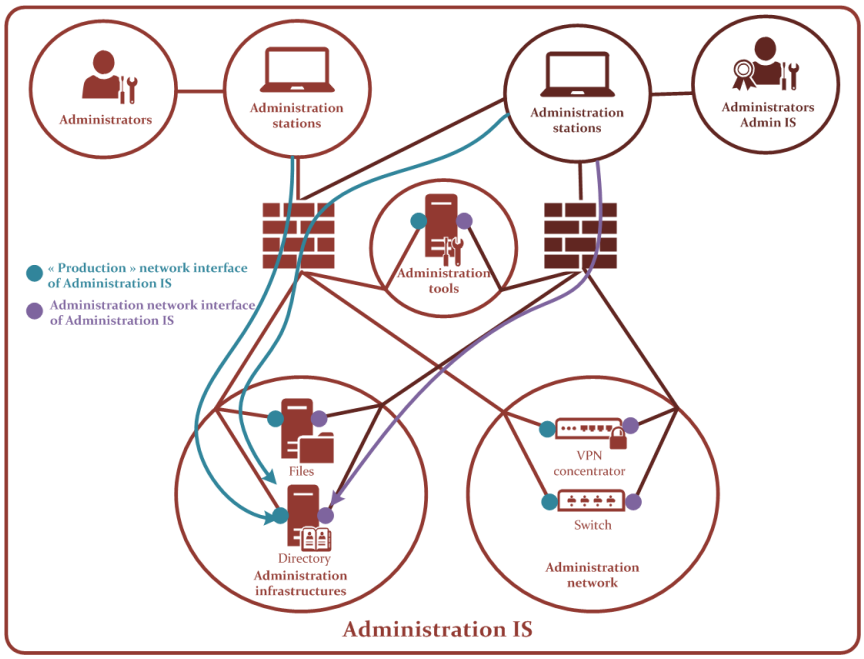

Figure 12.5: Administering administration resources

12.5 Administration of a disconnected IS

The guide’s recommendations also apply to the administration of a disconnected IS. Although they can appear to be preserved from outside threats, disconnected ISs and their administration ISs must be maintained in operational condition and be secure. Retrieving updates is the main point of concern.

If the IS is disconnected for regulatory reasons (e.g., classified defence) or criticality reasons and not for reasons of connectivity (e.g., absence of links), it may be considered, under certain conditions, to construct an exchange gateway. For this, the specific security needs of the disconnected IS (e.g., confidentiality or availability) must be taken into account. In particular, the design of the gateway

has to incorporate the related regulatory constraints that can be much more stringent than those of the update retrieval system described in figure 8.1.

For example, an interconnection gateway between two non-classified and classified ISs must be based on approved products and undergo a specific approval process [17]. The design of such a gateway is therefore beyond the scope of this document.

Otherwise, a procedure of the *air gap* type with the use of a removable device dedicated for exchanges between a connected thir- party IS and the administration IS of the disconnected IS is possible. Detecting malware beforehand must be carried out and check on the integrity can be done when loading files on the administration IS of the disconnected IS.

Recommendation List

Appendix A
Backwards compatibility matrix

In order to allow readers who have already worked based on the first version of the guide [21], referred to as v1.0 in the rest of the text, a backwards compatibility matrix is provided. It makes it possible to locate additions, deletions or equivalents to the recommendations.

Warning

This matrix is a tool for facilitating reading but it does not intend to establish a strict equivalence between the two versions of the guide. It is strongly recommended that you read the updated recommendations in detail.

New recommendations

The following recommendations are new in version 2.0 of this guide:

R2, R3, R4, R8, R27, R34, R40, R45, R50, R53, R56.

Correspondences from version 1.0 to version 2.0

Reference v1.0	Reference v2.0	Reference v1.0	Reference v2.0
R1	R1	R33	deleted
R2	R5	R34	R39
R3	R7	R35	R41
R4	R9	R36, R37	R32
R4 -	R9-	R38	R33
R4 - -	R9–	R39	R36
R5	R15 and R16	R40, R41	R37
R5 -	R15-	R42	R38
R5 - (bis)	R21	R43, R44	deleted
R6, R7	R10	R45	R25
R8, R9	R12	R46, R47	R26
R10	R11	R48, R49	deleted
R11	R13	R50, R51	R49
R12	R14	R52	R6
R13	R6	R53	R51
R14	R48	R54	R10, R11, R12, R13, R14
R15	R35	R55, R56	R52
R16, R17	R29	R57	R54
R18	R30	R58	R55
R19	R31	R59	R57
R20	R22	R60	R58
R21, R22	R23	R61	deleted
R23	R24	R62	deleted
R24	R24-	R63	R42
R25	R6	R64, R65	R43
R26, R27, R28	R18 or R18-	R66	R44
R29	R19	R67	deleted
R30	R20	R68	R46
R31, R32	R28	R69	R47
R32 -	deleted	R70-R73	deleted

Appendix B
Legal aspects

IT system security entails technical measures but also functional measures that incorporate obligations that bear down on the organisation. The administrator has become a key stakeholder in the IT system security and is charged with increased responsibilities. These recommendations do not claim to be complete and require seeking specialised legal council for more details.

