Ftp server in a data diode

Rusu George, Boulif Ilias, Orinx Cédric

December 4, 2017

Contents

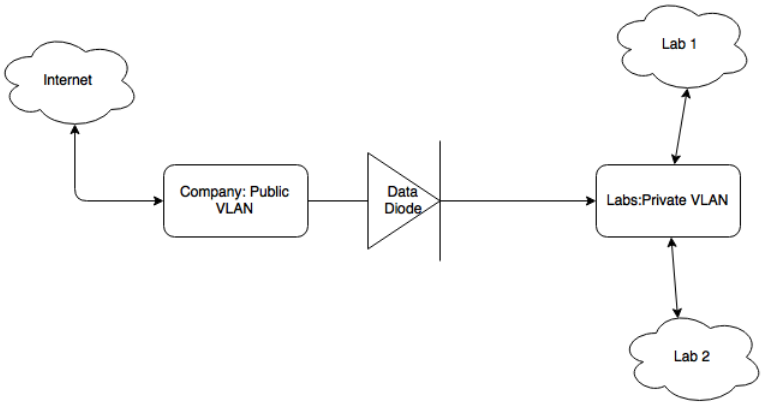

Figure 1: The schema of the usage of a data diode in a company network.

1 Concept of operations

1.1 Introduction to the problem

Our client would want to prevent his research and development labs against industrial espionage and confidential information leaking. He wants to divide the company network in order to maintain the labs in an isolated environment. Thus, the critical data could not leave the company using the network. But how to be able to transfer files or to assure that all the operating systems are up-to-date? This could be achieved using manual operations where an employee would manually copy the files or the updates on a mass-storage device[1] and then used them or install them on every node from the isolated network. However, this is not the most optimized way and for sure it is not cost less and timeless for the company, without mentioning that there could be dependency problems for applications or updates. This method is also prone to human errors and this could generate security vulnerabilities.

1.2 Our solution

In order to address this problem we are going to implement a data diode. In electronic, a diode is a component which conduct the current in one direction. Thus the term of data diode is a set of components that only let the data to travel in an unidirectional way. An example of use case is illustrated in Figure 1, letting the data pass from a low risk LAN to a high risk LAN but not the way around.

A data diode is made using one transmitter(Tx) and one receiver(Rx) both linked using only one fiber cable. Thus, when a digital data is sent through, every bit will be converted[2] into an electrical pulse which will be convert in light pulse using a LED[3]. Then, the output light will pass trough the fiber cable and as soon as the photons are reaching the receiver, they will be converted firstly into an electrical pulse by a photo diode and then in bits[4]. Since there is only one fiber, data can only travel in one way.

One major problem of this system is the network transport protocols(layer 4 in the OSI model) that applications are using. The most used transportation protocol nowadays is TCP. However, TCP is a bi-directional protocol which need the 3 way handshake in order to start a connection, thus there must be at least two fiber cables. In contradiction, UDP does not require a handshake process because it does not provide reliability, ordering, data integrity and does not set up a dedicated end-to-end connection automatically. Thus, UDP protocol does not necessary require a bi-directional data transfer. Therefore, the use of such a protocol is recommended when dealing with applications that are not sensitive to data loss or that implements an error checking system. Hence, the use of the UDP protocol within the data diode.

It seems obvious now that the transport protocol used between the transmitter and the receiver of the data diode is UDP. However, this brings multiple problems. One of the problems is how to be able to use applications that requires TCP. Another problem could be the reliability of the digital data transfer in the data diode, how can we ensure that there will not be any data loss during the transfer. We will address to those questions further down in this document.

[1] A USB-key for instance.
[2] Using a Digital-to-analog converter (DAC).
[3] Light Emitting Diode.
[4] Using an analog to digital converter (ADC).

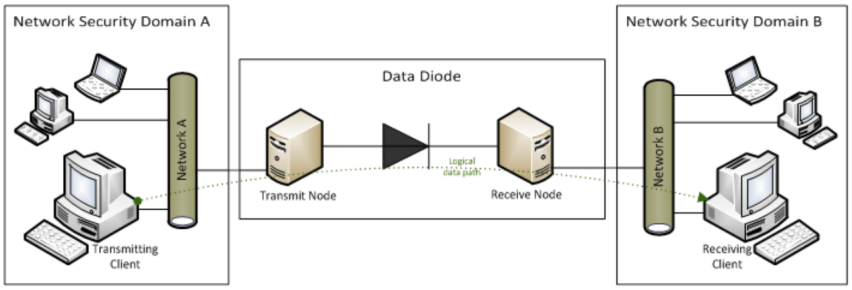

Figure 2: Data logical path within the data diode.

Furthermore, system administrators would dispose of a file transmission mechanism from the low level to the high level in order to maintain all the computers up to date. This will be done using the FTP protocol and will be explained in the next section.

1.3 Our System description

The data diode concept is well orchestrated combination between hardware and software. The data diode is composed of two servers: a transmitter and a receiver. We could consider that the transmitter server is connected to the low security risk LAN where a connection to the internet is made and where all the employees are connected. The receiver is connected to the high security risk LAN where all the labs are connected and where critical informations are stored.

The transmission of the information will be from the low side to the high side and blocked the way around as shown in Figure 2.

1.3.1 Hardware

The following table presents the components used for the data diode implementation. We should mention that both transmitter and receiver possess two NICs[5]: one for the communication within the LAN and one for the data diode.

Components	Description
Transmitter server	a physical machine or a virtual machine. The NIC for the data diode will be set in transmission mode only.
Receiver server	a physical machine or a virtual machine. Similar to the transmission, the NIC will only be set in a receiver mode.
One fiber cable	This optical fiber allows communication between the low server and the high server.
Two fiber NIC and two UTP/RJ45 NIC	On each side, there will be one fiber NIC for the data diode and one UTP/RJ45 NIC for the communication in the LAN.

Table 1: Components description

1.3.2 Software

The Linux distribution which will be used in our project will be Ubuntu 16.04 LTS. We will have two linux machine, one on the transmitter side and one on the receiver side.

The data diode will be easily administrated using a web interface running on a Django server. The web interfaces will be hosted on both servers according to the server location in the company network (transmission interface on the transmitter server, the same for the reception interface). It will be described in more details further in this document.

Every configuration script used by the web interfaces will be a combination of Python language and Bash language.

[5]Network interface controller.

