Network Automation and Security

Jean-Michel Farin [1], David Roy [1]

[1] *Orange France, DTSI*

Abstract

The security of an operator's network is crucial while being increasingly complex to ensure. This is all the more the case with the evolution of the network towards virtualization. In this paper, we will explain how to secure a network and then give some real examples of automation implemented to ensure this security. Finally, we will detail the new risks associated with the implementation of automation tools and share some good security practices around their implementation.

Keywords

Network security automation

1. Introduction

Our lives are transformed by access to digital networks. The majority of the world's population now has mobile coverage and half of them use the Internet.

Orange is one of the world's leading telecommunications network operators. We market connectivity services to individuals, companies and also wholesale for example other domestic and international operators, Internet access and content providers, etc. We use our own infrastructure: millions of kilometers of optical and copper cables, hundreds of thousands of equipment, tens of thousands of antennas and, to orchestrate the whole, thousands of technical sites and data centers.

The automation of the production of equipment and services has been an important issue to respond quickly to the needs of customers and ensure a high level of quality of service. Given the exposure of the equipment and services provided by Orange, security has always been an integral part of the construction of our offers.

Today, the threats we face are increasingly numerous and sophisticated, and the importance of the availability of our networks for our customers means that the impact of a breakdown or malfunction can have a significant impact for them. Moreover, the arrival of network virtualization significantly complicates the operation and security of network equipment as described in Article [1]. In these two contexts of threats and complexities, automation and security issues have become vital to the company and it is essential to work on these two topics together.

After presenting the key points of network security, we offer here a feedback on the use of automation in the operation of Orange France networks to meet our security requirements. We will then share our analysis of the new risks that have arisen as a result of this automation, as well as some countermeasures to be taken to protect against them, namely how to guarantee the security of security automation.

C&ESAR 2021: Automation in Cybersecurity, 16 - 17 Novembre 2021, Rennes, FRANCE

jean-michel.farin@orange.com (J.-M. Farin) ; david.roy@orange.com (D. Roy)

2. The security of the network

Ensuring network security for an operator consists of putting in place protections to maintain the components of the telecommunications network capable of providing the operator's customers with the services they have subscribed while respecting the legislation and the regulation.

From a technical point of view, the establishment of a network consists first of deploying equipment linked together by point-to-point links. Then it's a matter of configuring routing rules and protocols on this equipment that allow them to interact to move information packets from a network entry point to an exit point. These direct interconnections between equipment, combined with the use of peer-to-peer trusted routing protocols, may allow the compromise of all equipment from the compromise of a single equipment as shown in the diagram below.

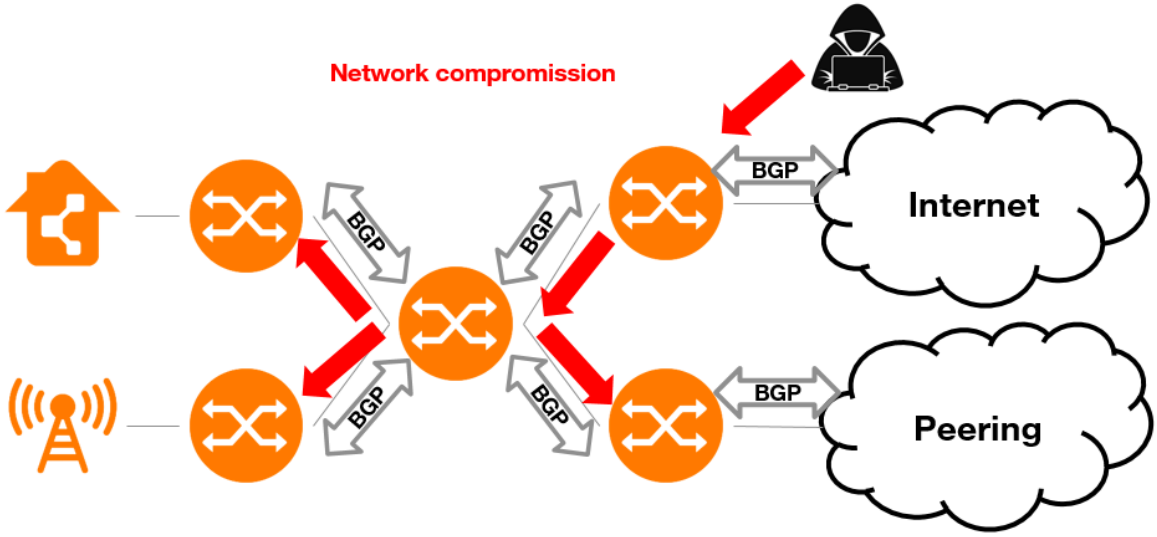

Figure 1: Propagation of network compromise from first equipment

Therefore securing a network requires securing every piece of equipment that makes up that network. The main difficulty in achieving this objective is the heterogeneity of the equipment. They may come from different vendors with different operating systems and control interfaces, but they also have different physical hosting environments and functions. The protections to be put in place are therefore multiple since they must take these characteristics into account. To illustrate our point, access equipment in a street cabinet will be considered less trusted than network core equipment hosted in an operator data center. Similarly, the impact of an incident on these two types of equipment for the operator and the customer will not be the same and therefore the level of protection to be applied is to be adapted.

The technical protections we are talking about are control measures that take place at different levels from the initial configuration of the equipment to the network function provided by the equipment. These key controls will be detailed here.

The first check to be performed on the equipment is to verify that the operating systems and software used on it are those that have been selected and validated by the operator and that have not been modified between the validated version and the deployed version. Some devices have a "secure boot" check function, in this case it is necessary to check that these functions are activated and configured to alert the operator if a fault is found. Otherwise, a manual or automatic signature verification system must be in place when installing the software. In all cases, the system and the software in place must be compared with a repository of the systems and software authorized to run on the equipment in their hosting and function context for the network.