First of all, the administrator is bound to obligations concerning:

- **loyalty**: as the administrator is invested with extensive monitoring powers on the data that circulates in the company's IT systems, he is expected to comply with the ethical rules. In light of the company's "dependency" with regard to this type of function, jurisprudence tends to be more severe when an administrator is in non-compliance with his duties. Criminal sanctions can be pronounced against him [6], just as serious cause can be retained in the framework of a dismissal procedure [7];
- **transparency**: the administrator must exercise his missions in the framework of the internal regulations and the IT charter set down by the company. The IT charter is a genuine tool for heightening the awareness of the employees that can be invoked against them when it is attached to the internal regulations. Non-compliance with it will be analysed as a violation of the labour contract which can give rise to disciplinary sanctions, including dismissal. On the contrary, tolerating actions that are however contrary to what is provided for in the IT charter will result in the absence of a sanction [8];
- **confidentiality**: the administrator is bound to a particular obligation of confidentiality [9], in particular concerning professional secrecy. He must not disclose the information to which he may have had access during the exercise of his functions, *a fortiori* when they are covered by laws on respect for private life and the confidentiality of correspondence, unless imposed by a legislative provision (e.g., in the case illicit content is discovered).

Moreover, the organisation must take the required measures in order to protect certain data contained in its IT system, resulting, in the event of failure, in bringing its civil and/or criminal liability into play.

The data security obligation applies, in particular, through article 34 of the French Data Protection Act and article 32 of the General Data Protection Regulation [10] (GDPR). As such, CNIL has become

6. Sentencing for access and fraudulent maintenance in an automatic data processing system, breeching the confidentiality of correspondence emitted electronically: Regional court of Annecy, 4 December 2015, Tefal and others.

7. Paris Court of Appeal, 4 October 2007, no. 06/02095, ARFP Association for the downloading of counterfeit files; Paris Court of Appeal, 29 October 2008, no. 06/14072, JurisData no. 2008 373540 or Paris Court of Appeal 10 April 2014, no. 11/04388, JurisData no.201 007648, consultation of private information concerning managers and colleagues and downloading of music, consultation of pornographic sites.

8. Cass. Soc. 10 May 2012, no. 11 11060 ; Metz Court of Appeal, 24 February 2014, no. 14/00120.

9. Cass. Soc., 17 June 2009, n° 08.40274.

10. Regulation (EU) no. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), applicable effective 25 May 2018.

increasingly severe in case of a lack in security that gives rise to a violation of personal data [11]. The criminal code moreover sanctions non-compliance with these provisions [12].

Other regulations, sector regulations where applicable, may apply. For example, the order of 3 November 2014 [13] concerning banking, more particularly articles 88 et seq., require banks to ensure *"the level of security retained and in that their IT systems are adapted"* by scheduling regular audits and emergency procedures as well as measures that make it possible to preserve in all circumstances the integrity and the confidentiality of the information or the Public Health Code that prescribes the approval of hosts of health data as well as compliance with security measures of IT systems with a nature to preserve medical secrecy [14]. The role of the administrator will depend directly on the regulatory environment in which he exercises his functions.

Jurisprudence tends, furthermore, to expect from the organisation that it measures the necessity of protecting its IT system, otherwise it will be considered as having participated in its own damage [15].

European regulations are increasingly demanding for securing the data of companies and administrations by imposing, according to the case, an obligation to report security breeches and/or to set up technical or organisational measures for managing risks that threaten the security of networks and the information falling under their responsibility [16]. Moreover, the General Data Protection Regulation, effective in May 2018, reinforces the consequences of failure to secure by increasing the amount of the financial penalties that can be pronounced by CNIL [17].

Warning

Through his actions, the administrator participates in providing security for the IT system, an obligation prescribed by many legislative and regulatory texts. Non-compliance with this obligation can call the organisation's civil and criminal liability into play.