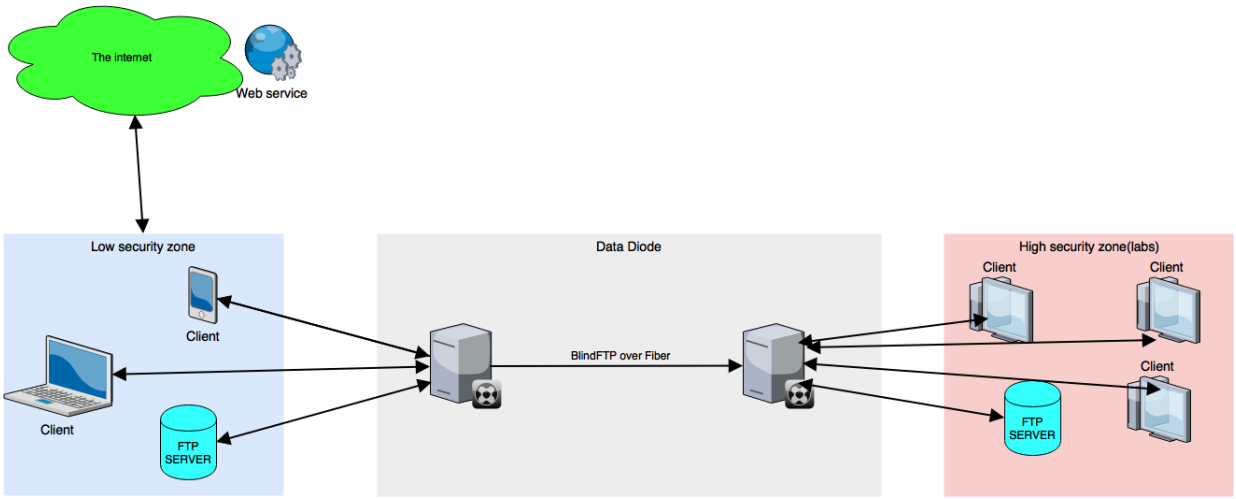

Figure 3: Entire system.

1.3.3 First overview on the project implementation

Let's start by explaining which protocol shall be used in the data diode. Remember that our main goal is to create an isolated environment but also to facilitate the files transfer process to the high security zone. As we mentioned earlier, we are going to use the FTP[6] protocol. There are some alternatives to FTP such as BlindFTP, SFTP, etc. However FTP and SFTP are using TCP as their transportation layer protocol. Thus, we are going to use between the transmitter and the receiver the BlindFTP which use UDP instead.

BlindFTP is a simple Python script which was especially created for the communication between the two servers over an unidirectional network. It is simply a tool for transferring files from one side to the other. Despite the fact that it uses UDP, there is no acknowledgement of received packets but this is compensated by a redundancy of the data. An other advantage is the language used, as it is written in Python the result code is relatively simple and very portable to Windows, Linux or MacOS.

It is now time to have a look at our entire system, let's have a look in Figure 3.

We should note that between the transmitter and the other peers a TCP connection can be used to communicate (transmitter web interface). And this is the same for the receiver, after the data goes out from the network diode the transportation protocol could be TCP with other computers (receiver web interface) . In this way, we are not dealing any more with the problem of application transportation layer.

1.4 Users

In general every employee of a company has a unique ID, a grade, a job title and so on. The company owner or the manager in charge with the security could choose which grade or which person can have access to the administration web interface, of course this exclude the systems administrators. Every user information is managed and stored by the company in their own databases and this is a requirement for the working of the data diode. Despite that this is out of our scope, we will assume that our client has his own users database and we will consider two types of users to make our explanation simpler : the *administrators* and all the others *users*.

A *user* is simply an employee of the company. Every employee has limited access into the company's files according to their job title or to the specific rule defined by their supervisor.

An *administrator* is a user in charge of operating and maintaining the data diode. It is the only authorized person to configure or maintain the well operating of the data diode and this is mandatory. He will have to know how the data diode is working, should know how to interact with it using the web interfaces but mostly he should be able to reconfigure it or restore it as quickly as possible in case of a security breach or a system failure. However, an administrator could not have access to some strict secret files of the company but only to the used IT mechanism.

[6]File transfer protocol.

1.5 User Interface

As we mentioned earlier, the administration of our data diode will happen through a web interface. There will be one web interface hosted on the transmitter which will allows to transmit files or update packages from the lower network to the higher network. But, on the other hand there will also be a receiver web interface for each user to manipulate his transferred data more easily.

Each user should login from both side to use the platform. Here is an overview of our login page:

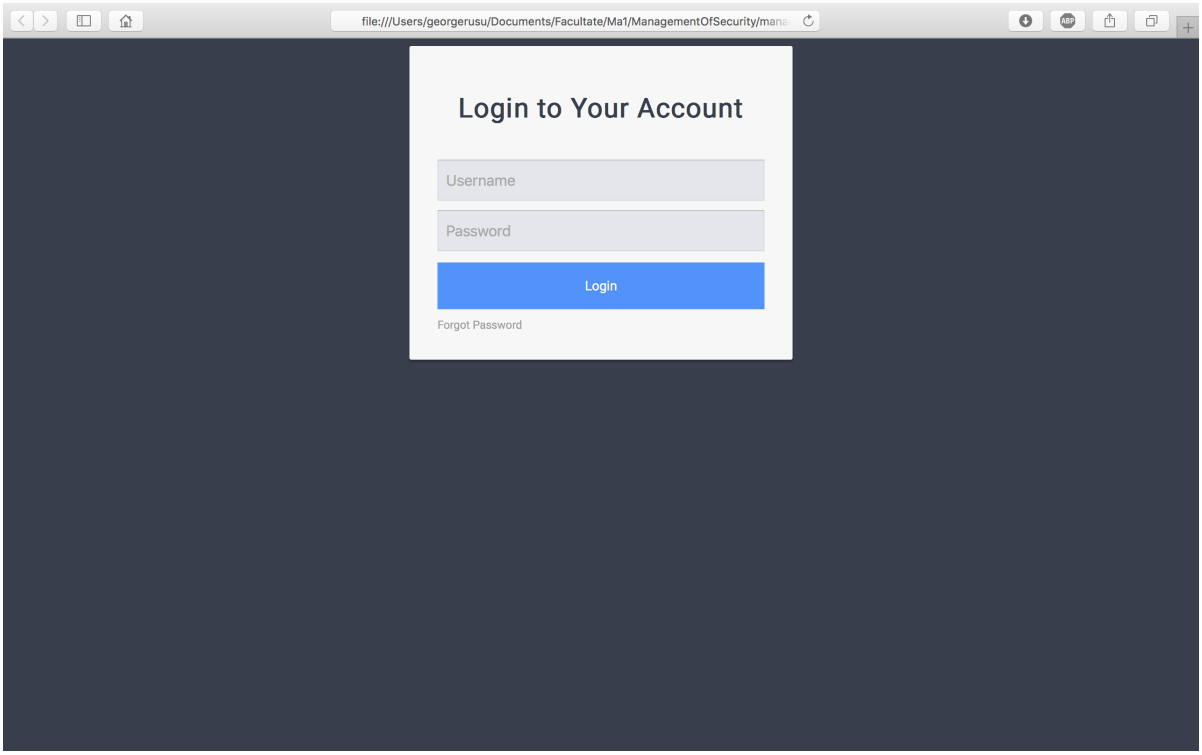

Figure 4: Login page.