Once systems and software are controlled, controls must be put in place on access dedicated to the management of equipment to allow only specific source IP addresses to connect to it before controlling the accounts and passwords used. In order to allow the implementation of the "least privilege" principle

and the traceability of actions, registered accounts must be used by the different users with rights corresponding to their role and tasks to be performed. To enable the management of passwords or authentication keys in accordance with the company's security policy, the use of a centralized identity server is strongly recommended and in this case it must be configured in the network equipment as a repository for authentication and authorization. Of course, it is also necessary to check that the default accounts and passwords are changed on the equipment.

To ensure access to equipment even in the event of network congestion, access to the management plan must be prioritized. This corresponds technically to the implementation of QoS (Quality of Service) mechanisms favoring management flows to other flows internally of equipment but also on their interconnections. It is important to note that, to be effective, the QoS configuration for both flow processing and tagging must be done consistently on each network node crossed by the flows. A configuration difference on a traversed equipment may negate the expected protection from a global perspective.

The equipment must also have adequate protection against denial of service. Some equipment, under special conditions, may indeed have erratic behavior. When these conditions are known, such as a threshold of packets per second received on a particular interface, protections must be put in place to prevent the equipment from meeting them. To use our example, this is typically the drop of packets on a network card when a threshold is reached.

Concerning the network function of the equipment, it is necessary to check that it is not possible to update the data used by it illegitimately. If we take the case of a routing equipment, the protection of its routing table requires the configuration of access control lists (ACL) and authentication at the level of routing protocols, such as BGP, to allow only the exchange of legitimate routes with legitimate equipment. This type of protection, to be effective, must be as precise as possible but this implies that the lists of legitimate routes and legitimate equipment authorized to exchange them are updated very regularly so as not to create a routing incident.

In order to ensure the reliability and stability of the network, controls must also be put in place to verify that the traffic carried by the network does not endanger third-party elements essential to the provision of service to customers. For example, we can identify DNS servers that are essential to the Internet service and must therefore be protected from denial of service attacks from the Internet. As for the protection of network equipment itself, once the conditions lead to erratic behavior of the services known, protections must be put in place to prevent them from occurring.

Finally, it is necessary to control that there is a homogeneity in the configuration of the components of the network to limit the occurrence of an incident or an unexpected reaction of an equipment following an incident. Indeed, in a redundant network, when a failure occurs on a network path then the traffic is routed on another path. If the backup route has not been planned to absorb the additional traffic without affecting it, then a new incident will be created.

We have defined the major elements necessary for the security of a network. The number of elements and equipment involved and the fact that these equipment are constantly evolving make it almost impossible to maintain these safety rules without resorting to automation.

3. Automation of network security

The purpose of automation for securing the network is to ensure that adequate protections are put in place on each equipment.

In this chapter, we discuss a few real-life cases as examples where we use automation to ensure network security.

3.1. Automate to ensure safe maintenance

Ensuring that all of our security conditions are maintained in time first goes through the documentation. It is essential to document the security rules and define the steps and processes that will enable them to be deployed and maintained. A “hat” document thus lists all of these rules and how to implement them technically on the network. The document can provide either a complete and detailed security configuration or a configuration template (“template”) that will be used later by the operational teams for the deployment of the configuration items.

Before detailing how these security rules are deployed in an automated manner, let’s briefly recall the two main attack vectors of the network equipment of an operator such as Orange.

Overall, a network equipment of an operator performing routing can be damaged by two methods:

- by attacking its management system (or control plan), i.e. the entity in charge of the administration of the equipment but also of all dynamic network protocols that ensure the smooth operation of the network as a whole;
- by attacking the transfer plan, in other words by saturating the links between the network equipment: we are talking about denial of service, a subject discussed in the next paragraph.

The diagram below illustrates these two attack vectors.

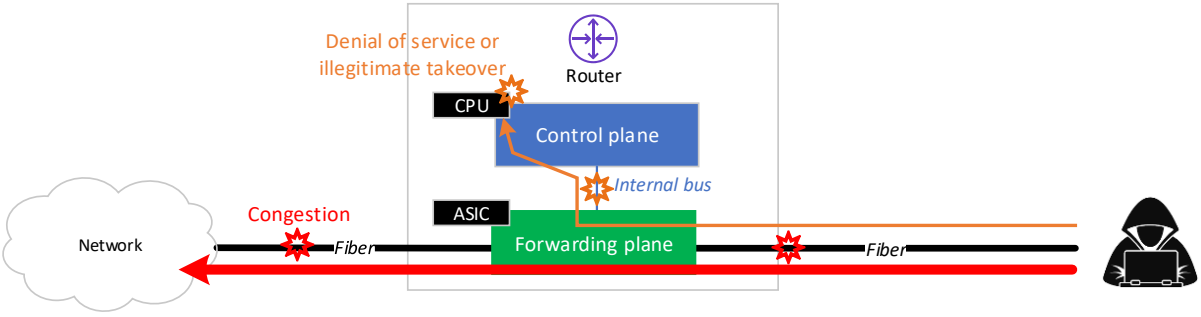

Figure 2: Attack vectors of network equipment

In this paragraph, we will focus on the first attack vector: the takeover or the malfunction of the router control plan.

To protect against an attack on the control plan, we put in place two countermeasures. The first is to maintain an access control list (ACL) equivalent to "stateless" firewall rules, that is, without maintaining a session table, on each device. This ACL only allows inter-router protocol relationships and access to router management by known and authorized address prefixes. The second counter-measure is also made up of ACL but this time is applied to the edge of the network, where the operator is either interconnected with its own end-customers or with third-party operators. The diagram below shows which equipment the different types of ACL are applied to.

