IDQ FROM VISION TO TECHNOLOGY

REDEFINING SECURITY

ID Quantique White Paper

Data in Transmission - Is Your Printer Network Secure?

Version 1.0

October 2012

Table of contents

ID QUANTIQUE SA

Ch. de la Marbrerie, 3
1227 Carouge
Switzerland

TEL: +41 (0)22 301 83 71

Fax: +41 (0)22 301 83 79
www.idquantique.com
info@idquantique.com

Information in this document is subject to change without notice.

1. Introduction

Many organizations spare no efforts to secure their sensitive data in long term storage or as it transits through public segments of the Internet. External exposure is however not the only high-risk situation which requires control – data can be misappropriated and misused internally just as easily, and it is known that internal data breaches are a significant risk for organizations.

One such situation for which there often is no dedicated security infrastructure is the printing network – the portion of the intranet used to transfer data from end-user PCs to printing clusters, often via resource management servers which dispatch the jobs to free printers.

A printing network is by no means simple to manage and configure. Printers support a variety of protocols such that they can receive data from a wide range of hosts, from mainframe computers to tablets. Two prominent examples are the older Line Printer Daemon Protocol (LPR) and the Internet Printing Protocol (IPP).

To secure such a network, a number of architectural decisions are required:

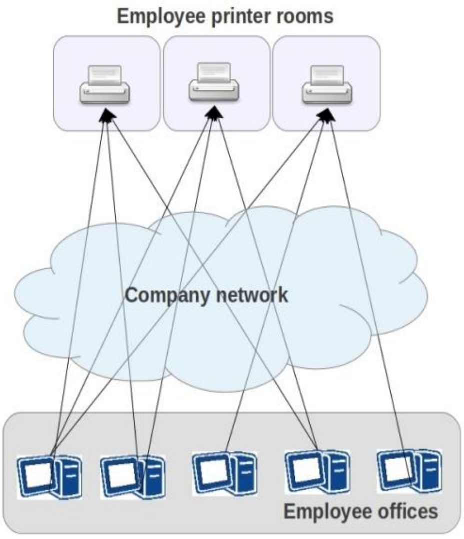
- A correct segmentation of the printer network, e.g. by department or printer purpose
- The implementation of physical security in the printer room itself
- Applying encryption at the appropriate level, which is the lowest common denominator of the supported protocols – the IP layer

Although there are countless options for deploying well-conceived printer networks, there are designs which recur throughout organizations. Before venturing further into printer network security, let's review how typical printing networks are organized.

2. Typical risk scenarios

Typical printing networks might look as follows:

Scenario 1: Daily employee printing

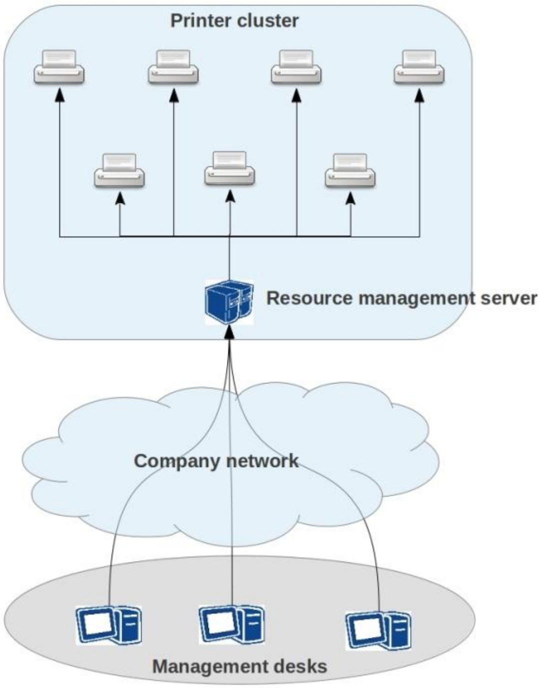


In this scenario, employees from a particular department send documents directly towards a common printing room. Although this room is in the vicinity of the offices, the documents are transferred via the company network, which is not physically confined to that department, and may in some architectures even exit the physical limit of the building during routing.

A malicious employee or external person can tap these lines and accumulate documentation concerning the company's operations, and even sensitive client- or financial data.

The sheer number of employees accessing the printing room is another risk factor, even with effective printing room access control in place. Since communication towards the printer comes from many different sources, and transits a large number of networking equipment, it is difficult to control all devices on the path from the employees to the printer. A malicious entity may easily connect snooping equipment on an intermediate switch without being noticed by the busy personnel.

Scenario 2: End-of-year bulk printing



The most sensitive time period for the printing network is the end of the fiscal- or calendar year. Managers from all departments print documents such as financial reports and summaries of the year´s business. The printer cluster used for this purpose is usually heavily guarded to prevent unauthorized access. But since the printer cluster is rarely next to the offices, the documents pass through a large portion of the company network before getting queued for printing.

There is a major risk that during this time someone might take advantage of this concentration of vital data and cause serious harm. Again, any intermediate networking devices are a potential risk, and an attacker may easily find a switch or router in a little frequented part of the building and use it for malicious purposes.

Towards security in the printer network

To prevent exploitation of the printing network for gaining access to sensitive data, encryption needs to be incorporated into the network.

However, it is not trivial to find a solution which is not only secure, but also simple to use due to the properties of a printing network.

Next to state-of-the-art security, there are three other requirements in such a scenario:

- ***Non-disruption of the current network architecture:***
  The company network architecture is carefully elaborated to best suit the needs of the organization. A security solution must not affect this architecture.
  Problems with an encryption device must not affect the rest of the network in any way.

- ***Low-cost installation and maintenance:***
  The amount of equipment to be purchased and its cost must be kept to a minimum. In addition, maintenance should require as little effort and time as possible from busy network and system administrators. Centralized management of all units must be possible.
  Redundancy/disaster recovery options must be available.

- ***Multipoint connectivity must be preserved:***
  Installing point-to-point encryption between each pair of communicating devices not only entails exceedingly difficult maintenance, but is also simply not scalable. Instead, having to install a security policy per encrypted connection, there must be the possibility to add new encryptors simply and efficiently to a single, fixed security policy.

We could restate these requirements as follows:

In a printing network, network performance and ease of maintenance cannot be compromised for security. Network administrators and system administrators must be as satisfied with the solution as the security administrator.

3. Conventional solutions

What about conventional solutions sometimes deployed in such cases?

IPSec

As a well-established and trusted solution to data encryption and authentication in IP networks, IPSec might spring to mind in the context of printing encryption as well. Unfortunately, it has two serious drawbacks that will prevent an IPSec deployment in the case of printing security:

- **Not scalable:**
  The most problematic issue of conventional encryption in networks such as a printer network is the lack of scalability caused by their inability to handle encrypted multipoint traffic. In solutions such as IPSec – which is entirely based on point-to-point tunnels - one would have to configure point-to-point encryption tunnels between each pair of encryptors, which represents significant time overhead for the responsible administrator.
  Consider for example a network of 20 encryptors. Using IPSec, the administrator would need to create 20*(20-1) = 380 tunnels. With each tunnel taking about 10 minutes to set up, this would amount to about 63 hours of work. This is because it is necessary to create a different policy per encryptor. The more encryptors there are, the more policies must be handled – clearly this doesn't scale with network size.

- **No management centralization:**
  With IPSec, each tunnel must be managed separately. Since configuration is done per device rather than per encryption policy, this is complex even for the simplest of cases.

These limitations significantly reduce IPSec's scalability, and therefore makes it unpractical in a printing network.

GET VPN

GET VPN prides itself on multi-point encryption support, and the possibility of central management through key servers. It might therefore look like a candidate for securing your printing network. It has, however, the following faults, which will prevent a GET VPN deployment from being useful:

- **Disruption of the current network architecture:**
  Since encryption is performed on GET VPN routers, you must replace or upgrade all routing equipment to the correct vendor or even the correct firmware version. This is expensive and entails vendor lock-in.
- **High-cost management and maintenance:**
  GET VPN supports using central key servers to provide encryption keys to the encrypting routers. Although these are not required, the alternative is to manage each tunnel separately, which does not scale, so purchasing key servers is strongly recommended. These servers cost in excess of CHF 10,000 each, which significantly increases the cost of deploying a GET VPN network.
- **Serious security faults:**
  - Redundant key servers are synchronized by a manual copy-paste of the master encryption key – this exposes the key and therefore corporate secrets to employees
  - Encryption can be disabled on encrypting routers by turning them on and off, or by simply rebooting the network interface – any technician can force your traffic to pass in the clear

GET VPN should be discounted on account of its security problems alone. In addition, it requires changes to the network architecture that are potentially expensive, not only in equipment cost but also in employee time.

Application-layer security

Another conventional solution might be to encrypt the outgoing connection from the end-user PC in software. Although this type of encryption happens at the highest OSI layers, it has the same disadvantages with respect to printing network deployment:

- **Not scalable:** Since the OSI application layer is responsible for end-to-end connections, setting up this type of encryption requires installing and maintaining a separate application on each single end user machine.
- **Powerful printers required:** Not all printers have the capacity to perform encryption and key exchanges, which reduces the usability of this type of solution to the rarest of cases.
- **Potential security problem:** Since encryption happens on the end-user´s machine, this solution effectively gives him control of the encryption, turning all employees into authorized security administrators. The probability of security problems due to mistakes or bribing increases.

Although often a cheap solution since only software components are required, its limited scalability, usability and potential authorization flaw reduce its applicability significantly.

4. Arcis – Quality and ease of use

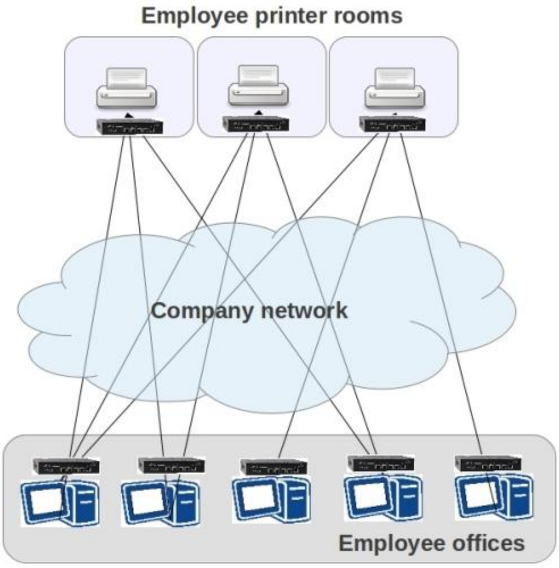
ID Quantique's Arcis family implements state-of-the-art security while also catering to the needs of network and system administrators, and is therefore a convenient, high-quality solution to printing network encryption. It requires minimal effort from the maintenance team while being completely transparent to end users.

The Arcis management platform, TrustNet Manager, is the tool that allows you to achieve easy management. One TrustNet Manager instance allows you to manage all devices in your entire network.

Securing Scenario 1 with Arcis

In scenario one, employees send day-to-day documents to printers. Accumulated, these documents may reveal a significant amount of information regarding the company's business or IP, and are therefore important to encrypt.

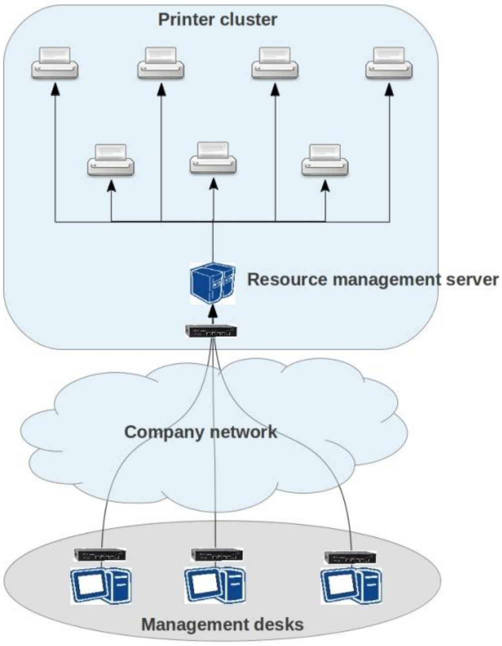
To secure the day-to-day printing of your employees, place an Arcis on your employees´ connection, and then secure the printer rooms. The encryptors can share a single key if desired, so that print jobs can be decrypted by any encryptor. Alternatively, you can divide users and printers into groups, and by distributing keys by group only allow specific employees to print on specific printers. This is configurable in a flexible, centralized manner through TrustNet Manager.



Securing Scenario 2 with Arcis

In scenario two, we need to ensure that bulk printed end-of-year financial and business data cannot be intercepted on their way to the secure printing cluster.

To ensure that no one can gather end-of-year documentation from the printing network, simply secure the outgoing connection of the management desks and the incoming connection in the printing cluster with Arcis. If more than one printer cluster exists, each requires only one Arcis at the entry point. At any time, more resource management servers can be added for load balancing or redundancy, either behind the existing Arcis, or with an Arcis of their own for complete independence.



5. Arcis Features in detail

Central management

The Arcis management solution, TrustNet Manager, is a virtual machine that can be conveniently accessed via a web interface. It is possible to access the management interface from anywhere, and all Arcis encryptors are managed centrally from one instance of TrustNet Manager. All operations needed to manage Arcis, such as the installation of a new device or the deployment of a new security policy, are centralized in the TrustNet Manager web interface.

TRUSTNET MANAGER

This ensures fast access to all your encrypted network and keeps maintenance operation complexity at a minimum.

Easy maintenance

Easy management

TrustNet Manager gives you immediate access to your entire encrypted network, and it also features a very easy-to-use user interface. As an example, consider this short instruction on how to deploy a new security policy, which in other products is usually one of the most complex operations:

To deploy a new security policy:

1. In the policy window, click on the features you wish your security policy to have to activate them (e.g. AES-256b encryption)
2. Drag-and-drop the encryptors you want to operate under this policy into the security policy window
3. Click ‘Deploy Policies’ – and you’re finished

Policy deployment using TrustNet Manager is so easy that anyone with a basic notion of security can deploy a simple policy intuitively.

Easy problem handling

Should you have a hardware problem with one of your encryptors, removing it from your network is simple: You only need to remove it from your policy, and redeploy the policy. No other part of your network is affected by the failed node, and you can handle the required re-configuration in less than a minute.

Multi-point encryption - Group keys

In an IPSec or application-layer secured network, the example network of 20 nodes took 63 hours to configure. Additionally, if the rekeying frequency is set to once per hour, that would result in 380 simultaneous key agreement algorithm executions clogging up the network every hour, and thus decreasing the available bandwidth.

With Arcis and TrustNet Manager, the same network is configurable in less than half an hour, since you can create a small number of policies and drag-and-drop your encryptors into them. This is the inverse approach to traditional solutions: You create the policies you want, and you add or remove encryptors as needed. This approach is truly scalable.

Thanks to this central approach, Arcis supports true and easily configurable multi-point encryption using so-called group keys – one key is distributed to all encryptors as are in the policy, rather than a having a different key per encryptor pair. This also reduces the rekeying traffic and allows to use more of the bandwidth for user traffic.

TrustNet Manager creates the key centrally, and then sends it to every concerned encryptor over a secure TLS channel. TrustNet Manager will space out the key communications over time in case there is a high traffic load – this way user traffic always has priority.

Support of group key encryption is only possible thanks to Arcis' unique approach to security: Although it is based on the well-known IPSec protocol and follows the standard to the letter, it does not force tunneling, but leaves it as an option. For multi-point architectures, it suffices to turn off tunneling to leverage group key encryption.

Failsafe rekeying

Those who have tested solutions such as GET VPN as a group key solution know the problem: A central key sever initiates a rekeying, but is not able to reach all encryptors with the new key. Two encryption keys now exist in the network, and you have two network partitions which can't communicate with each other.

TrustNet Manager solves this problem in two ways. First, old keys are always kept for another few minutes after a new key is received, in case delayed communication encrypted with the old key arrives. Secondly, it supports the fail-safe rekeying option: TrustNet Manager will contact all encryptors prior to distributing a new key. If even one encryptor isn't reachable, TrustNet Manager will not perform the rekeying at all, preferring to keep an old key for a little longer over network partitioning.

Redundancy / disaster recovery cluster

TrustNet Manager is never a single point of failure in the network: It is possible to install redundant copies or even deploy a disaster recovery cluster. The TrustNet Manager instances will update each other in real time, so that in case one instance fails, all others have full up-to-date configurations stored in them.

There are extensive back-up options to prevent loss of TrustNet Manager configurations and logs.

Easy integration

The architecture of a company network has been elaborated to fit as well as possible with the company's needs, so it would not only be expensive but also undesirable to change it. Arcis integrates into any existing network – it is fully vendor independent, and operates in all architectures. There is no need to adjust firewall settings for Arcis or TrustNet Manager, they will be completely transparent.

Although Arcis is IPSec based, it does not force to use tunneling, which could cause problems in firewall configurations and in the network architecture. Depending on current needs, you can at any time choose to enable tunnels to protect your IP addresses from prying eyes, or disable tunnels to simplify your firewall and addressing settings.

You can also specify your policies to be VLAN based for even more flexibility.

State-of-the-art security

Arcis offers the best security features available on the market

- Encryption using AES-128 to 256b, 3DES or Aria
- Authentication using the HMAC-SHA1 or HMAC-MD5
- With or without tunneling
- FIPS 140-2 certified physical tamper protection mechanisms

Additionally, Arcis and TrustNet Manager support a very fine-grained access control and authorization policy. The available user roles can be accumulated or held separately by each employee authorized to operate Arcis and TrustNet Manager.

6. Conclusion

Encrypting a printing network has special requirements that are not met by most conventional encryption products.

ID Quantique's Arcis, with its management platform TrustNet Manager, meets all these requirements while not compromising on security.

Using Arcis, you can install high security with minimal effort and minimal maintenance – Arcis offers security, simplicity and scalability.

All these qualities make ID Quantique's Arcis the recommended solution for encrypting printing networks in organizations of any size and dynamics.