Once login is made, the user will be prompted to the web interface of the transmitter or the receiver. The page are shown in Figure 5 and Figure 6.

On the other hand, an admin can transfer files but also can transfer updated packages from official sources or he can upload a package from his own PC. The admin interface is shown in Figure 7 and in Figure 8.

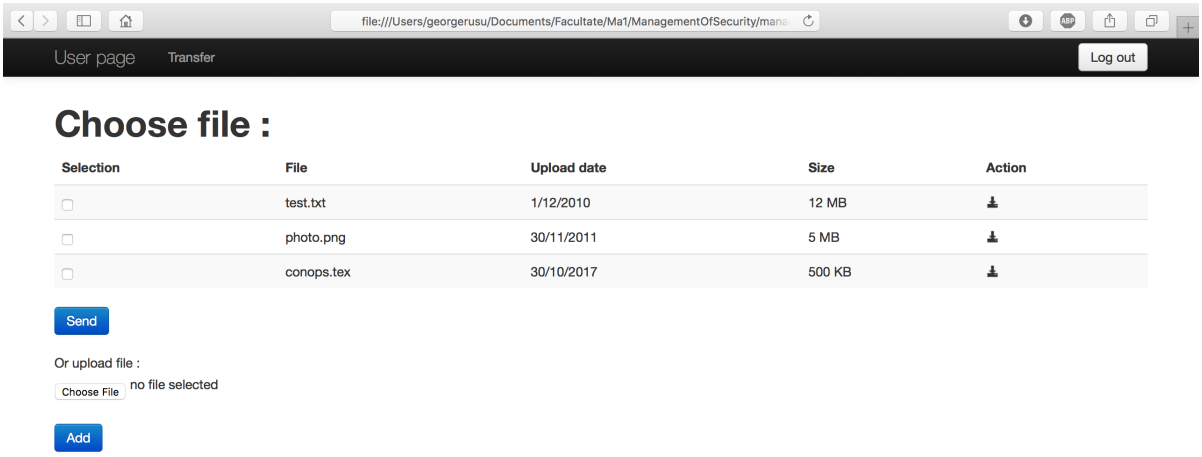

Figure 5: Transmitter user page.

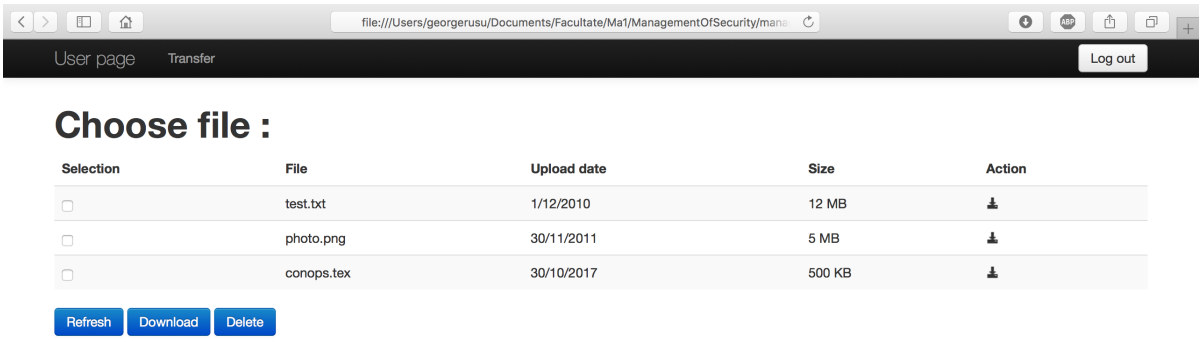

Figure 6: Receiver user page.

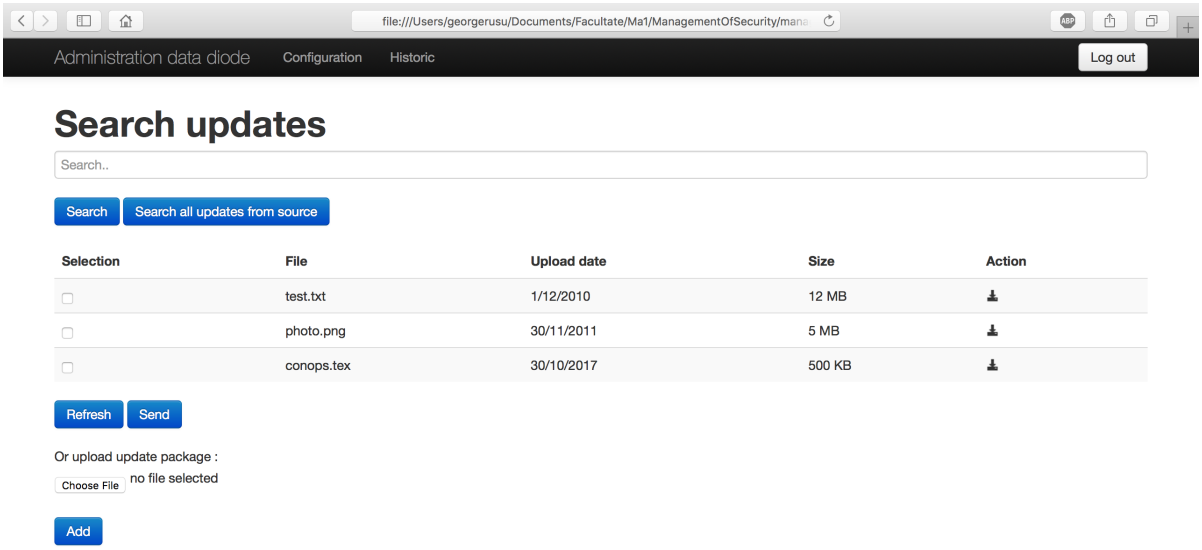

Figure 7: Transmitter admin page.