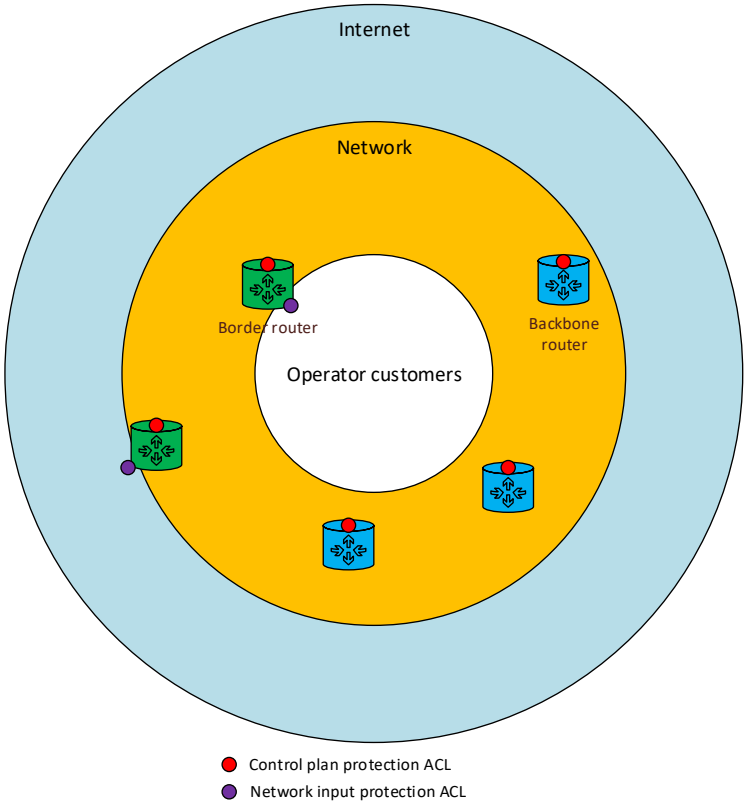

Figure 3: Disposition of Access Control Lists (ACL) in a Network

Although these lists of addresses and protocols remain relatively stable over time, new needs or adjustments in terms of network protocols or administration may occur over the course of a year. This is why the operational teams have put in place an automation solution to quickly deploy an update of the security rules, avoiding any errors that could disrupt the smooth functioning of the routers.

This automation is based on the following processes:

1. Based on safety engineering rules, operational teams create Jinja2 configuration models. This modeling language («templating»), provided by the Python language, makes it easy to take into account all possible exceptions (network position, connection specificity, etc...): one model per need and per equipment manufacturer is maintained. These models input, as a data source, the provided variable files in YAML format.
2. These variable files include the ports and addresses allowed for each protocol. These files are provided by the security team.
3. With these Jinja2 models written by the operational teams and the YAML variables maintained by the security team, a configuration instance for a given equipment is self-generated. This automation of the creation of the management system protection (or control plan) configuration portion is provided by an Ansible/AWX opensource engine.
4. Finally, the configurations are deployed in parallel on the network equipment by the Netconf protocol ensuring a transactional interaction with the equipment. The deployment is usually done by “pool” of equipment.

The diagram below illustrates the automation chain put in place for updating the management system protection ACLs and those applied at the network input to prohibit or limit the visibility of network infrastructures.

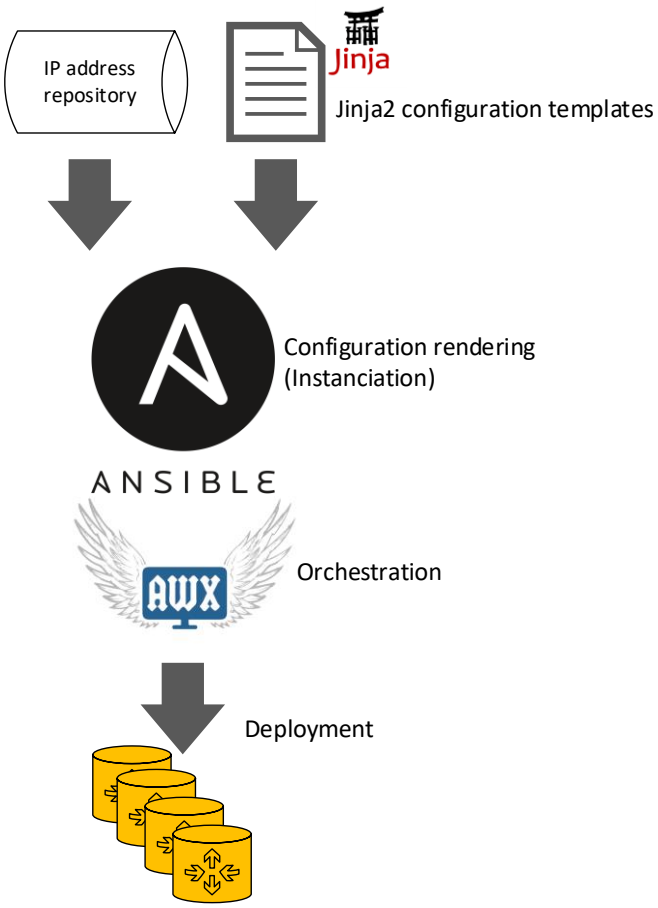

Figure 4: Equipment Update Automation Process

3.2. Automate to ensure protection against denial of service attacks

The amplification/reflection attacks were born a few years ago with the explosion of Cloud services. This type of attack is based on two properties:

- on the one hand on vulnerabilities (bug, behavioral flaw) of certain public Internet services (DNS, game servers, databases);
- and on the ability of these services to generate a bandwidth disparity between a request and a response. We are talking here about amplification factors. For example, between a request using a 128 byte packet and the return response of 1280 bytes, the amplification factor is 10.

The US CERT regularly updates the network services used by the best known attacks and their network signatures through an alert bulletin. These attacks are all based on the UDP protocol because of its "not connected" mode to oppose TCP. Operators like Orange maintain static ACLs protecting the transfer plan. As soon as they enter the operator network, the best known and referenced attacks are mitigated in terms of throughput, thus limiting to the maximum the impact on the network and especially at the extremities of it where traffic congestion is more likely to occur as a result of lower transit capacity compared to the core network.

The update of these associated ACL and bandwidth regulators ("rate-limiter") are also maintained automatically. The same process based on modeling and distribution via Ansible/AWX is used for these ACL.

However, in recent years, operators have seen more and more dynamicity in the signatures of DDoS attacks. The combination of a classic amplification attack with an attack using so-called dynamic ports (other than known services) has become a very common thing on operator networks. These dynamic attacks cannot be mitigated (rate-limit) or suppressed (blackhole) with simple static filters presented previously. Orange France relied on two mechanisms to counter these types of attacks automatically:

- a real-time traffic sample analysis probe;
- dynamic countermeasures based on internal development and the BGP Flowspec protocol.

Orange France uses a probe to collect sampled traffic data (via the Netflow/IPFIX protocol) particularly at the network edge where attacks are most likely to enter the network. This traffic data is particularly useful for detecting traffic anomalies such as DDoS attacks. The probe then provides, where possible, a more or less detailed network signature of the type of attack: protocol used UDP/TCP/RAW IP, source and destination IP addresses in play, source and destination ports, etc.

On this basis, Orange has developed its fully automated dynamic attack countermeasures solution. The solution was developed in Python. It interfaces on the one hand with the Netflow probe and on the other hand with routers dedicated to the propagation (we also speak of «reflection») of routing information in BGP FlowSpec (FS) format. The BGP Flowspec protocol described, among other things, by RFC 5575, allows to distribute via BGP a network signature (IP address, protocol, ports, etc.) and an associated action, for example: discard, rate-limit, QoS remarking, redirection, etc. It can be considered as an ACL/filter distribution solution via the BGP protocol. Routes Reflectors have an iBGP FS session with all Operator Edge Routers that directly propagates one or more dynamic ACLs protecting all external network interconnections.

The solution is notified of attacks by the Netflow probe. Upon receipt of an attack, the tool will come to place a static FlowSpec route via the Netconf protocol on the BGP reflection routers. The FlowSpec route then has a macroscopic signature with a discard (blackhole) action. As a general rule, the target will be blackholed out. This static FlowSpec route is then distributed, by reflection routers, to all network edge routers via BGP. In parallel, the tool begins to periodically query the Neflow probe in REST API for more details about the signature. As soon as the detailed signature is available, the tool updates in real time via Netconf the definition of the static FlowSpec route which is again distributed by BGP. This makes it possible to be much more selective about the traffic to be dropped: only the ports participating in the attack on the destination are dropped. As long as the tool is not notified by the Netflow probe that the attack is complete, it continues to monitor the evolution of the attack signature and updates, if necessary, the attack on the reflection routers. This operation is shown below.

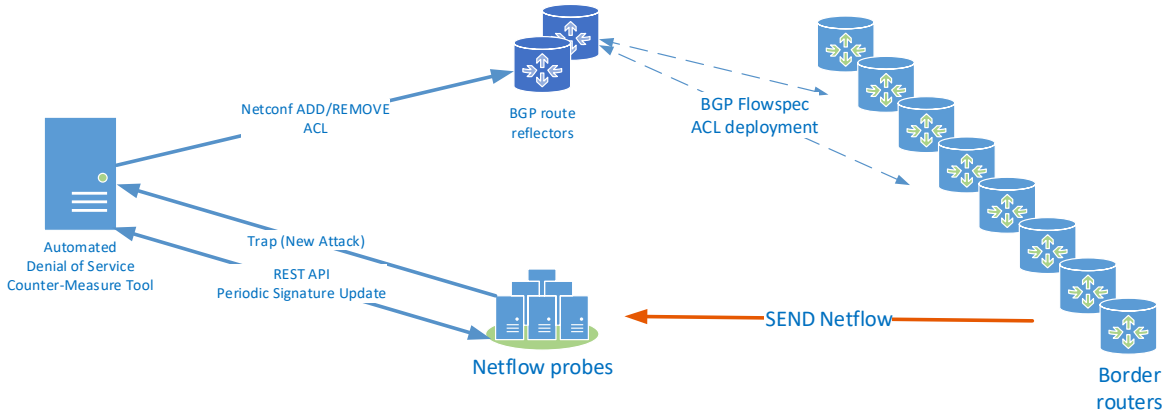

Figure 5: Interactions of the automated counter-measure tool against DDoS

3.3. Automate to ensure vulnerability management

Automated vulnerability management on network infrastructures is more complex to implement. The engineering and operational teams automatically receive the reported vulnerabilities:

- through alerts issued by equipment manufacturers;
- through alerts from official entities such as CERT FR or CERT US.

A manual analysis of these vulnerabilities is then performed. Depending on the result of the analysis, 3 choices are possible:

1. the hardware or software is not affected by this vulnerability;

2. the hardware or software is impacted: depending on the criticality and if the vulnerability can be avoided by adding configuration elements, then the operational teams will distribute the configuration patch via the Ansible/AWX solution on the relevant fleet;
3. in the event of a proven impact and if the countermeasure is only possible via the software update, depending on the criticality, the software update may be triggered on all or part of the fleet concerned.

For this latter case, automation also allows significant gains because it allows to process several equipment in parallel via the use of an orchestrator. The role of this orchestrator will be to configure the routing protocols of an equipment so that it no longer processes client traffic, check that it does not actually process client traffic, update it, reboot it, and reconfigure network protocols, then move on to the next equipment. This makes it possible to process a whole fleet of equipment as quickly as possible, avoiding service interruptions as much as possible.

3.4. Automate to ensure security in the context of network virtualization

As detailed in document [1] presented at the 2019 C&ESAR conference, the virtualization of network functions requires the use of various software to replace the use of dedicated hardware. Thus, as described below, to replace physical equipment, the virtualized network function must be provided with a virtualization infrastructure consisting of various elements: operating system, hypervisor, Software Defined Network (SDN) component, etc.

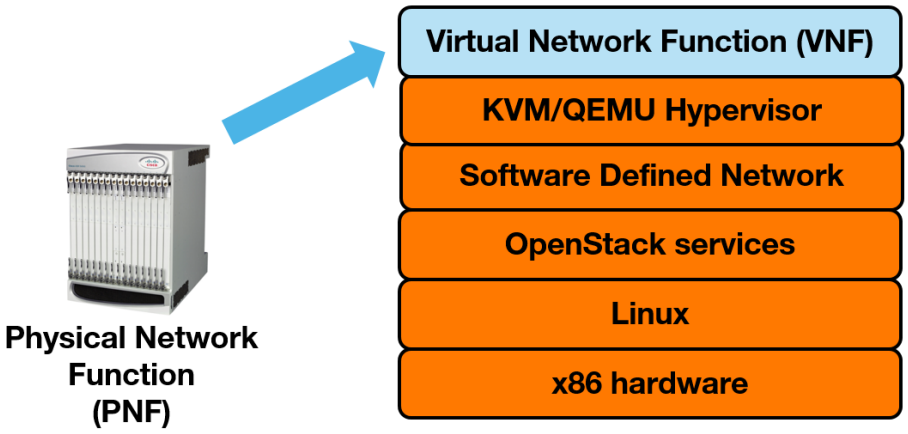

Figure 6: Elements added during network function virtualization

These various software are new sources of vulnerabilities to be analyzed and against which a response must be adopted. This is very complex because each software layer has interactions with the other layers and the operation of the whole can be jeopardized if one of the components does not respond in the same way after the application of a patch or counter-measure. Moreover, the exposure of an operator's network equipment means that the probability of exploitation of a vulnerability is greater than for equipment housed in a data center behind security equipment. Being able to deploy a security patch quickly is therefore imperative while being very complex. It is therefore necessary to have tools and processes to be able to apply as quickly as possible a security fix or a counter-measure on one of the elements of the virtualization infrastructure without having an impact on the functioning of the virtualized function.

It is on this point that automation improves security because it allows to implement automated phases of integration and validation of security patches. Until now, it could be difficult to free up time on the test benches to validate security patches and be able to deploy them. Automation consists here of being able to deploy virtualization infrastructure and virtualized network function in a simulation environment reproducing customer traffic and interactions with other network equipment and operator's information system and apply security patches or countermeasures to measure their potential impact on the operation of the network.

The ongoing work at Orange on this topic is based on the use of a CI/CD channel and the Xtesting structure to validate the smooth operation of a network service from end to end. This will ultimately validate the security patches or countermeasures to be applied in a significantly reduced time frame and will also prepare the deployment of these on production equipment.

4. Network automation security

As we have seen, automation makes it possible to ensure a uniform level of safety on a large number of equipment. In this chapter, we will look at the risks associated with this automation and some ways to respond to them in order to raise the reader's awareness of the key points to be taken into account when implementing the tools enabling this automation.

4.1. Risks related to network automation

To be able to provide the features presented in previous chapters, automation tools must, in most cases, have access with high rights on network equipment see role of "super administrator". This is especially the case when tools change security settings. Some devices require the use of these very high privilege accounts to access even read-only security settings such as password hash, SSH keys, IPSec configuration, etc.

The first risk to be addressed is therefore the compromise of automation tools. Indeed, because they are allowed to access network equipment and contain high-privilege account keys or passwords, they are a prime target to reach the network by bounce as shown below.

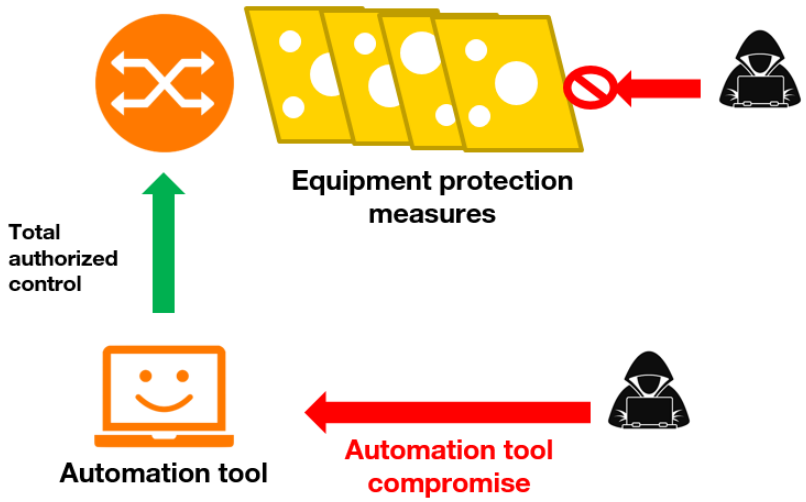

Figure 7: Automation Tool Compromise

The second risk we want to address is the theft of network equipment configurations that can allow an attacker to have key information for a larger attack or perform blackmail. Indeed, in order to be able to audit or update configuration elements, tools need to have upstream configurations in place on equipment in a local base to refer to them. For the security features, the most sensitive elements of the configurations are thus kept in these tools and their knowledge would allow an attacker to know the protections put in place to better foil them. In other cases, it is personal data of customers that can be stored such as their IP identifiers or addresses and the attacker could blackmail the operator not to disclose the theft of this information protected by the General Data Protection Regulation.

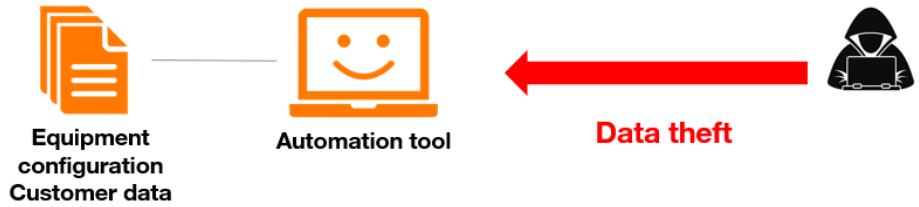

Figure 8: Theft of data via automation tool

These first two risks see their probability of occurrence being all the more important when the hosting of the tools is not completely controlled. For example, when a tool is run in a hosting environment using virtualization technologies, the risk of illegitimate access is related to the number of people with administrative rights to the virtualization solution. Without specific encryption measures in place, the data stored by the tools are technically accessible to people with administrative access to hypervisors but also to storage solutions, internal data center networks or backup solutions. Thus it may be possible for an attacker to take control of the automation tool after taking control of an element of the hosting environment of this tool as in the diagram below.

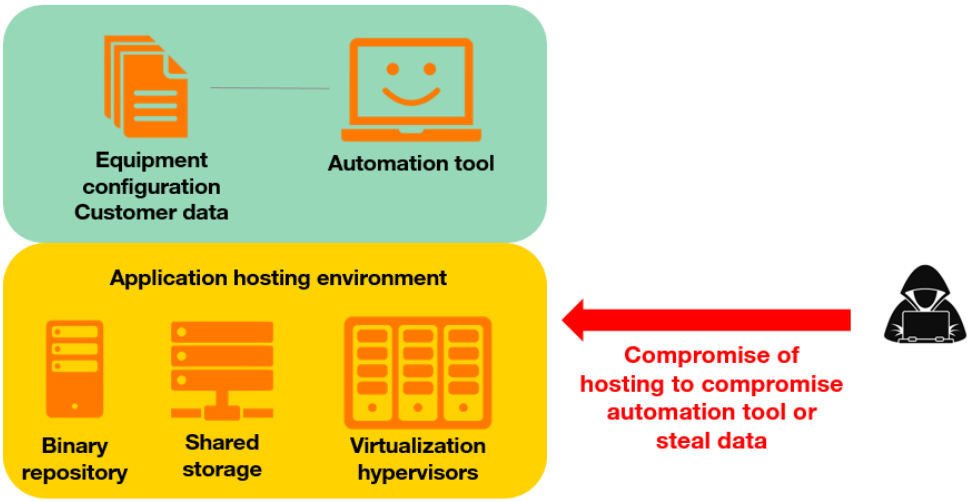

Figure 9: Automation Tool Hosting Compromise

Finally, one last risk that we want to put forward is the loss of control of the network when these tools are unavailable. As systems become increasingly complex, there is a risk of reaching a point of no return where network operation will only be possible through automation tools.

4.2. Good security practices for network automation

The setback we have today on the implementation of network automation tools leads us to share the best practices below in order to reduce the risks brought by these new tools described in the previous section.

4.2.1. Control and traceability

The main security objective to be achieved on the tools must remain the same as that set up to secure the network that is to apply the maximum of a priori and a posteriori measures to control who does what, how, when and on what resources.

Automation makes the exercise more complex because it introduces numerous machine-to-machine connections that can lose as context elements or make them unreliable. Thus, for example, the name of the user who has changed an equipment configuration on a tool will not necessarily be used for the connection to the network equipment receiving the new configuration at the end of the chain. In this example, we see that the controls put in place on the network equipment will not be able to verify that the requested changes are authorized for the originating user. It will therefore be necessary to define machine users corresponding to the tools with the maximum rights necessary for them and then delegate control to the tools if they are used by different user profiles. This difference in the positioning of user rights management is shown in the following diagram.

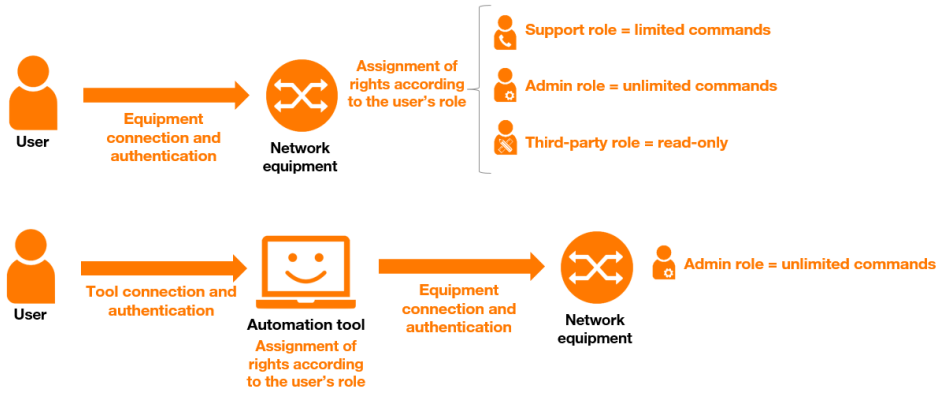

Figure 10: Positioning Authorization Management with an Automation Tool

Like control, the elements of traceability will also be divided between equipment and tools. This problem must be taken into account as soon as possible when implementing the tools because the solution to be implemented to handle it will not be to simply centralize the elements in a common server. A treatment work will be necessary to enrich the traces so that a correlation is possible afterwards. Without these treatments and with an increasing number of tools and users, the traceability elements can no longer be linked to each other and will therefore lose interest.

4.2.2. End-to-end risk analyses

As we have seen for the implementation of control elements, the same is true for risk analyses: it is necessary to have a global view of the automation chain.

For various reasons, the tools are not necessarily set up and operated by the teams in charge of the network and the same can be true for risk analyses which may be limited to the perimeters of each team. This can lead to harmful omissions "at the borders" of the perimeters. The same is true for tool supports such as servers and their operating systems, hypervisors, cloud management systems, storage systems, data center networks, data centers themselves, etc.

It is therefore important that all the teams in charge of security (network, tool, development, hosting...) work together from the start of the projects to exchange on the data to be secured and the potential weaknesses of the solutions implemented.

Thus, for example, if a tool making it possible to exploit the network is installed in a virtual machine hosted on a hypervisor managed by a subcontractor, it will be necessary to go back in the risk analysis that this subcontractor has the technical capacity to operate the network by giving himself administrative rights on the virtual machine

4.2.3. Protection of access to equipment and passwords

As we have seen, tools need to connect to network equipment with accounts with high fees. As the number of automation tools increases very rapidly, the management of these accounts becomes very complex and the compromise of one of them becomes increasingly plausible.

It is therefore necessary to put in place from the outset mechanisms to protect and update these accounts and associated SSH passwords or keys. An application should not incorporate such elements as static variables into its code.

Two solutions can be implemented or combined to meet this need:

- a password vault;
- a "proxy" between applications and network equipment.

The password vault allows you to securely store passwords and limit their access. The use of a vault and a centralized identity management solution means that "static" passwords or keys are no longer used in applications or equipment. In this way, automated password/key rotation mechanisms can be implemented in accordance with the company's security policy. If an application is considered compromised, it is sufficient to remove its access rights and to initiate an automatic rotation of the passwords/keys that it was allowed to use to protect itself from illegitimate access to the equipment via theft of these passwords/keys. The following diagram shows the steps in the authentication process when using a vault and authentication server.

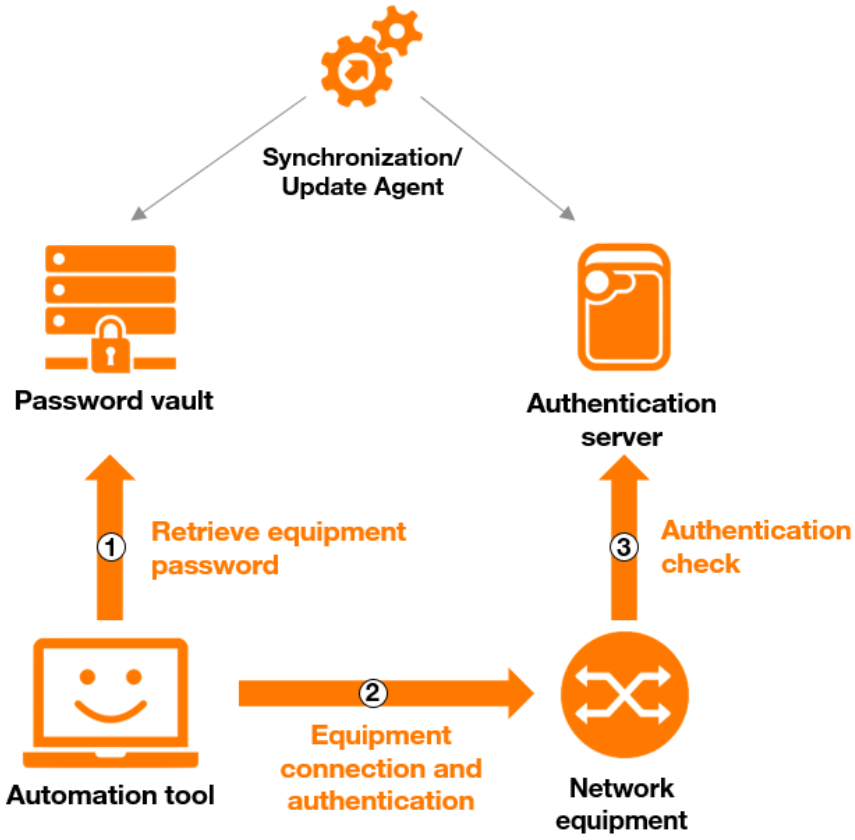

Figure 11: Using a safe to connect to network equipment

The proxy, on the other hand, prevents the direct access of an application to a network equipment and can also limit the authorized commands when the possibilities on the target equipment are limited. In addition, in some cases, allow permissions to be set up based on attributes such as working and non-working hours to make it more complex for an attacker to focus on their actions during time periods when operators are taking longer to react. Thus, a normal operation in working time can be authorized by default on the proxy while it must be the subject of a specific authorization action in non-working time. It also serves to ensure the traceability of orders sent on the equipment. The passage by a proxy/bastion is schematized below.

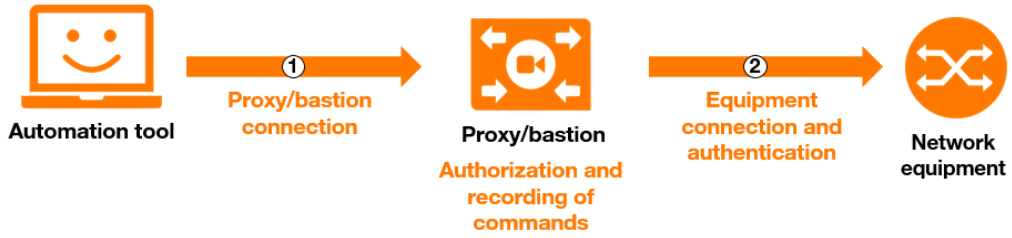

Figure 12: Using a proxy/bastion to connect to network equipment

It is possible by combining the two solutions to provide applications with only one proxy access account that will connect from the application to the password vault to establish the connection with the network equipment. This combination makes it possible to apply control on the authorized controls to a given application upstream of the connection to the equipment, do not need to leave access to passwords/production keys to the applications and finally ensure the traceability of orders sent to the equipment. This is shown in the summary diagram below.

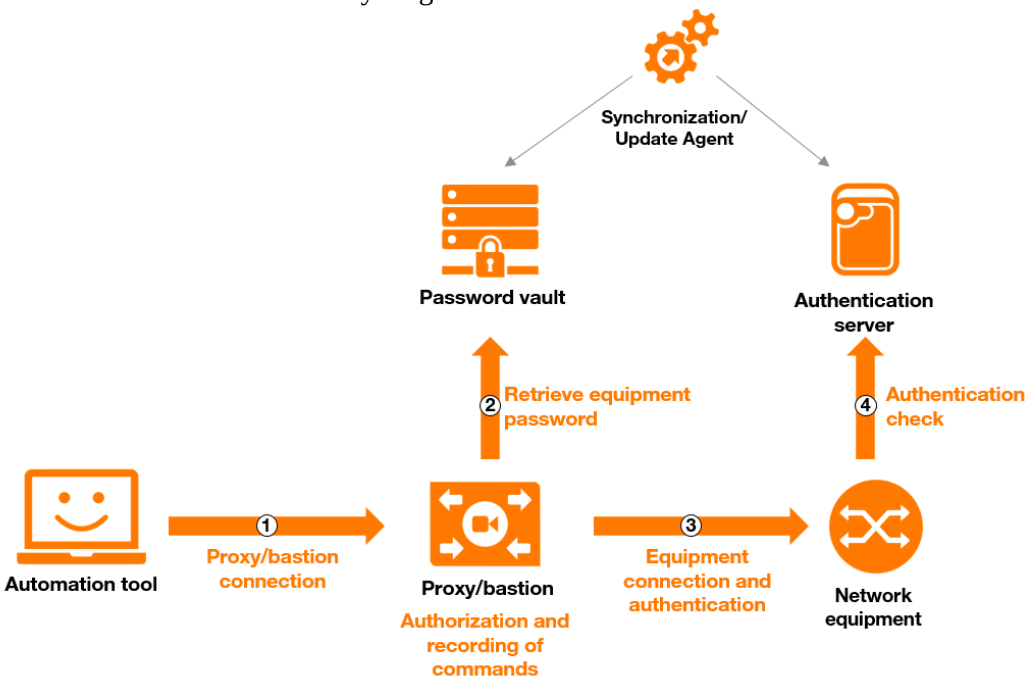

Figure 13: Simultaneous use of a proxy/stronghold and a safe

This solution therefore offers a lot of advantages but it requires integration with applications that can be complex if not initially planned and becomes a critical element to secure.

This problem of an identity management system and common access to the network and applications is probably today the most crucial point to solve to guarantee the security of the network. This point was also raised in our review of the virtualization of network functions [1].

4.2.4. Code Protection

Even if passwords are protected, equipment access is controlled, and application data is encrypted, if the application itself contains malicious code, the network may be compromised.

Automation assumes that confidence in the application is strong enough to give it operational access to network equipment. The first applications were thus offered access to the network after a rather meticulous code audit.

But very quickly the increase in the number of applications requiring network access and the use of regularly updated third-party code made the systematic audit system obsolete, it was no longer possible to audit the code manually before each application production.

In order to limit the risks of compromised code, it is therefore necessary to focus on the security of the development, integration and deployment of code and insert the appropriate controls.

The application holders were asked to:

- implement project access protections in the code repository server;
- implement code review processes with multiple levels of validation;
- limit their use of external code only from trusted referenced sources;
- implement vulnerability scanners within the CI/CD chain;
- use dedicated code deployment servers at each level of application sensitivity and limit their access only to projects identified as legitimate to access them;
- don't allow code deployment in production without manual human validation.

Security awareness workshops are also regularly set up with all actors working on automation tools because automatic controls will never be able to handle all possible cases of failure, Vigilance must be everyone's business.

4.2.5. Protection of the hosting environment

The protection of the hosting environment will require technical but also organizational measures. The aim here is to put in place measures adapted to trust in this accommodation in order to protect against its compromise. Thus hosting with a third party will require an audit of its offer and its processes, an internal hosting will require to verify that the administrators of the different elements of the hosting follow the same authorization procedures as those of the network equipment. In addition, some technical measures are interesting to minimize the risk, such as the encryption of the logical disks used by the tools or the implementation of remote certification of the virtualization hypervisor.

4.2.6. Business Continuity Plan

Finally, the Business Continuity Plan must provide for the event that the automation tools are no longer operational. The number of tools deployed and the complexity of the tasks assigned to them must not make it impossible to operate the network without them. From the outset, the possibility of operating the network with the tools disconnected must be foreseen, even if this operation is degraded in relation to its nominal operation. This will be made possible by the provision of emergency access and adequate procedures.

5. Conclusion

The security of an operator network depends on many different configuration parameters from one equipment to another.

Automation tools quickly became essential to manage this configuration. As we have seen in several examples, their use has greatly improved the level of security and compliance of the network to such an extent that they have become indispensable.

Today, customer expectations are growing and the network is increasingly complex. In addition, due to the ongoing transformation towards the virtualization of network functions, the control of network security will depend on many new elements. The use of automation to guarantee the security of the network will become even more essential and the number of tools implemented will be constantly increasing.

However, it must be taken into account that the risks associated with the compromise of these tools or access to their data are such that they become one of the main concerns in the protection of the network.

It is therefore essential to work with all those involved in setting up and using these tools to share the risks and vulnerabilities of these solutions and to provide them with appropriate security services in order to limit as much as possible the loss of control of the network.

And of course, as with any topic dealing with security, it is mandatory to make all actors working on these tools aware of the security risks, because automated controls, no matter how advanced, will never be enough.

6. References

[1] J.-M. Farin, G. Veille, SDN/NFV Deployment Safety Feedback, C&ESAR 2019 Conference