Note that the secure administration of an IT system will also entail securing the contracts that the organisation holds (labour contracts, *software* or *hardware* purchases, hosting and or backup services, etc.). Clauses that are essential for the proper execution of contracts are to be provided, such as, in particular, clauses on confidentiality, security, audit, liability including where applicable

11. Deliberation of the restricted formation no. 2014 298 of 7 August 2014 pronouncing a warning against the company Orange: *"Although the company remedied the technical weaknesses observed within a satisfactory period of time and has demonstrated for the future a better taking account of the data confidentiality issues, it nevertheless remains that it failed in its obligation to provide security and confidentiality of the personal data of its customers."*; Deliberation of the restricted formation no. 2015 379 of 5 November 2015 pronouncing a financial sanction of €50,000 against the company Optical Center for failure to secure its customer database: *"the restricted formation observes that the failure concerning the securing of the site was characterised on the day of expiration of the allotted time form for bringing into compliance and persisted on the day of the second audit. The fact that the HTTPS protocol is now in place over the entire site has no effect on the characterisation of this failure."*

12. Art. 226 17 of the criminal code: five years imprisonment and a fine of €300,000 and art. 131 38 of the criminal code: €1,500,000 for legal entities as well as additional sanctions.

13. Order of 3 November 2014 concerning the internal control of companies in the banking sector, payment services and investment services subjected to the control of the Autorité de contrôle prudentiel et de résolution (the Prudential Supervision and Resolution Authority).

14. Art. L. 1111 8 of the Public Health Code.

15. Paris Court of Appeal 4 May 2007, Normaction c/ KBC Lease France, DMS, JurisData no. 2007 334142 ; TGI Paris, 21 February 2013, Sarenza c/ Jonathan and others.

16. Directive (EU) no. 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures intended to ensure a common high level of security of networks and of IT systems in the Union (NIS Directive).

17. The sanctions pronounced by the inspection authorities can now reach up to €20M or 4% of turnover, with the higher of the two retained, General Data Protection Regulation, art. 83. Previously, the maximum amount of the sanctions that could be pronounced by CNIL was €150,000.

penalties, business continuity or reversibility. The risk is even greater when the service provider chosen can be subject, sometimes, to complying with laws that can be considered as intrusive viewed by the organisation from a data sensitivity standpoint. Assistance from legal council specialised in these matters will be an advantage when negotiating the latter.

Warning

Securing the IT system must also be provided for in the framework of suitable clauses in the contracts signed by the organisation for the operation of its IT system. These clauses, according to the type of contract involved, can have an impact on the extent of the powers of the administrator.

Finally, training and heightening the awareness of employees to the need of protecting the organisation's IT system must not be neglected. Indeed, certain behaviours, which can give rise to sanctions (disciplinary or even criminal), do not necessarily stem from the intent to cause damage but solely from not understanding the consequences that may potentially be damaging for the organisation.

The administrator, in collaboration with the data protection officer [18] where applicable, must have essential action in terms of heightening awareness. This is one of the functional measures to plan for when securing the IT system.

The administrator is responsible for monitoring the use of the resources of the IT system in order to overcome the possibility of an incident.

18. Provided for in articles 37 et seq. of the General Data Protection Regulation.

Appendix C
Glossary

As it does not rely on standardised definitions and with a concern for clarity, the glossary hereinbelow defines the terms that are specific to this guide:

Administration actions: all of the installation, deletion, modification and consulting actions for the configuration of a system participating in the IS and able to modify the operation thereof or alter the security of the IS;

Administrator: an administrator is an individual who is in charge of the administration actions on an IS, and is responsible for one or several technical areas;

Functional administrator, operator, integrator, support: the functional administrator or the member of the operating, integration or support team is considered in this guide as a subset of the administrators. This is an individual in charge of operating or using an administration service or resource in particular. He has the privileges that are suited to his functions;

Remote administration: designates any access to the administration IS outside the organisation's internal network;

Administration authenticators: combination of an identifier and one or several secrets associated with an administrator or a service;

Remote access: from a workstation, remote access consists in connecting to another environment (physical or virtual) in order to open a graphical session (e.g., RDP [19], ICA [20]);

Administration account: account that has the privileges required for administration actions, it can be associated with an administrator or with a software service;

Demilitarized Zone (DMZ): a DMZ is an intermediate zone that is between two different networks or IT systems. It makes it possible to protect the resources of the zone with the highest sensitivity using a certain number of filtering tools, and even relay servers;

Administration flow: communication flow to an administered resource for the carrying out of an administration action;

Administration tools: technical tools used to carry out the administration actions (consoles, utilities, etc.);

Administration station: hardware terminal, fixed or mobile, used for administration actions;

Administration network: communications network over which travel the flows internal to the administration IS and the administration flows intended for administered resources;

Administered resources: they are all of the physical or virtual devices of the administered IS that require administration actions;

19. RDP (*Remote Desktop Protocol*): remote access protocol proposed by Microsoft solutions.
20. ICA (*Independent Computing Architecture*): remote access protocol proposed by Citrix solutions.