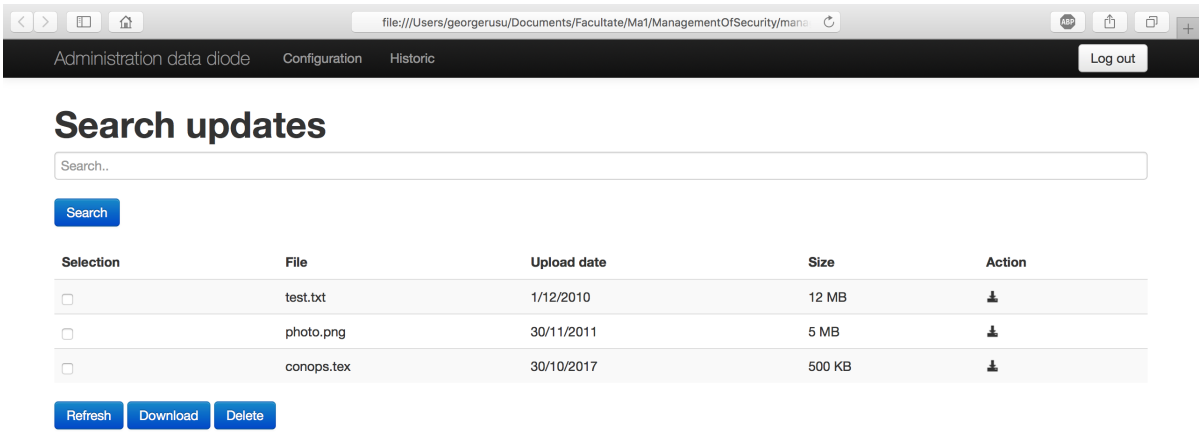

Figure 8: Receiver admin page.

1.6 Usage of the WEB UI

In this section we will explain how to use our web interfaces from different point of views.

1.6.1 General usage

In both cases, all users have to identify themselves through the login page with their credentials. They must fill in the form with their own username and password (Figure 4). Once the form is submitted, the authentication will bring them respectively to their dedicated page.

In the case of a user connection, he will be redirected to the user transmission page according to his network location: if he is in the low security zone he will be prompted to use the transmission interface (Figure 5) or he will get the receiver interface page (Figure 6) if he stand on the high security zone (after the data diode).

On the transmission page the user can select the files he needs and send them through the data diode by using the *send* button. The user have also the possibility to upload a file from a computer and to add it in the selection list in order to transfer it. On the reception page, the user has a list of all the received files which he can depending on the button chosen and his selection, refresh, download or delete.

When an administrator will log in, similarly to the user mechanism, he will be redirected according to his network location : on the transmission interface or on the receiver interface, respectively Figure 7 and Figure 8.

On the transmission page, a *searchbar* is displayed to allow the administrator to search for available updates. He can search a specific update (button search) or display all available updates from officials repositories(button search all updates from sources). In this way he can select from a list the updates that he wants to transfer to the secure network. He can also upload files or new update packages from his computer.

Furthermore, the administrator has an history page. With this page he can browse all the updates installed previously in the system but he can also monitor all the passing data traffic between the two servers. This is made possible using a log information (user, date, size,...).

On the reception page, the administrator has access to all updates that have been send through the data diode. He can update all the machines using some Linux script or to use the web interface to download each update package manually on the desired machine and install them manually. Of course this manual method is not the most optimal but it could serve in case of a need for a system downgrade or an application downgrade on one workstation.

The administrators have the rights to manage all the updates within FTP sharing systems, they can choose to keep or delete updates.

1.6.2 A Technical file transfer usage

We have said earlier that their will be a web interface running on both side of the data diode. When a user will want to send a file, he would have to first login. The login page will use the data base of the company in order to authenticate users and to verify each user permissions. However, on the high security zone, the database would not be reachable because of the unidirectional data diode. Thus, once a user would want to send a file to the other side, there will be a daemon which will create a permission and ownership system in order for the other side to recognize to whom the file belongs to. For example, when the UserX would want to send the *file.txt* to the other side, the transmitter daemon will rename the file using the following rule:

$$file.txt \triangleright userName\_password\_fileName\_timestamp\_size\_extension.zip$$

Every file will be converted into a zip archive in order to reduce the initial size, thing that could sometimes have a major impact on the speed of the transfer (hence the time).

On the other side, there will be of course another receiver daemon which will for each file received, decompress the file into the original extension[7]. However to ensure that only the owner (thus the userName) may see the file, the second daemon will create for every userName a folder where received files will be stored. The rule for this operation is:

[7]This is why the initial extension is putted in to the name of the sent file.

userName_password_fileName_timestamp_size_extension.zip ▷ folder: *userName_password* ▷ files in folder: *file.txt*

Furthermore, when a user wants to login from the secure zone of the data diode, instead of queering a database, the web interface will query a daemon which will use all the folders name to authenticate the user. Every password will not be shared in clear text, a hash of SHA-256 will be used. In this way there is no need of database duplication. The main verification will take place on the transmitter side where the database can be accessed: if a user has the permission to transfer a file, he will be able to transfer the file from the transmitter side. Thus, if the file is transmitted to the receiver side, it means that the user has an access granted on the security zone and thus he has already been verified. However, if a user has not yet used the transmission system of the data diode, he will not be able to connect to the interface from the receiver side.

1.6.3 Configuration panel for the admin

The admin can configure the IP address of both the transmitter and the receiver. In this case, we are not talking about the communication within the data diode but about the communication to other peers of the network. Using the following panel, administrator can manually configure the static IP for the servers hosting both the web interface and the data diode.

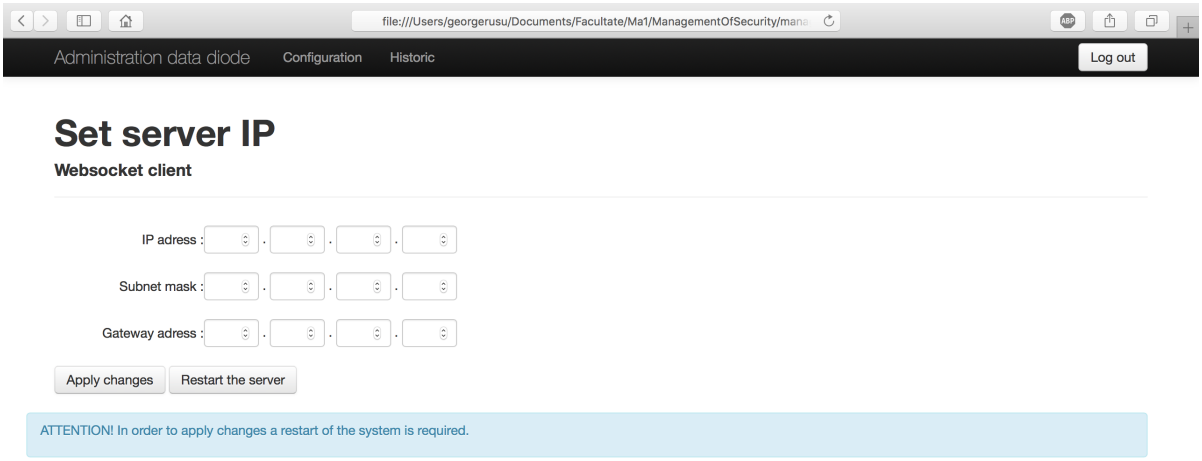

Figure 9: Configuration panel for admin.

About the data diode installation, our product is plug&play. It means that the administrator should only power on the data diode and access for the first time the transmitter and the receiver from *localhost*. In this way, he can configure using the panel shown in Figure 9 the IP-address for the web servers according to the company network. Once this is done, the data diode is completely set up. However in case of anything, there is a hard-reset function which restore the data diode in its factory setting state.

2 Risk Analysis

2.1 Introduction to the risk analysis

In this section, we are going to asses any risk that could harm or lead to the destruction of our data diode. But first, lets define what is a risk: *A probability or threat of damage, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action*[8]. Generally, the term risk is associated with the probability of occurrence of a damage or a loss during an event. Thus, we can illustrate the risk by the following rule:

$$Risk(e) = impact(e) \times likelihood(e), \forall e \in Events$$

In our risk analysis we will start by defining all the assets of our project. Those assets could be threatened by some hackers which could exploit some vulnerabilities found and harm the entire system. Hence, the need to asses all potential threat sources and all the vulnerabilities and their impact. Finally, we will conclude by presenting some countermeasures.

2.1.1 Physical Assets

An Asset can be physical such as computers or printers. In our client work space, we could have the following components categorized as physical assets:

- All the computers of the low security zone. Those computers could be employee's personal workstations such as laptops but also company's desktop workstations.
- All the company's firewalls systems (routers and switch). Despite the fact that they are not part of our implementation, they could represent a potential asset for malicious persons. This could led afterwards to the attack of our data diode.
- Our data diode implementation. This comprise our transmitter server and our receiver server.
- Data diode web servers for the web user interface.
- The company data base server.
- All the computers within the high security zone.
- All the servers of the company such as Mail servers, FTP servers and other services servers. This comprise the servers in low and high risk networks.

To all those components a stakeholder would want to have physical access in order to harm the well being of our client company. Thus, it is very important that the physical integrity of every equipment shall be preserved. In other words, a physical access to some physical assets such as routers or servers could harm or destabilize the company core system which could easily be done for example by simply cutting the power source cable or by disconnecting the internet cable of the main server, compromising his availability).

2.1.2 Logical Assets

A logical asset could be a sensitive information. A list of logical assets used by our client's company could be:

- The company data base containing sensitive information.
- The data data diode web interface.
- Data on the hard drives of every employee personal computer or desktop workstation used for company purpose.
- Data within the research labs.
- Company's storage system.
- Company's operating systems: this contain also every application used within the company. For example the Microsoft Office Suite.

In other words, logical assets represent all the sensitive information which belongs to the company and all the software and applications used by the company's employees.

[8] Definition from the businessdictionary website.

2.1.3 Persons involved into the company

At this point, we should identify every person in the company which could have access to some physical and logical assets. Generally in a company, there are several departments where employees or contractors are working. In order to be able to distinguish every user, we should tag every user with a value according to his loyalty and his hard work for the company. Let's fix 4 valuable stage:

- Very loyal and very hardworking employee.
- Loyal and hardworking employee.
- Not loyal and not hardworking employee.
- Contractors.

It should seems obvious that a very loyal employee which invest a lot of time and work is unlikely to want the destruction or the malfunctioning of the company, because he knows that he will probably lose his job. On the other hand, a non-loyal employee or a contractor could easily want to destabilize the company activities for any kind of reasons such as, an employee could receive a job offer from a competitor, or a contractor who has not been paid yet for his work. Another reasons could be industrial espionage, an employee could be a spy.

However, as we do not know every employee of our client's company and because it is out of our scope, we will simplify the picture by mainly focusing on the administrators and in general the other users. Thus, there are two categories of person :

- The administrators which could have a disastrous impact, they have access to both logical assets and physical assets.
- All other users which could have a moderate impact, they only could have access to physical assets.

Thus, identifying users using a value tag could be very useful when identifying potential threat sources. However, verifying employee loyalty and implication has to be done and pursued only by the company itself.

2.2 Threat Sources

As we mentioned earlier, identifying potential threat sources can be a difficult operation. However, a system failure could be caused by inevitable events or in contrary, it could be caused by a lack of interest (security by obscurity). In order to have a clear view over these kinds of events, we will present all those events using two categories:

- Unpredictable or inevitable events.
- Predictable or avoidable events.

2.2.1 Unpredictable events

Such events could be related to natural disaster which cannot be always predicted in advance. Thus, there is no way in which to prevent the mass destruction, however the company could take some measures in order to minimize the impact. Such events could be:

- Earthquakes.
- Storms.
- Floods.
- Sinkholes.
- Volcanic eruptions.
- Tsunami.
- Wildfires.

However, some event could have a much higher probability of appearance depending on the location where the company has her headquarters. For example, it is more likely to have floods or a tsunami if the company is located near the Ecuador of the globe or in a tropical area, similarly wildfires could occur much often in warm regions. Hence, the importance of the company location chosen. For example, the company could prevent some of those events by choosing where to host their main servers or by implementing measures such as water or fire sealing doors for the labs.

2.2.2 Predictable events

We can define predictable events as security lack that we are or not acknowledged about our system. The administrators could secure the systems by not divulging the vulnerabilities or the backdoor left. This is what *security by obscurity* means, however this is a very bad idea and should be avoided! We defined a list of persons which could be implicated in the hacking action of our client's company system, those persons could be aware of the vulnerabilities of the system or not. Such persons could be:

- Employees or company daily users
- Administrators
- Visitors or unauthorized users
- Script Kiddies
- Skilled Hacker

Each one in this list could be a potential threat source or serve as so. If the company network for example is vulnerable, our data diode could potential be threatened.

Let's assume the following scenarios in which the system could get infected.

After a lot of work and time spent on projects for the company, an administrator or simply an employee could for example make a mistake which could destabilize the entire system. As an example, we could assume that an administrator forget to close a configuration port or an employee could share without his willing his login password. As we said earlier, tagging every user of the company using a value could be a good thing when assessing the threat source. Indeed, a valuable employee despite his tiredness would for sure look twice before finishing his work or sharing some sensitive information of the company. But this is not the same for a newbie which just started on his new job.

Furthermore, having visitor into the company can be a good thing for the image and the brand, however it could be very dangerous. Assuming that a visitor could install a *Femtocell* into the company which could get him full access into the network. Despite the fact that it would be for sure the low security network, the malicious user could sniff every network packet transiting trough and thus could steal some information.

For the last two categories, they represent a constant threat for every company. Hence the need for a security policy always up to date and a good strategic network and workstation deployment in order to minimize the risk. Those categories could exploit the vulnerabilities left in the system by administrators using the *security by obscurity* concept.

2.3 Risks assessment

In this section, we will give a set of possible threats that we should take into account in order to secure the most possible our data diode. In order to have a clear view, we will explain every threats by ordering them according the type of assets it affects.

2.3.1 Levels of affection

We define three different level of affection of our client's company:

- Availability: affecting the physical functioning of the system. For instance, if a server is shut-down, his availability is compromised.
- Confidentiality: affecting the sensitive information of the company by sharing them. For example, a server could be infected and could automatically sends some files to a hacker. It should be obvious that only servers located in the low security zone, in which there is an internet connection, could present such a risk.

- Integrity: affecting some sensitive information of the company by alteration. Similarly to the confidentiality level, a hacker could modify or delete some information in order to hide it or to prevent the company in succeeding their projects. This could be the case when a competitor would want to curb the company in order to be the first one on the market selling a same product on which both were working on.

In this section we are going to assess the risk by assessing a level of the impact and a level the likelihood of every threats.

We define as follow three level of impact in terms of failure time:

- Low: less than 10 minutes.
- Medium: between 10 minutes and 50 minutes.
- High: more than 50 minutes.

We also define the three levels of likelihood:

- Low: maximum 1 time per year.
- Medium: between 1 and 10 times per year.
- High: more than 10 times per year.

The threats will be divide in three part, affecting physical assets, affecting logical assets and affecting persons. For each of this three part, we will give the possible threats, describe them and give a level of impact, a level of likelihood and a resulting risk level.

2.3.2 Threats affecting physical assets

In this section, we will present the threats affecting only the physical assets of the company:

Threat 1 : Power outage

In the case of a power outage, obviously the data diode system will not work because of the need for an electrical power source, which means it will not be available until the power will be re-establish. A power outage usually does not exceed one hour which mean there is not a high impact.

Weather is responsible for the majority of major power outages that occur, but there are many others causes such as short circuits, blackouts and so on. Thus power outage has a medium likelihood to happen.

Source : Nature
Affecting level : Avaibility

Impact : Medium
Likelihood : Medium
Risk Level : Medium

Threat 2 : Fire

Because of a fire in a building in which the data diode is installed or because of to much heat gathered, damage to the data diode system could be done, which leading to his non-operation.

The impact depends on the damages caused by the fire. The data diode can suffer significant or irreparable damages which could lead to the replacement of the hardware.

A fire can occur due to several causes. The probability of fire is in generally low.

Source : Nature
Affecting level : Avaibility

Impact : High
Likelihood : Low
Risk Level : Medium

Threat 3 : Data diode hardware failure

If a failure in the data diode's hardware occurs, such as in the NIC, it can lead to the non-operation of the data diode. In this case, it is the whole operation of the system which can be disturbed. However, the system administrator could easily replace the broken component. Anyway, the data diode hardware are well chosen and tested in order to keep a low risk of failure, however hardware failure can happen. There is no perfect product to last forever in this world.

Source : Nature, Administrators, Employees, Unauthorized user
Affecting level : Avaibility

Impact : Low
Likelihood : Medium
Risk Level : Medium

Threat 4 : Data diode hardware degradation

This vulnerability is possible once an unauthorized person has a physical access to the data diode itself. This could lead to a simple destruction of the data diode or robbery of some element (availability), trying to copy the data from it (confidentiality), or trying to add/modify/delete an element to falsify the data (integrity). There is also a possibility that the hardware degradation is done unintentional (disconnecting a cable, spilling a drink on it). Since then this vulnerability could affect the three part of the information security and also lead to non-reversible damage. However, the impact time is according to the broken hardware component.

A clumsiness is always possible (medium). Furthermore, if the access in the room of the data diode is not controlled, this attack is really simple and is likely to happen very often(high).

Source : Nature, Administrators, Employees, Unauthorized user
Affecting level : Avaibility, Confidentiality, Intergrety

Impact : Medium
Likelihood : Medium
Risk Level : Medium

Threat 5 : DDOS attack

A DDOS is a cyberattack in which the hackers wants to make a system unavailable to its users by temporarily or indefinitely disrupting the services of the host. The attack is accomplished by flooding the targeted resources with superfluous requests from many different sources from the internet, in an attempt to overload the systems and thus prevent the legitimate requests from being fulfilled. The administration of our data diode happens through a web interface which means that it is vulnerable to DDOS attack. In case of such attack the data diode web server will become unavailable as long as the attack lasts. Hence, the transmission system will be disrupted.

If the website of the data diode suffers from a DDOS attack, the secured network productivity can grid to a total halt if the transfer of important files cannot be done. This can lead to an important cost for the business, it is why a DDOS attack can have a big impact. Futhermore, if the company is popular, the secured network will be a prime target for the hackers. Therefore, attempts may be numerous because DDOS attacks have grown in scale and have become very popular since their are easy to implement.

Source : Skilled Hacker
Affecting level : Avaibility

Impact : High
Likelihood : High
Risk Level : Medium

2.3.3 Threats affecting logical assets

In the same order of idea, lets focus now on the vulnerabilities affecting the logical assets of the company.

Threat 6 : Zero Day Attack

Since there is always the probability to be attacked by a new and unknown form of cyberattack, this represents a vulnerability due to the fact that the future can not be predicted. Therefore, such attack could affect one or more parts of the company, but it still remains theoretically and unknown until the beginning of such type of attack. In this cas and since we don't know the attack, its impact could be as low as high. This kind of attack is constantly sought after by different people like skilled hacker, but its difficult to find one, and more of this, find one that can affect our system.

Source : Skilled Hacker
Affecting level : Availability, Confidentiality, Integrity

Impact : High
Likelihood : Medium
Risk Level : Medium

Threat 7 : SQL injection

An SQL injection vulnerability could affect any website that makes use of an SQL-based database. In the case of SQL injection attack, it will allow the "attacker" to bypass a web application's authentication or view data contained in the database and alter it. Hence, data confidentiality and integrity are concerned. This represents a vulnerability because our company detain such a database containing sensitive information.

The possible consequences of the SQL injection attacks such as consultation, modification or deletion of the database, correspond to a big risk because it will affect the login page of the web interface of the data diode. The SQL injection is one of the oldest, most prevalent and most dangerous method to attack systems and steal information from web application. It can be done on any website, so the likelihood is high.

Source : Skilled Hacker, script kiddies, unauthorized user
Affecting level : Confidentiality, Integrity

Impact : High
Likelihood : High
Risk Level : Medium

Threat 8 : Brute force attack

A hacker could try as many passwords as he wants in order to find the correct password. This could be done using dictionaries attacks on a web login page or another type of identity check-in systems of the company. In the cas of the hacker find or guess a correct password, he would use it as long as he can and it works.

Similarly to the SQL injection, there are tools in order to crack passwords. Since it is very easy to do, this kind of attack has a high probability to occur.

Source : Skilled Hacker
Affecting level : Availability, Confidentiality

Impact : High
Likelihood : High
Risk Level : Medium

Threat 9 : Virus and malwares

An infected computer's user could without acknowledgement send a virus trough the data diode. Despite the fact that the communication from the isolated network is not possible, a ransom ware[9] virus could led to the destruction or the non availability of data from the labs.

Depending of the type of the virus, the impact is as well depending on the type of the virus: a Trojan virus would not halt the system however confidentiality will be broken.

This kind of attack is really diversified and used. However, this attack could only success if a user file is infected which means there are several attack to do before. Thus, the likelihood remains medium.

Source : Skilled Hacker, Script kiddies, Administrators, Employees
Affecting level : Availability, Integrity

Impact : Medium
Likelihood : Medium
Risk Level : Medium

Threat 10 : Misconfiguration

A misconfiguration of the data diode, which is only possible from the administrator interface, could cause his non-function or malfunction. This vulnerability has a direct impact on the availability and the integrity but could also represent a potential confidential threat.

In this case, a reconfiguration of the data diode will be required. This will not take much in terms of time and will not have a major impact thanks to the administration interface, which allows to reconfigure easily the data diode. Futhermore misconfiguration by the administrator occurs rarely on a year.

Source : Administrator
Affecting level : Availability, Integrity

Impact : Medium
Likelihood : Medium
Risk Level : Medium

Threat 11 : Failure in maintenance from the provider

A vulnerability can also be introduced by the provider during the installation of the data diode or by an application update or new release. This is generally caused by a lack of communication or documentation between the company.

In case of failure in maintenance or design the data diode can be non-functional until the problem or bug is fixed. This could lead to a halt of the system for a undetermined period of time. The likelihood of that to happens is extremely low on a year, because generally the product is well tested before being released to the client. Thus, in our case the likelihood is medium.

Source : Provider
Affecting level : Availability, Integrity

Impact : High
Likelihood : Medium
Risk Level : Medium

Threat 12 : Remote connection

If the company posses a remote connection system in order for the employee to work from home, if such a system is not well encrypted nor implemented, a hacker could pretend to be an employee and gain access to the company's LAN. He will then be able to steal, destruct or stop any data, process or server he wants to.

Since then the impact will depends of the purpose of the hacker. He could halt the system or simply violate the integrity and confidentiality of the data.

[9]This kind of virus could encrypt all the data on a drive and request some money in order to decrypt it.

Similarly to the virus attack, in order to succeed there must be several other attacks done before. However, it can happen a few time on a year.

Source : Skilled hacker, Administrators, Employees
Affecting level : Availability, integrity, confidentiality

Impact : High
Likelihood : Medium
Risk Level : Medium

Threat 13 : Sniffing the network

If a hacker managed somehow to gain access in the company LAN, he could *sniff* every passing through traffic. This could represent a real threat if the communications/transfers within the LAN are not encrypted. In this case, the hacker could sniff the entire passing traffic of the network for months if no one detect him. But it is still very rare that somehow a hacker could get into the network without being discovered.

Source : Skilled hacker
Affecting level : Availability, integrity, confidentiality

Impact : High
Likelihood : Low
Risk Level : Medium

2.3.4 Threats affecting persons

Similarly as for the previous sections, we explain the vulnerabilities affecting persons

Threat 14 : Social engineering

Social engineering is a practice of manipulating people so they give up confidential information or sensitive data such as their credentials. The most common forms this kind are the ransomware viruses and phishing techniques.

Because this method allows to steal the credential of a user and then the attacker can simply log in and snoop around for sensitive data. Hence, it results in a high risk. But administrators are aware of these techniques so only users are potential victims.

Source : Skilled Hacker, unauthorized user
Affecting level : Confidentiality

Impact : High
Likelihood : Medium
Risk Level : Medium

Threat 15 : Data credentials lost

There is a possibility of a user to lose his credentials which mean that he will no longer be able to connect to the data diode. In this case, a user should immediately contact the administrator in order to reset his credential.

An administrator know the importance of his role and will take care of the data credentials. In addition, every user of the company are using his credential every day so it very rare and unlikely that an employee could forget his in 24 hours.

Source : Administrator, Employees
Affecting level : Availability

Impact : Medium

Likelihood : Low
Risk Level : Medium

Threat 16 : Data credentials theft

Data credentials theft can occur in several ways such as hackers attacks (brute force, social engineering,...) or because of the negligence of a user (easy password, credential stored in a non-secured place such as the office, and so on...) or because of a malicious administrator which has the right to modify read the company database (password table)[10]

If it is the administrator's credential that are stolen, the attacker can change the data diode administration and it implies a big impact. On the other hand, if it is the user's credential that are stolen, they can use it and transfer what they want and access the data of the user. In both case, the attacker can do what he likes and could prevent the access for legitimate persons such as the administrator.

Source : Skilled Hacker, unauthorized user, Employee, Administrator
Affecting level : Confidentiality

Impact : High
Likelihood : High
Risk Level : Medium

2.3.5 Risk level

After we have analysed the impact and the likelihood of each vulnerabilities, we can now define for each one of them a risk level, this is shown in Table 2.

	Impact		
Likelihood	**Low**	**Medium**	**High**
Low	Low	Low	Low
Medium	Low	Medium	Medium
High	Low	Medium	High

Table 2: Risk level assessment.

ID	**Vulnerability**	**Impact**	**Likelihood**	**Risk Level**
1	Power outage	Medium	Medium	Medium
2	Fire	High	Low	Low
3	Data diode hardware failure	Low	Medium	Low
4	Data diode hardware degradation	Medium	Medium	Medium
5	DDOS attack	High	High	High
6	Zero Day attack	High	Medium	Medium
7	SQL injection	High	High	High
8	Brute force attack	High	High	High
9	Virus and malwares	Medium	Medium	Medium
10	Misconfiguration	Medium	Medium	Medium
11	Failure in maintenance from the provider	High	Medium	Medium
12	Remote connection	High	Medium	Medium
13	Sniffing	High	Low	Low
14	Social engineering	High	Medium	Medium
15	Data credentials lost	Medium	Low	Low
16	Data credentials theft	High	High	High

Table 3: Risk level

[10] This is generally in case of any employee lose his credential, the administrator can reset it or change it manually.

2.4 Countermeasures

In this section we will explain which and how countermeasures could be taken in order to address every vulnerability of the system. We will use the Table 2 in order to adapt our countermeasures accordingly to the risk level of each vulnerability.

However, before starting, we should mention that most of the vulnerabilities nowadays are coming from the internet. Thus, our data diode should not be exposed to such a danger. Despite the fact that the data diode could be installed within a LAN which has an internet connection, it should not be possible to access it form the outside but only from the LAN. In this way, it will be much difficult to a hacker to directly threat our data diode. In order to succeed his attempts he should therefor, try infecting a computer within the LAN and only then, by redirecting all his traffic trough his new bot, try to hack our data diode.

ID	Vulnerability	Countermeasure(s)
1	Power outage	For this vulnerability we accept the possible risks.
2	Fire	The data diode must be placed in a room protected against fire, closed with fire doors to mitigate as much as possible the risk of the data diode being affected by fire.
3	Data diode hardware failure	Since an administrator must be ready to intervene in case of any hardware failure, we can accept the risk of this vulnerability. In addition, administrators should use administration tools such as *SNMP protocol* in order to face the issue as quickly as possible.
4	Data diode hardware degradation	The data diode must be placed in a closed room locked with a key or locked using access card possessed only by the administrators or authorized employees. A camera could also be installed in order to monitor activity into the room. Since there are only few persons who have access in the room, the risk is limited to a clumsiness of the administrator.
5	DDOS attack	This could be faced by limiting the number of connection to the data diode. It will then be impossible to overload the system and thus to halt it. However, the data diode servers can only be accessed from the LAN. Thus, in order to create a DDOS on the data diode server, all the company's computers should be infected.
6	Zero Day attack	Due to the fact that we can not be prepared against this kind of attack, we accept the risks of this vulnerability.
7	SQL injection	In order to avoid the SQL injection, we must use in the code source of the web interface the especially developed function which prevents the execution of the SQL language.
8	Brute force attack	In order to stop dictionary password attack, we could implement a number of password trial times before blocking the account. In this way, after 3 wrong password, the account have to be manually reset by an administrator.
9	Virus and malwares	This vulnerability is out of our scope. The client is responsible for securing access to internal network and so he should use appropriate anti-virus and other anti-malware system.
10	Misconfiguration	The configuration is only possible through the administrator interface and by an administrator. Hence, an administrator must be well chosen. However, the company should create a modification policy in which a system alteration should be approved by at least two administrator in order to take place.
11	Failure in maintenance from the provider	We test all the features of the data diode (such as the transfer) before providing it to the client. We make sure we always have a well operating version.
12	Remote connection	The company should have a two step verification system. If a hacker manage to gain access, the second step verification will block him. This second step verification could be for example a 6 characters code sent to the user's phone.
13	Sniffing	There should be log of every path of the data trough the network. Thus if a person is sniffing the traffic, an administrator can rapidly identify the redirection of the whole traffic. But also the traffic and the communication should be encrypted and thus the sniffer would not be able to read especially confidential information.

14	Social engineering	Since it concerns the employees, the company should provide security awareness training in order to avoid social engineering.
15	Data credentials lost	Having more than one administrator is recommended but it is not an imperative countermeasure
16	Data credentials theft	In order to mitigate the risk of credential theft, employee should not save them into their browser or write them into a secure file and should change it several times.

Table 4: Countermeasure

2.5 Residual risk

ID	Vulnerability	Countermeasure	Risk level	Residual riskl
1	Power outage	Accept	Medium	Medium
2	Fire	Mitigate	Low	Low
3	Data diode hardware failure	Accept	Low	Low
4	Data diode hardware degradation	Mitigate	Medium	Low
5	DDOS attack	Transfer	High	High
6	Zero Day attack	Accept	Medium	Medium
7	SQL injection	Avoid	High	Low
8	Brute force attack	Avoid	High	Low
9	Virus and malwares	Transfer	Medium	Medium
10	Misconfiguration	Trnasfer	Medium	Medium
11	Failure in maintenance from the provider	Mitigate	Medium	Low
12	Remote connection	Trnasfer	Medium	Medium
13	Sniffing	Transfer	Low	Low
14	Social engineering	Transfer	Medium	Medium
15	Data credentials lost	Transfer	Low	Low
16	Data credentials theft	Transfer	High	High

Table 5: Risk level

3 Implementation

4 Test and demo scenario

References

[1] DEEP SECURE, *How Does a Data Diode Work?* Discussion Paper, February 2017.

[2] SANS Institute InfoSec Reading Room, *Tactical Data Diodes in Industrial Automation and Control Systems*, January 2015.

[3] CS Risk Management and Compliance Ltd, *Data Diode vs Firewall Feasibility*, September 2016. [Online]. Available: `https://csriskmanagement.co.uk/data-diode-vs-firewall-feasibility/` [Accessed: 30- Oct- 2017]

[4] BlindFTP, *Blind ftp protocol*[Online]. Available: `https://www.decalage.info/fr/python/blindftp` [Accessed: 30- Oct- 2017]

[5] David Basin AND Patrick Schaller AND Michael Schlapfer, *Applied Information Security, A hands-on Approach*, Springer.