Administration resources: these are all of the physical or virtual devices of the administration IS: administration station, administration infrastructure servers, administration tool servers, etc.;

Administration IS: IT system used to administer resources that are present in another IS called the administered IS, separate from the administration IS;

Administration zone: subset of the administration IS of which the objective is to isolate or segregate administration resources via protective measures that are suited to the context (e.g., filtering, network software partitioning, authentication, implementation of IPsec VPN) and according to the real operational need. In order to define these zones as effectively as possible, it is necessary beforehand to define the trust zones of the administered IS.

Trust zone: set of IT resources grouped together according to the homogeneity of diverse and varied factors (linked to security or not).

Bibliography

[1] *Guide pour les employeurs et les salariés*.
Guide, CNIL, 2010.
https://www.cnil.fr.

[2] *Recommandations de sécurité relatives aux mots de passe*.
Note technique DAT-NT-001/ANSSI/SDE/NP v1.1, ANSSI, juin 2012.
https://www.ssi.gouv.fr/mots-de-passe.

[3] *Recommandations de sécurité relatives à un système GNU/Linux*.
Note technique DAT-NT-002/ANSSI/SDE/NP v1.1, ANSSI, juillet 2012.
https://www.ssi.gouv.fr/reco-securite-systeme-linux.

[4] *(Open)SSH Secure use recommendations*.
Note technique DAT-NT-007-EN/ANSSI/SDE/NP, ANSSI, août 2015.
https://www.ssi.gouv.fr/nt-ssh.

[5] *Recommandations pour la sécurisation d'un commutateur de desserte*.
Note technique DAT-NT-025/ANSSI/SDE/NP v1.0, ANSSI, juin 2016.
https://www.ssi.gouv.fr/nt-commutateurs.

[6] *Mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation*.
Guide ANSSI-BP-039 v1.0, ANSSI, novembre 2017.
https://www.ssi.gouv.fr/windows10-vsm/.

[7] *Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10*.
Guide ANSSI-BP-036 v1.2, ANSSI, juillet 2017.
https://www.ssi.gouv.fr/windows10-collecte-donnees/.

[8] *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous windows*.
Note technique DAT-NT-013/ANSSI/SDE/NP v2.0, ANSSI, janvier 2017.
https://www.ssi.gouv.fr/windows-restrictions-logicielles.

[9] *Externalisation et sécurité des systèmes d'information - Un guide pour maitriser les risques*.
Guide Version 1.0, ANSSI, janvier 2013.
https://www.ssi.gouv.fr/infogerance.

[10] *Guideline for a healthy information system*.
Guide ANSSI-GP-042 v2.0, ANSSI, septembre 2017.
https://www.ssi.gouv.fr/en/guide/40-essential-measures-for-a-healthy-network.

[11] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[12] *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-006/ANSSI/SDE/NP v1.0, ANSSI, mars 2013.
https://www.ssi.gouv.fr/politique-filtrage-parefeu.

[13] *Recommendations for securing networks with IPsec*.
Note technique DAT-NT-003-EN/ANSSI/SDE/NP v1.1, ANSSI, août 2015.
https://www.ssi.gouv.fr/ipsec-en/.

[14] *Nettoyage d'une politique de pare-feu*.
Note technique DAT-NT-032/ANSSI/SDE/NP v1.0, ANSSI, août 2016.
https://www.ssi.gouv.fr/nettoyage-politique-fw/.

[15] *Recommandations de securité concernant l'analyse des flux https*.
Note technique DAT-NT-019/ANSSI/SDE/NP v1.2, ANSSI, février 2016.
https://www.ssi.gouv.fr/analyse-https/.

[16] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v2.0, ANSSI, avril 2018.
https://www.ssi.gouv.fr/securisation-admin-si.

[17] *Instruction générale interministérielle n° 1300*.
Référentiel Version 1.0, ANSSI, décembre 2006.
https://www.ssi.gouv.fr/igi1300/.

[18] *Instruction interministérielle n° 901*.
Référentiel Version 1.0, ANSSI, décembre 2006.
https://www.ssi.gouv.fr/ii901/.

[19] *Expression des besoins et identification des objectifs de sécurité*.
Guide Version 1.1, ANSSI, janvier 2010.
https://www.ssi.gouv.fr/ebios/.

[20] *RGS : Référentiel Général de Sécurité*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[21] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Note technique DAT-NT-022/ANSSI/SDE/NP v1.0, ANSSI, février 2015.
https://www.ssi.gouv.fr/securisation-admin-si.

[22] *Security incident detection service providers*.
Référentiel Version 1.0, ANSSI, octobre 2015.
https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-exigences.

[23] *Qualification*.
Page Web Version 1.0, ANSSI, mars 2016.
https://www.ssi.gouv.fr/qualification/.

[24] *Licence ouverte / Open Licence*.
Page Web v2.0, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

ANSSI-PA-022-EN
Version 2.0 - 24/04/2018

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN