Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES
AFFAIRES ÉTRANGÈRES
ET EUROPÉENNES

Atos

scytl

# Ministère des Affaires Etrangères et Européennes

## Elections législatives de 2012 pour les Français de l'étranger – vote électronique

## Online Platforms Configuration Guide

Version 0.0

02 December 2011

## Strictly confidential

*Scytl Secure Electronic Voting*

*STRICTLY CONFIDENTIAL*

*Use only for evaluation purposes*

*The property of the cryptographic mechanisms and protocols described in this document is protected by their owners*

## Revision chart

| *Version* | *Date* | *Primary Author(s)* | *Reviewed by* | *Description* |
|---|---|---|---|---|
| 0.0 | 02-12-2011 | HJA/ARA | ASM/ARA | Initial document |

## Table of content

## List of tables



## List of figures

## Preface

This document lists the recommended hardware, software and connectivity requirements in order to install and configure the online infrastructure for the Electronic Voting Solution in a high availability environment at a data center which must cope with a high volume of connections/voters as in the case of Elections législatives de 2012 pour les Français de l'étranger – vote électronique project.

This document also includes the security measures implemented by ATOS Worldline to fulfill the project's requirement on this area.

NOTE about the document language:
This document has been created to provide the ANSSI with a single document compiling the online platforms configuration details. This is the result of the compilation of two previously existing documents:

- Online HW Requirements, a working paper between ATOS Worldline and Scytl;
- Dossier d'Architecture Technique, an extinct document containing general information about the solution.

For that reason, the sections including information to be agreed between ATOS Worldline and Scytl are written in English, while the security measures, corresponding to internal ATOS Worldline inirmation is written in French.

This document will evolve by adding new details on the different topics to be agreed between Scytl and ATOS Worldline.

### Document structure

This document is organized as follows:

- Chapter 1 provides details on the Hardware and Software requirements
- Chapter 2 provides details on the Required Services to be provided by the Data Center;
- Chapter 3 provides details on the VPN configuration
- Chapter 4 provides details on the installation and configuration procedures;
- Chapter 5 provides details on the supervision strategy and architecture;
- Chapter 6 provides details on the security strategy.

### Related documents

- MAEE_eVote2012_InventaireInfrastructure_v1.2.xlsx, Atos/Scytl, November 2011.
- MAEE_DAT_2012, Atos/Scytl, November 2011.

# 1 Hardware and Software requirements

Pnyx is a highly scalable solution, as it is made up of independent components that only need to be replicated on more servers to be able to support a higher load. In the description below Scytl is assuming the data center includes all standard physical and logical security measures, as well as high availability on power source and Internet access.

## 1.1 Hardware platforms sizing

### *1.1.1 Common infrastructure*

- 2 active-passive firewalls connected to an Internet Service Provider on one end and to load balancers on the other.
- All required switches to configure VLANs and interconnect the previously listed devices.
- 1 pre-production front-end server, running 4 NGINX and mail relay, and connected to the pre-production application servers
- 1 pre-production application server, running 8 Tomcats, the voting portal T1 and T2 , password recovery portal T1 and T2 , ActiveMQ, Pnyx Portal component T1 and T2 and Pnyx Back-Office component T1 and T2, connected to the pre-production database server.
- 1 pre-production database server (PDS), running 4 Oracle DB ; One for Vote T1, one for Vote T2, one for Password recovery T1 and one for Password recovery T2.

### *1.1.2 Voting System*

The servers and software required to run Pnyx for the e-voting solution at the data centre are:

#### *1.1.2.1 First Round Voting Platform*

- 2 load balancers working in failover (active-passive), connected to the "voting system" front-end servers. The load balancing is carried out at IP level.
- 2 "voting system" front-end servers (VFS), and connected to the voting application servers.
- 2 "voting system" application servers (VAS) running Tomcat, ActiveMQ, Pnyx Portal component and Pnyx Back-Office component, connected to the voting database cluster.
- 2 voting database servers (VDS) configured in cluster (active-pasive with data guard).

#### *1.1.2.2 Second Round Voting Platform*

- 2 load balancers working in failover (active-passive), connected to the "voting system" front-end servers. The load balancing is carried out at IP level.
- 2 "voting system" front-end servers (VFS), running, and connected to the voting application servers.

- 2 "voting system" application servers (VAS) running Tomcat, ActiveMQ, Pnyx Portal component and Pnyx Back-Office component, connected to the voting database cluster.
- 2 voting database servers (VDS) configured in cluster (active-pasive with data guard).

### 1.1.3 Password Recovery System

- 2 load balancers working in failover (active-passive) connected to the "password recovery" front-end servers. The load balancing is carried out at IP level.
- 2 "password recovery" front-end servers (PRFS), running NGINX, and connected to the "password recovery" application servers. The mail relay will also be installed on these two front servers.
- 2 "password recovery" application servers (PRAS), running Tomcat, the voter portal and "password recovery" back office connected to the "password recovery" database cluster
- 2 "password recovery" database servers (PRDS) configured in cluster (active-pasive with data guard).

Note that all the components except for the pre-production environment is replicated to ensure a high availability environment. Only the production databases (voting and password recovery) are connected using dual path. Firewalls and load balancers do not need to be dedicated (they could be shared in the data centre if required). Servers should be dedicated due to security measures.

The following figure shows a diagram of the hardware layout.

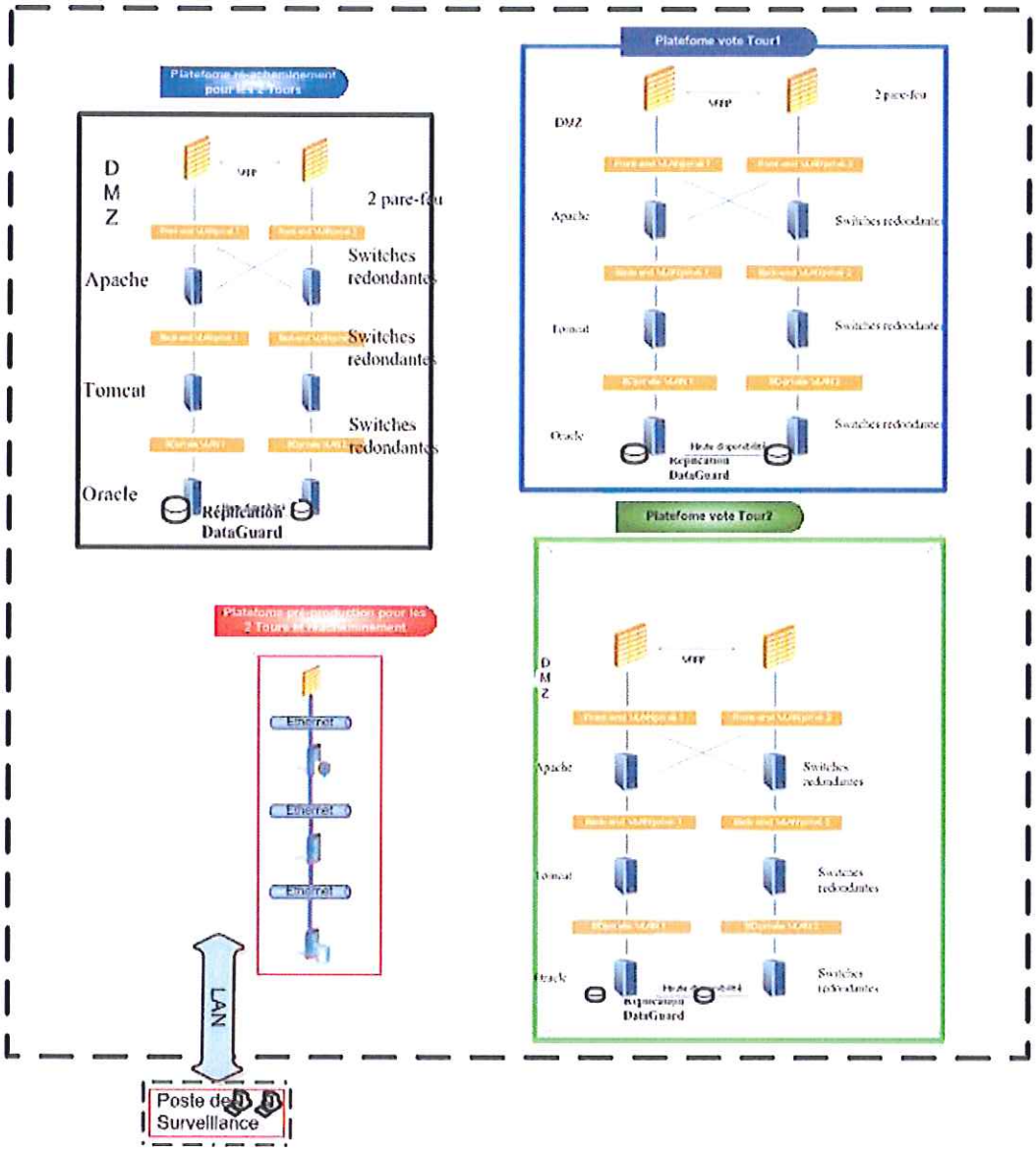



*Figure 1-1 – Infrastructure – General architecture at Data Center*

## 1.2 Architecture

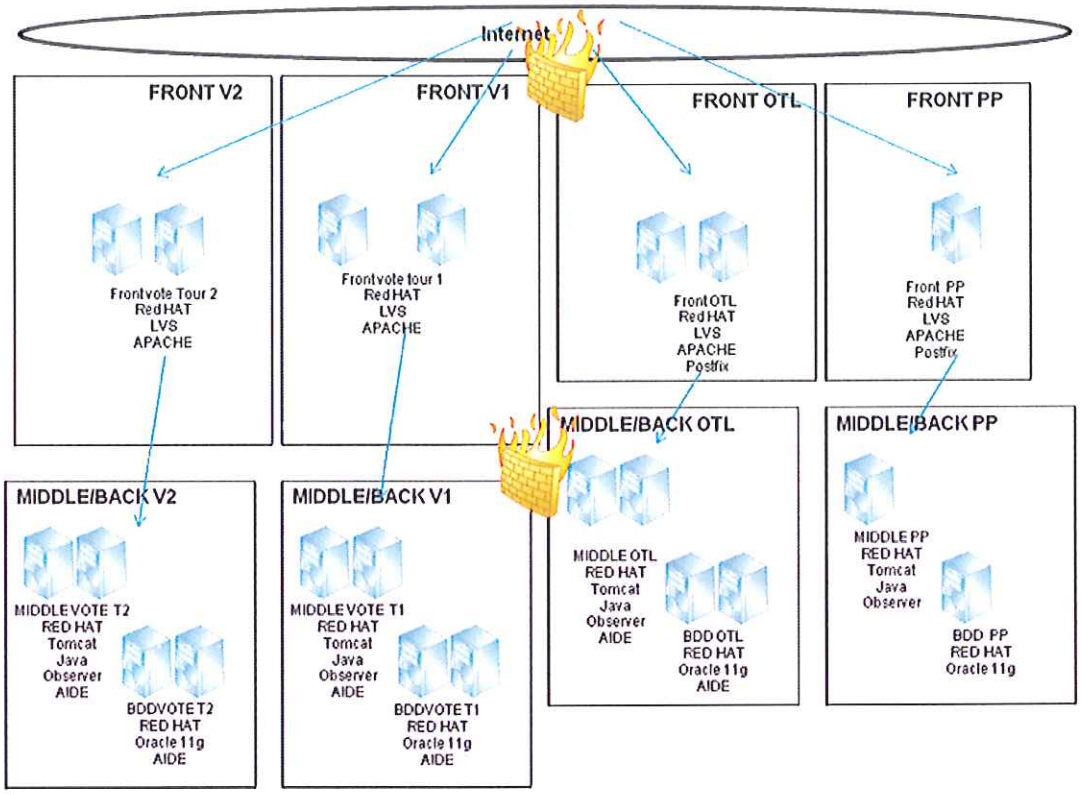



*Figure 1-2 – Infrastructure – Detailed architecture*

## 1.3 Platform Components

### 1.3.1 Firewall / Load Balancers / Switches

The firewalls and load balancers available in the data center need to support the number of connections required by the voting platform based on customer's requirements, and allow sticky sessions and/or persistence based on IP address, unless the front-end servers provide it. There should be a pair of each of them, configured as active-passive for redundancy purposes.

| Firewalls | Load Balancers |
|---|---|
| Firewalls Front : 2 x Cisco ASA 5510 active-passive<br>Firewalls Middle : 2x Fuji Rx100 /OpenBSD | 2 LVS active-passive |

*Table 1-1 Infrastructure – Network components*

### 1.3.2 Voting System

The configuration of the voting servers for each round is listed below. This configuration is to support 1.2 Million voters for May 2012 (or June 2012) elections.

| Machine | Front | Application | Database |
|---|---|---|---|
| # Servers | 2 | 2 | 2 |
| Server Model | Moyen de gamme (e.g. Proliant DL360 G7) | Moyen de gamme (e.g. Proliant DL360 G7) | moyen de gamme (e.g. Proliant DL380 G7) |
| RAM | Xeon Quad-core x2 | Xeon Quad-core x2 | Xeon Dual-core x1 |
| RAM | 8 GB RAM | 64 GB RAM | 16 GB RAM |
| HD | 2*146 GB SAS 10k Raid 1 | 2*146Go Raid 1 + 2*300 GB SAS 10k Raid 1 | 4*146 GB SAS 10k Raid 1 |
| Network | 1 x Dual Ethernet card | 1 x Dual Ethernet card | 2 x Dual Ethernet card |
| Other | 1 x Power Supply | 1 x Power Supply | 2 x Power Supply |
| Software | • Red Hat Linux Enterprise Server 5.6 64bit (Linux 2.6.18-274.el5)<br>• NGINX web server ( (x2)<br>• AIDE | • Red Hat Linux Enterprise Server 5.6 64bit (Linux 2.6.18-274.el5)<br>• Tomcat 6.0.29<br>• Java 1.6.0_u24 SE + Install Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6<br>• add **rngd** entropy daemon<br>• component Pnyx Portal<br>• component Pnyx Back Office<br>• activeMQ 5.4.2<br>• Oracle SQL Client<br>• AIDE | • Red Hat Linux Enterprise Server 5.4 64bit (Linux 2.6.18-164.el5)<br>• Oracle 11g Enterprise Database with Data Guard and UTF8<br>• AIDE |

*Table 1-2 Voting system platform components for one round*

NOTE: Oracle has to be configured to create a copy of all the stored data in the local tapes. A new tape has to be used every day during the electoral process. Notice that the data of all the elections will be stored by the same RDBMS in the same physical storage device and back-up tapes.

Backup strategy: on tapes

- Full every week
- Archive logs :twice a day
- Data guard: max availability: change applied on all nodes.

#### 1.3.2.1 Voting Application server partition needs

| Directory | Allocated Space desired in GB after adding new HDD |
|---|---|
| /MIDDLE | 120,0 |
| /MIDDLELOGS | 120,0 |
| /usr/local/oracle | 0,0 |
| /usr/local/activemq | 0,0 |
| /tmp | 60,0 |

### 1.3.3 Password Recovery System

The configuration of the password recovery servers is listed below. This configuration is to support 1.2 M voters for May and June 2012 elections.

| Machine | Front | Application | Database |
|---|---|---|---|
| **# Servers** | 2 | 2 | 2 |
| **Server Model** | HP DL380G5 | HP DL380G5 | HP DL380G5 |
| **CPU** | 1 CPU quad core | 2 CPU quad-core | 1 CPU DualCore |
| **RAM** | 4 GB RAM | 8 GB RAM | 16 GB RAM |
| **HD** | 2*72 GB SAS 10k Raid 1 | 4*72 GB SAS 10k Raid 0+1 | 4*146 Go SAS 10k Raid 0+1. Allocated space : 60 GB for each round |
| **Network** | 1 x Dual Ethernet card | 1 x Dual Ethernet card | 2 x Dual Ethernet card |
| **Other** | 1 x Power Supply | 1 x Power Supply | 2 x Power Supply |
| **Software** | • Red Hat Linux Enterprise Server 5.6 64bit (Linux 2.6.18-274.el5)<br>• NGINX web server (x2)<br>• Postfix<br>• AIDE | • Red Hat Linux Enterprise Server 5.6 64bit (Linux 2.6.18-274.el5)<br>• Tomcat 6.0.29<br>• Java 1.6.0_u24 SE + Install Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6<br>• add **rngd** entropy daemon<br>• Recovery password Portal | • Red Hat Linux Enterprise Server 5.4 64bit (Linux 2.6.18-164.el5)<br>• Oracle 11g Enterprise Database with Data Guard and UTF8<br>• AIDE |

| | | | |
|---|---|---|---|
| | | • Recovery password BO<br>• AIDE | |

*Table 1-3 Recovery Password system platform components*

NOTE: Oracle has to be configured to create a copy of all the stored data in the local tapes. And a new tape has to be used every day during the electoral process. Notice that the data of all the elections will be stored by the same RDBMS in the same physical storage device and back-up tapes.
Backup strategy : on tapes

- Full every week
- Archive logs :twice a day
- Dataguard : max availability : change applied on all nodes.

#### *1.3.3.1 Password Recovery Server partition needs*

| Directory | Allocated Space desired in GB after adding new HDD |
|---|---|
| /MIDDLE | 36 |
| /MIDDLELOGS | 18 |
| /usr/local/oracle | 0 |
| /tmp | 18 |

### *1.3.4 Preproduction System*

The preproduction platform should allocate 3 applications, 2 Voting Systems and 1 Password Recovery System.

| Machine | Front | Application | Database |
|---|---|---|---|
| **# Servers** | 1 | 1 | 1 |
| **Server Model** | Moyen de gamme (e.g. Proliant DL360 G7) | Moyen de gamme (e.g. Proliant DL360 G7) | moyen de gamme (e.g. Proliant DL380 G7) |
| **RAM** | Xeon Quad-core x2 | Xeon Quad-core x2 | Xeon Quad-core x1 |
| **RAM** | 8 GB RAM | 64 GB RAM | 16 GB RAM |
| **HD** | 2*146 GB SAS 10k Raid 1 | 2*146 GB SAS 10k Raid 1+ 2*300 GB SAS 10k Raid 1 | 4*146 GB SAS 10k Raid 1 |
| **Network** | 1 x Dual Ethernet card | 1 x Dual Ethernet card | 2 x Dual Ethernet card |
| **Other** | 1 x Power Supply | 1 x Power Supply | 2 x Power Supply |
| **Software** | • Red Hat Linux Enterprise Server 5.6 64bit (Linux 2.6.18-274.el5) | • Red Hat Linux Enterprise Server 5.6 64bit (Linux 2.6.18-274.el5) | • Red Hat Linux Enterprise Server 5 64bit (Linux 2.6.18-164.el5) |

| | | | |
|---|---|---|---|
| | • NGINX web server (x2)<br>• AIDE | • Tomcat 6.0.29<br>• Java 1.6.0_u24 SE + Install Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6<br>• add **rngd** entropy daemon<br>• component Pnyx Portal<br>• component Pnyx Back Office<br>• Recovery password Portal<br>• Recovery password BO<br>• activeMQ 5.4.2<br>• Oracle SQL Client<br>• AIDE | • Oracle 11g Standard Database withUTF8<br>• AIDE |

*Table 1-4 Pre-production platform components*

#### *1.3.4.1 Prepoduction server partition needs*

| Directory | Allocated Space desired in GB after adding new HDD |
|---|---|
| /MIDDLE | 120,0 |
| /MIDDLELOGS | 120,0 |
| /usr/local/oracle | 0,0 |
| /usr/local/activemq | 0,0 |
| /tmp | 60,0 |

### *1.3.5 Monitoring System*

There must be a system to alert the BVE (Bureau de Vote Electronique) in case on intervention in the Voting System.

*Le processus serait le suivant :*

*1) Un script est effectué périodiquement (la période est à définir mais disons quotidiennement) sur la plate-forme de vote qui examinera les logs du système d'exploitation. (Il faut savoir que toute personne qui se loggue est automatiquement enregistrée par le système dans un fichier syslog). Le script extrait toutes les lignes de ce fichier relatives à une connexion. Et les mettra dans un fichier daté du jour.*

*2) Il y aura donc un fichier de trace par jour. Ces fichiers seront créés avant la période de vote et suivis par le logiciel AIDE (donc inclus dans le scellement).*

*3) Ainsi si il y a eu connexion, le fichier de trace du jour sera modifié (par le script) et AIDE l'indiquera.*

*4) L'exploitant récupère le fichier et le transmet à qui de droit*

Details of procedure from AWL:

- Each server will be sealed logicaly using aide. Each day a check is performed on each server and a report is sent by email to BVEC, scytl, Atos and AWL addresses To be defined.
- Each day a script will run to check ssh access, if a ssh access is detected, a mail will be sent to BVEC, scytl, Atos and AWL addresses. To be defined.
- A desktop computer will be used by operators to run daily procedure, access the server if needed.

## 1.4 Logical distribution of the different applications

The proposed deployment of the voting platform components and the password recovery platform in the previously described infrastructure for **May's and June's elections** is as follows.

### *1.4.1 Voting System*

The voting servers will need to support up to 1,000,000 votes per day during May and June 2012.

- There will be a single institution configured in Pnyx, supporting all required elections and a common electoral roll of 1.200,000 voters
- Each of the VFS will run 2 instances of NGINX.
- Each VAS will run 2 instances of Tomcat:
  - One Tomcat will manage the instance of Pnyx Portal.
  - One Tomcat will manage the instance of Pnyx Back-Office.
- There will be the following mapping:
  - **1 to 2 between one Nginx in the VFS and the Pnyx Portal Tomcat in the VAS. i.e. Once a session is opened there won't be any kind of balancing between tomcats.** Loadbalancers will redirect to the both nginx without handling IP persistence because Nginx will redirect to the same tomcat for all connection from the IP (not if tomcat is down).
  - **1 to 1 between one NGINX in the VFS and the Pnyx Back-Office Tomcat in the VAS.** As each Tomcat will have a different URL, **NGINX** will redirect the queries to the appropriate Tomcat.
- Therefore, Voter's connections to each of the two **NGINX** servers will be redirected to the 2 voting portals to balance the incoming connections from voters for a IP the connection is made between the same servers when tomcat servers is available.. Both Pnyx Portal instances will share the same URL (URL_A).
- Each VAS will also run an ActiveMQ service in cluster, used by the Pnyx Back-Office to deploy different configuration files to each of the Pnyx Portals
- The access to the 2 instances of Pnyx Back-Office will not be balanced t NGINX level. Each Pnyx Back-Office instance will have a different URL (URL_B1 and URL_B2).

- All 2 Pnyx Portal and 2 Pnyx Back-Office instances will connect to the active node of the database cluster.
- There will be a single instance of Oracle RDBMS in each of the VDS, which will be synchronized by means of Data Guard. There will be a single database managed by this RDBMS.

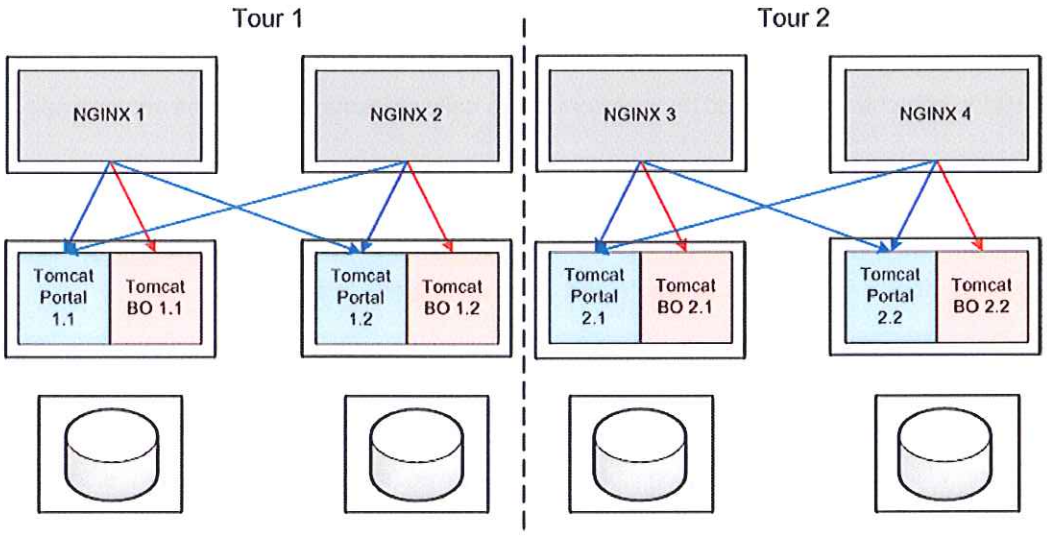



*Figure 1-3 – Distribution of the logical components in voting servers*

### *1.4.1.1 Service on each server:*

#### 1.1.1.1.1 Front:

Official URLs to be provided by MAEE/AOSI

2 NGINX services:

- https://www.scrutin.diplomatie.gouv.fr/portal/
- backoffice.scrutin.diplomatie.gouv.fr -> Redirection rules to the 2-Tomcat backoffice (VPN Only, no Public IP).

Voting BO 1: https://DNS_NAME/pnyx-bo1

Voting BO 2: https://DNS_NAME/pnyx-bo2

#### 1.1.1.1.2

Here is the AWL IP/DNS :

Portail T1

https://www-election2012-t1-afe.aw.atosorigin.com/

BO T1

https://backoffice.election2012-t1.afe.priv.atos.fr/bo1

https://backoffice.election2012-t1.afe.priv.atos.fr/bo2

Portail T2

https://www-election2012-t2-afe.aw.atosorigin.com/

BO T2

https://backoffice.election2012-t2.afe.priv.atos.fr/bo1

https://backoffice.election2012-t2.afe.priv.atos.fr/bo2

#### 1.1.1.1.3 Middle :

2 **services Tomcat /server:**

**1 portal services :** www.**scrutin**.diplomatie.gouv.fr

**1 BO services : backoffice.scrutin.diplomatie.gouv.fr**

#### 1.1.1.1.4 BDD:

1 instance BDD /server

**Tour 1 :**

**Instance active on bpafe101v** : AFE1PRD ,

**Instance standby (passive) on bpafe102v** : AFE1PRD_STB,

**Tour 2 :**

**Instance active on bpafe201v** : AFE2PRD ,

**Instance standby (passive) on bpafe202v** : AFE2PRD_STB

### *1.4.2 Password Recovery Platform*

The password recovery servers will need to support up to 200,000 connections per day during May and June 2012.

- The password recovery servers will host two different applications (2 tomcats):
  - The first tomcat hosts the password recovery portal
  - The second tomcat runs the password recovery back-office
- Each PRFS will run 1 instance of NGINX: Portal and BO will have different URLs so NGINX will redirect using the rules below
  - /bo* to Tomcat BO password recovery (reacheminement-elections-diplomatie-gouv-fr)
  - /portail* to Tomcat portal password recovery (mdp-scrutin-diplomatie-gouv-fr)
- Each PRAS will run 2 instances of Tomcat:
  - One for the password recovery back-office. **There will be a mapping 1 to 1 between the NGINX in the PRFS and the Tomcats in the PRAS, i.e. NGINX WILL only connect to a specific Tomcat always, and will NOT do any kind of balancing**. This condition, together with the balancing done by the load balancers which address the petitions of the same voter to the same NGINX (based on IP address), is what we call **STICKY SESSIONS**, and it is a requirement.
- Both password recovery back-office instances will connect to the active node of the database cluster.

- There will be a single instance of Oracle RDBMS in each of the PRDS, which will be synchronized by means of Data Guard. There will be a single database managed by this RDBMS for the password recovery back-office.

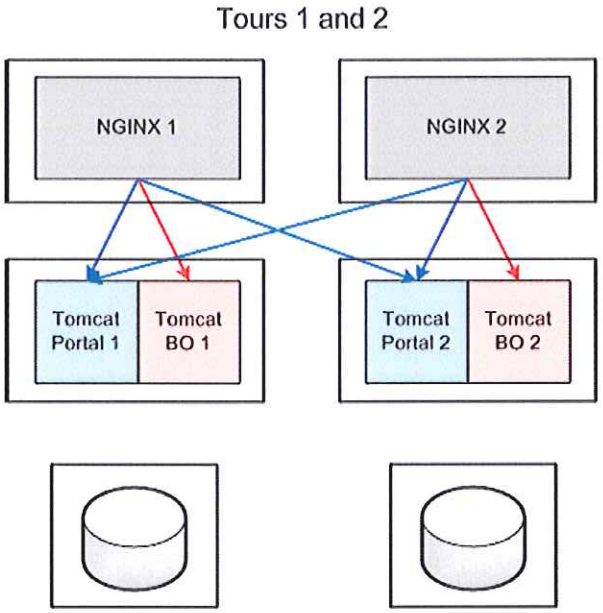



*Figure 1-4 – Distribution of the logical components in password recovery servers*

### *1.4.2.1 Service on each server:*

#### 1.1.1.1.5 Front:

1 NGINX services/server + 1 postfix (mail)

- https://www.reacheminement.elections2012.diplomatie.gouv.fr/portail/ (public access / no VPN / no Warning about security )
- mailrelay.vdm.afe.priv.atos.fr postfix

DNS AWL for tests

Portail T1 https://www-reacheminement-election2012-t1-afe.aw.atosorigin.com/

Portail T2 https://www-reacheminement-election2012-t2-afe.aw.atosorigin.com

BO T1

https://www-reacheminement-election2012-t1-afe.aw.atosorigin.com/reacheminement1

https://www-reacheminement-election2012-t1-afe.aw.atosorigin.com/reacheminement2

BO T2

https://www-reacheminement-election2012-t2-afe.aw.atosorigin.com/reacheminement1/

https://www-reacheminement-election2012-t2-afe.aw.atosorigin.com/reacheminement2/OK

#### 1.1.1.1.6 Middle:

2 services Tomcat

portail.election2012.diplomatie.gouv.fr

- https://tpafe001v.priv.atos.fr:8002/portail ( VPN access)
- https://tpafe002v.priv.atos.fr:8002/portail ( VPN access)

reacheminement.election2012.diplomatie.gouv.fr

- https://tpafe001v.priv.atos.fr:8001/bo ( VPN access)
- https://tpafe002v.priv.atos.fr:8001/bo ( VPN access)

#### 1.1.1.1.7 BBD:

2 instance BDD /server

**Instance active sur bpafe001v** : AFE0PRD , AFE3PRD,

**Instance standby (passive) sur bpafe002v** : AFE0PRD_STB, AFE3PRD_STB,

### *1.4.3 Preproduction Platform*

**qlf.www.election2012-t1.diplomatie.gouv.fr**

IP/Nom publique: 160.92.182.217 qlf-www-election2012-t1.aw.atosorigin.com

IP/Nom interne: 10.18.113.220 qlf-www-election2012-t1.afe.priv.atos.fr

curl -k https://qlf-www-election2012-t1.aw.atosorigin.com/portail/OK

⇨ tqafe01v - www.election2012-t1.diplomatie.gouv.fr

**qlf.www.election2012-t2.diplomatie.gouv.fr**

IP/Nom publique: 160.92.182.218 qlf-www-election2012-t2.aw.atosorigin.com

IP/Nom interne: 10.18.113.221 qlf-www-election2012-t2.afe.priv.atos.fr

curl -k https://qlf-www-election2012-t2.aw.atosorigin.com/portail/OK

⇨ tqafe01v - www.election2012-t2.diplomatie.gouv.fr

**qlf.www.reacheminement.election2012-t1.diplomatie.gouv.fr**

IP/Nom publique: 160.92.182.221 qlf-www-reacheminement-election2012-t1.aw.atosorigin.com

IP/Nom interne: 10.18.113.224 qlf-www-reacheminement-election2012-t1.afe.priv.atos.fr

curl -k https://qlf-www-reacheminement-election2012-t1.aw.atosorigin.com/portail/OK

⇨ tqafe01v - portail.election2012-t1.diplomatie.gouv.fr

**qlf.www.reacheminement.election2012-t2.diplomatie.gouv.fr**

IP/Nom publique: 160.92.182.223 qlf-www-reacheminement-election2012-t2.aw.atosorigin.com

IP/Nom interne: 10.18.113.226 qlf-www-reacheminement-election2012-t2.afe.priv.atos.fr

curl -k https://qlf-www-reacheminement-election2012-t2.aw.atosorigin.com/portail/OK

⇨ tqafe01v - portail.election2012-t2.diplomatie.gouv.fr

**qlf.backoffice-election2012-t1.diplomatie.gouv.fr**

IP/Nom publique: 160.92.182.219 qlf-backoffice.election2012-t1.aw.atosorigin.com

IP/Nom interne: 10.18.113.222 qlf-backoffice.election2012-t1.afe.priv.atos.fr

curl -k https://qlf-backoffice.election2012-t1.aw.atosorigin.com/bo/OK

⇨ tqafe01v – backoffice-election2012-t1.diplomatie.gouv.fr

**qlf.backoffice-election2012-t2.diplomatie.gouv.fr**

IP/Nom publique: 160.92.182.220 qlf-backoffice.election2012-t2.aw.atosorigin.com

IP/Nom interne: 10.18.113.223 qlf-backoffice.election2012-t2.afe.priv.atos.fr

curl -k https://qlf-backoffice.election2012-t2.aw.atosorigin.com/bo/OK

⇨ tqafe01v – backoffice-election2012-t2.diplomatie.gouv.fr

## 1.5 Connections and bandwidth

The complete voting platform (including pre-production, password recovery, voting and monitoring) has certain requirements in terms of interconnecting the different services, connecting to external services or allowing connections to certain applications. Also, a scenario to estimate the required bandwidth is presented.

### *1.5.1 Bandwidth calculations*

Bandwidth calculations are based on the MAEE electoral scenario and the assumptions listed below:

#### 1.1.1.1.8 Voting process by voters:

Considering a typical access where a voter casts one vote.

- Web pages: approx. 250 Kbytes plus the size of a ballot in the ballot page, 50 Kbytes
- Voting client (applet): around 800 Kbytes for Java 6.
- Java detect (applet to detect your configuration): around 100 Kbytes for Java 6

#### 1.1.1.1.9 Access to Pnyx back-end:

There is one applet plus pure web navigation. There is also information to be uploaded.

- Login applet (required every time I log into the system): around 200 Kbytes for Java 6
- The other actions (web navigation through the BO to see things): standard web navigation pattern, we cannot predict.
- Uploading of electoral roll: about 10-10Kbytes per voter (includes the PKCS12 per voter)
- Uploading the candidates: small XML file, maybe in this scenario 50 Kbytes.

#### 1.1.1.1.10 One time link

The access will be limited to a two pages process:

- Initial page with the form that asks for different information (about 60Kbytes)
- Page with the authentifiant if the access is successful, or an error page otherwise (40Kbytes)

### 1.5.2 Database connections requirements

Below are the database connections requirements for the Password Recovery (PRAS) and the Voting system (VSAS)

| **DB Connections** | | | | | |
|---|---|---|---|---|---|
| Physical machines | 2 | Physical machines | 2 | Physical machines | 2 |
| Tomcats per Machine | 3 | Tomcats per Machine | 3 | Tomcats per Machine | 2 |
| Wars per Tomcat | 1 | Wars per Tomcat | 1 | Wars per Tomcat | 1 |
| Connections per War | 100 | Connections per War | 100 | Connections per War | 100 |
| **Total for VSAS T1** | **600** | **Total for VSAS T2** | **600** | **Total for PRAS** | 400 |

| **DB SPACE** | | | | | |
|---|---|---|---|---|---|
| | **size in GB** | | **size in GB** | | **size in GB** |
| **Total for VSAS T1** | **30** | **Total for VSAS T1** | **30** | **Total for PRAS** | **5** |

Remark: The number of connections per War will depend on the configuration of Tomcat and how many inbound connections are accepted by the NGINX server

### 1.5.3 External connections

The following connections between the services hosted in the data center and external systems/users are foreseen:

| Origin | Destination | Connection type | Comments |
|---|---|---|---|
| Réacheminement BackOffice (x2) | Email service | HTTPS with server authentication<br>Pas HTTPS mais SMTP. | Name: mailrelay.vdm.afe.priv.atos.fr<br>Address: 10.18.113.151<br>Ip Publique visible for MAEE : 160.92.182.209 |
| Computers used by MAEE staff and other actors to be defined | Réacheminement BackOffice (single URL) | HTTPS with bidirectional authentication | This will be the "VPN" secure connection |
| Initialization users at system startup | Réacheminement BackOffice initialization page (one different URL per instance) | HTTPS with bidirectional authentication | This will be the "VPN" secure connection |

| | | | |
|---|---|---|---|
| Initialization users at system startup | Réacheminement Portal initialization page (one different URL per instance) | HTTPS with bidirectional authentication | This will be the "VPN" secure connection |
| Voters and visitors | Onte-time-link (single URL) : Password recovery Portal or ??? | HTTPS with server authentication | |
| Voters and visitors | Pnyx Portal (single URL) | HTTPS with server authentication | |
| Computers used by MAEE staff and other actors to be defined | Pnyx BackOffice (one different URL per instance) | HTTPS with bidirectional authentication | This will be the "VPN" secure connection |
| Computers MAEE staff and other actors to be defined | Monitoring Server Apache (single URL) | HTTPS with server authentication | No monitoring server. |
| Scytl's offices | All servers but the databases | IPSec VPN using Cisco client | Used for deployment, configuration and testing. To be closed during the election. |
| Scytl's offices | Réacheminement servers | IPSec VPN using Cisco client | Used for deployment, configuration and testing. To be closed during the election. |
| The same users as in the production environment | All services available in the pre-production server | HTTPS with server authentication for public services<br>HTTPS with bidirectional authentication for private services | Replicate the connection type found on the equivalent production servers |

*Table 1-5 External Connections*

### 1.5.4 URLs

- mailrelay.vdm.afe.priv.atos.fr/mailrelay-afe.aw.atosorigin.com
  - 10.18.113.151/160.92.182.209.
- reacheminement.election2012.diplomatie.gouv.fr :
  - 10.18.113.150/160.92.182.201 www-reacheminement-election2012-t1.afe.priv.atos.fr/www-reacheminement-election2012-t1-afe.aw.atosorigin.com.

- 10.18.113.154/160.92.182.202 www-reacheminement-election2012-t2.afe.priv.atos.fr/www-reacheminement-election2012-t2-afe.aw.atosorigin.com

- https://www.elections2012.diplomatie.gouv.fr/portal/ :
  - 10.18.113.20/160.92.182.210 www-election2012-t1.afe.priv.atos.fr/www-election2012-t1-afe.aw.atosorigin.com.
  - 10.18.113.80/160.92.182.193 www-election2012-t2.afe.priv.atos.fr/www-election2012-t2-afe.aw.atosorigin.com
- backoffice.elections2012.diplomatie..gouv.fr : No Public IP
  - 10.18.113.21 backoffice.election2012-t1.afe.priv.atos.fr.
  - 10.18.113.81 backoffice-election2012-t2.priv.atos.fr.

Public IP will be available when DNS/URL is validated.

### 1.5.5 Internal connections

| Origin | Destination | Connection type | Comments |
|---|---|---|---|
| Réacheminement BackOffice | SMTP Server | SMTP | |
| Monitoring Server | Pnyx Back Office | Read only Database connection. | In order to execute the log validation on the monitoring server. No monitoring server. |
| All the servers | Monitoring Server | File copied with rsynch | Information to validate AIDE sealing |
| Pnyx Portal and BackOffice (x4) | Monitoring Server | File copied with rsynch | Immutable logs. Details of this interface not agreed yet |
| Réacheminement BackOffice (x2) | Monitoring Server | Files copied with rsynch | • Immutable logs.<br>• Details of this interface not agreed yet |
| Voter web Portal (x4) | Pnyx Back Office web services interface (x2) | HTTP | Accès to NGINX or TOMCAT ? |

*Table 1-6 Internal Connections*

## 1.6 Monitoring the voting application

Pnyx Portal and Pnyx Back-Office incorporate a service check facility that allows load balancers to verify if the application is up and running properly. In case there is any failure on the NGINX server or individual tomcat servers, the load balancers (assuming that support service check queries) detect the failed service check response and redirects the connections of the election/s correlated to the service check to any other logical branch.

# 2 Required Services to be provided by the Data Center

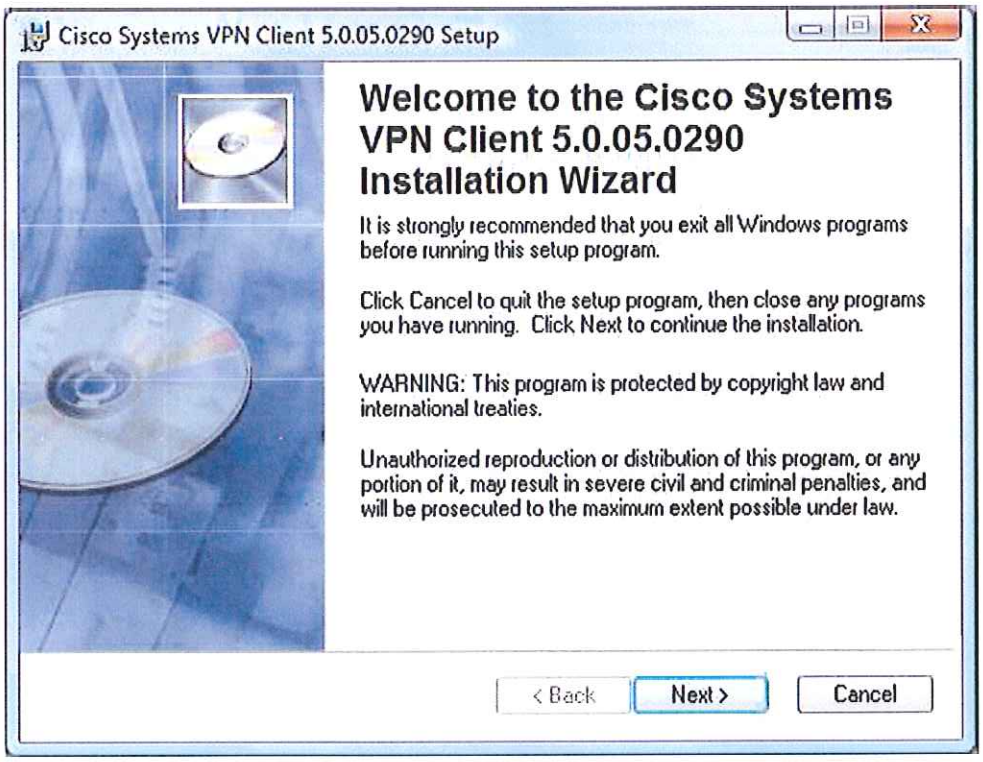
Besides the previous components, Scytl requires that the data center offers the services listed below:

- Installation of all the hardware and software components. Scytl, once everything is installed, will deploy Pnyx and the password recovery components.
- Full system administration
  - Hardware and COTS software 24x7 monitoring
  - Upgrades and patches application
  - Performance and issues reporting
  - Networking and security appliances
- Hardening of all elements
- Redundant internet connectivity and valid internet IP's
- Enough band-width for the service (as defined above)
- Real time monitoring of all its elements
- Intrusion Detection System (some firewalls/load balancers include this feature)
- Everything installed in a dedicated rack that could be, if required by customer, sealed physically.
- On-site support if required by auditors or third trusted parties in terms of site reviews, logical sealing and alike
- Backup of the information and Secure destroy (wipe conform military standards) of storage media after the end of election.

# 3 Configuration du VPN

Un compte VPN est créé sur le serveur VPN, puis l'utilisateur de ce compte configure son ordinateur avec les éléments suivants :

1. Installation du client VPN cisco :




2. Démarrage du client VPN
3. L'utilisateur importe le fichier de configuration « .pcf » (menu import), ce fichier est fourni par AWL.
   Ce fichier contient des éléments nécessaire à la connexion VPN tels que l'IP à atteindre, le nom de Group, un mot de passe crypté…
4. Une connexion VPN est établie avec toutes les plates-formes MAEE E-VOTE

En ce qui concerne les différents points de sécurité concernant la partie serveur du VPN :

a) La désactivation des interfaces inutilisées. En cours
b) Paramétrage du BIOS sécurisé : Au vu de la sécurisation du site, de la salle et des serveurs, l'accès au BIOS des serveurs est extrêmement difficile. AOW a donc estimé qu'il n'est pas nécessaire de sécuriser le BIOS du serveur.
c) La Sécurité physique du serveur VPN est assurée par une baie fermée à clef.
d) Les ouvertures de session sont sécurisées par login/mot de passe.

e) Les correctifs de sécurité sont pris en compte au moment de la configuration du système et en fonction des caractéristiques de la machine. Par contre, la prise en compte des derniers correctifs pourraient remettre en cause les tests effectués et nécessiter une nouvelle campagne. C'est pourquoi les derniers correctifs pourraient ne pas être installés.

f) Le mode utilisé est tunnel.

g) L'algorithme utilisé pour le chiffrement des flux est bien AES.

h) Pour la protection en intégrité l'algorithme HMAC-SHA1 est utilisé. L'algorithme HMAC permet effectivement le contrôle d'intégrité des paquets reçus.

i) La passerelle IpSec est un Cisco ASA 5510. Les clients Ipsec compatibles et conseillés sont les clients VPN Cisco.

j) Le group DH actuellement utilisé est DH2. Les PSKs utilisées comportent 13 caractères alphanumériques.

k) La liste des comptes mis en œuvre est sous le contrôle du MAEE contrôlable par un auditeur externe et justifiée par rapport aux besoins.

   I. La taille des clés est de 2048. Par contre, Entrust, notre fournisseur de certificat, ne fait pas parti des prestataires qualifiés RGS

   II. ATOS fournira la liste complète des accès réalisés sur la passerelle.

En ce qui concerne le composant IPsec du VPN, un Pre –SharedKey (PSK) est utilisé :.

1. Cette clé PSK est générée par AWL . Cette clé est utilisé pour crypter tous les échanges entre le postes client VPN et la bulle (fW) dont les échanges, login/password.
2. il y a un PSK car un seul groupe est configuré.(pour le MAEE )
3. cette clé PSK est incluse dans le fichier PCF qui sera transmis au MAEE
4. Les algorithmes utilisés pour la phase ipsec :
   - Encryption : esp aes 128
   - Authentification : esp sha

# 4 Procédure de Configuration, Installation des plates-formes

Une équipe « opérations en salle » est dédiée aux opérations en salle. Ce sont les seules personnes avec le pilotage autorisées à pénétrer dans les salles machines. Cette équipe procède à l'installation des serveurs en appliquant une image paramétrée avec les informations propres au serveur : *IP, nom, partition disque.*

Ces images ont été définies et validées par les équipes techniques : équipes transverses et spécifiques.
Il existe différents profils d'installation suivant les OS et besoins exprimés. Le choix de l'OS et des options est effectué par l'ingénieur système en charge du projet en fonction des besoins et contraintes exprimés.

Dans le cadre de ce projet Evoting, nous installons un système RED HAT. Ensuite des scripts sont appliqués sur les serveurs pour les sécuriser en désactivant les services inutiles suivants :

- NetworkManager
- anacron
- atd
- autofs
- bluetooth
- conman
- cpuspeed
- dnsmasq
- dund
- hidd
- ipmi
- ipvsadm
- irda
- iscsi
- iscsid
- kudzu
- mdmonitor
- mdmpd
- netfs
- nfs
- nfslock
- nscd
- pand
- pcscd
- portmap
- rawdevices
- readahead_later
- rpcgssd
- rpcidmapd
- rpcsvcgssd
- syslog
- wpa_supplicant
- ypbind

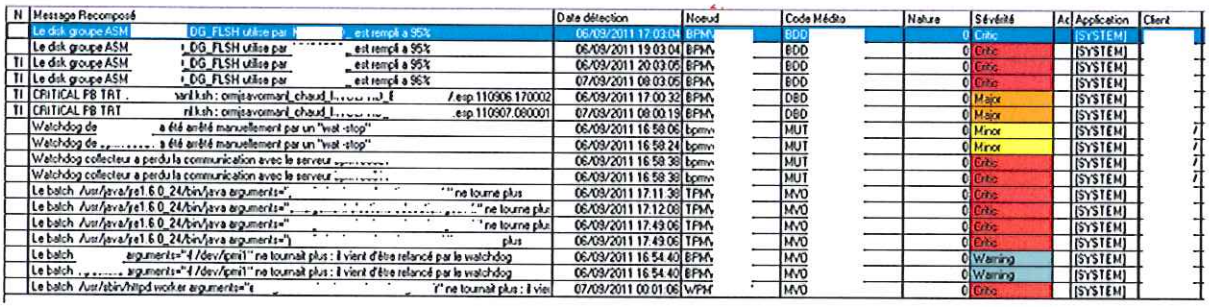
# 5 Stratégie et architecture pour la supervision du système

La supervision du système est effectuée via la plate-forme O.S.C.A.R.E. (Outil de Supervision de Contrôle et d'Administration des Réseaux d'Entreprises).

Il s'agit de la plate forme centrale mutualisée utilisée par les pilotes à Vendôme. Cette plate-forme, présentée avec une interface homme machine conviviale et basée sur le traitement des alarmes remontées par l'ensemble des équipements et applications à superviser, permet de garantir la bonne marche de l'ensemble des services opérés par Atos Worldline.

La performance de cet outil est obtenue par:

- Une optimisation poussée des fonctions de reconnaissance et d'identification des messages
- Une conception modulaire permettant de distribuer les différents composants d'O.S.C.A.R.E. sur plusieurs serveurs afin de répartir la charge.
- La possibilité de mettre en œuvre plusieurs process d'identification de messages (fonctionnalité la plus coûteuse dans le cas de la supervision) sur plusieurs serveurs avec un load-balancing intégré.
- La mise en œuvre d'une base d'historique Microsoft SQL Server simplifiant les extractions de données et permettant de les traiter simplement avec les outils bureautiques classiques.



| N | Message Recomposé | Date détection | Noeud | Code Média | Nature | Sévérité | Ac | Application | Client |
|---|---|---|---|---|---|---|---|---|---|
| | Le disk groupe ASM DG_FLSH utilise par N _ est rempli a 95% | 06/09/2011 17:03:04 | BPMV | BDD | 0 | Critic | | [SYSTEM] | |
| | Le disk groupe ASM _DG_FLSH utilise par _ est rempli a 95% | 06/09/2011 19:03:04 | BPMV | BDD | 0 | Critic | | [SYSTEM] | |
| TI | Le disk groupe ASM _DG_FLSH utilise par _ est rempli a 95% | 06/09/2011 20:03:05 | BPMV | BDD | 0 | Critic | | [SYSTEM] | |
| TI | Le disk groupe ASM _DG_FLSH utilise par _ est rempli a 96% | 07/09/2011 08:03:05 | BPMV | BDD | 0 | Critic | | [SYSTEM] | |
| TI | CRITICAL PB TRT . xarl.ksh: omjsavomarl_chaud_l... /.esp 110906.170002 | 06/09/2011 17:00:32 | BPMV | DBD | 0 | Major | | [SYSTEM] | |
| TI | CRITICAL PB TRT rll.ksh: omjsavomarl_chaud_l... .esp 110907.080001 | 07/09/2011 08:00:19 | BPMV | DBD | 0 | Major | | [SYSTEM] | |
| | Watchdog de a été arrêté manuellement par un "wat -stop" | 06/09/2011 16:58:06 | bpmv | MUT | 0 | Minor | | [SYSTEM] | |
| | Watchdog de a été arrêté manuellement par un "wat -stop" | 06/09/2011 16:58:24 | bpmv | MUT | 0 | Minor | | [SYSTEM] | |
| | Watchdog collecteur a perdu la communication avec le serveur | 06/09/2011 16:58:38 | bpmv | MUT | 0 | Critic | | [SYSTEM] | |
| | Watchdog collecteur a perdu la communication avec le serveur | 06/09/2011 16:58:38 | bpmv | MUT | 0 | Critic | | [SYSTEM] | |
| | Le batch /usr/java/jre1.6.0_24/bin/java arguments=" " ne tourne plus | 06/09/2011 17:11:38 | TPMV | MVO | 0 | Critic | | [SYSTEM] | |
| | Le batch /usr/java/jre1.6.0_24/bin/java arguments=" " ne tourne plus | 06/09/2011 17:12:08 | TPMV | MVO | 0 | Critic | | [SYSTEM] | |
| | Le batch /usr/java/jre1.6.0_24/bin/java arguments=" " ne tourne plus | 06/09/2011 17:49:06 | TPMV | MVO | 0 | Critic | | [SYSTEM] | |
| | Le batch /usr/java/jre1.6.0_24/bin/java arguments=") plus | 06/09/2011 17:49:06 | TPMV | MVO | 0 | Critic | | [SYSTEM] | |
| | Le batch arguments="-f /dev/fpmi1" ne tournait plus : il vient d'être relancé par le watchdog | 06/09/2011 16:54:40 | BPMV | MVO | 0 | Warning | | [SYSTEM] | |
| | Le batch arguments="-f /dev/fpmi1" ne tournait plus : il vient d'être relancé par le watchdog | 06/09/2011 16:54:40 | BPMV | MVO | 0 | Warning | | [SYSTEM] | |
| | Le batch /usr/sbin/httpd.worker arguments="-t -f" ne tournait plus : il vien | 07/09/2011 00:01:06 | WPM | MVO | 0 | Critic | | [SYSTEM] | |

La gestion des services et le suivi de la production est effectué via le portail d'information : **ISMP**

La surveillance est effectuée à deux niveaux :

- D'une part la présence de l'infrastructure : on vérifie de manière standard la présence des machines, du réseau, des process de base (apache, Tomcat, BDD, ...)
- D'autre la réponse de l'application aux sollicitations d'un robot : la sonde applicative Watchservice est paramétrée pour surveiller à intervalle régulier les URL suivantes :

| Plate forme | URL à surveiller | Résultat attendu |
|---|---|---|
| | | |
| | | |

***Ce tableau sera complété dans une prochaine version, préalablement à la mise en place des surveillances***

# 6 Stratégie de sécurité du système

## 6.1 Procédure de durcissement des plates-formes

La protection des diverses plates-formes de services hébergées par Atos Worldline est assurée par des routeurs frontaux dont la charge principale est d'assurer le cheminement correct des paquets entre les équipements réseaux et les différents services hébergés.

Ces routeurs assurent de plus un premier niveau de filtrage, qui empêche les connexions sur les ports privilégiés non explicitement spécifiés (***par défaut, tous les ports sont fermés, seuls les ports nécessaires sont explicitement ouverts***). Les routeurs frontaux effectuent aussi un filtrage des paquets incorrectement formatés (trop longs), les options IP non autorisées (source-routing), les broadcast, certains types de paquets ICMP, etc.

Ce premier niveau de filtrage permet d'éliminer des attaques grossières (connexions telnet ou NetBIOS) et des attaques de déni de service (broadcast ICMP). Il permet de plus de bannir temporairement des adresses IP à l'activité douteuse.

La politique standard de sécurité d'Atos Worldline appliquée aux machines consiste, entre autres, à minimiser les services accessibles, et ce quelle que soit leur position dans le réseau (DMZ ou interne). Les services non indispensables ne sont pas disponibles (chargen, echo, ...), et la plupart des démons présents par défaut sont désactivés (certains RPC, lpd...).

De plus, les services accessibles au grand public (HTTP ...) utilisent des adresses IP spécifiques virtuelles (système d'adressage virtuel réseau pour les adresses externes des services - fonction NAT), dans un souci de sécurité (filtrage par service), et de souplesse d'administration (bascules des services plus simples)

La sécurité est aussi assurée logiquement :

- par l'architecture de la plateforme, protégée des intrusions extérieures par un double rideau de pare-feux, de technologies hétérogènes afin d'en augmenter la résistance,
- par les limitations d'accès aux serveurs (politique de sécurité du centre serveur, avec accès distant par bastion aux serveurs et utilisation durant la période de vote d'une authentification forte à l'aide de token).
- par un scellé logique des applications avant la période de vote afin d'en garantir la non modification jusqu'à l'extraction des données du vote. Ce scellement logique consiste à signer numériquement l'application afin de vérifier qu'elle demeure inaltérée durant l'élection. La

signature numérique est implémentée dans le code audité par les auditeurs. Cela permet de garantir que le code ne subit aucun modification après le processus d'audit dus système.

- par le logiciel lui-même, qui garantit la confidentialité des données manipulées (chiffrement).

## 6.2 Sécurité

Le centre de production Atos Worldline de Vendôme est opérationnel depuis 28 ans avec une infrastructure et une sécurité éprouvées et sans cesse en amélioration.
Le bâtiment est spécialisé dans l'hébergement de moyens informatiques. Seul le personnel nécessaire à la supervision des applications et à l'exécution des taches sur sites, y est attaché. Ainsi, pendant les heures de bureaux, 25 personnes travaillent sur le site, en dehors de ces heures, au moins 4 personnes sont présentes. Le centre est opérationnel 24/24 heures, 7/7 jours, 365 jours par an.
L'implantation spécifique de ce centre permet de se prémunir des risques :

- Industriels et liés au vandalisme, puisque le centre a été construit loin des zones d'activités et d'habitations.
- Météorologiques, le centre se trouve dans une zone non inondable et placé bien au-dessus des niveaux hydrostatiques.
- Aériens, il n'y a pas de couloir aérien dans cette zone.
- Sismiques, cette zone n'est pas à risque sismique.

Le site de Vendôme regroupe les plateformes de paiement opérées par Atos Worldline, et fait donc l'objet d'un très haut niveau de sécurité physique :

- Un contrôle d'accès très exigeant.
- Une sécurité périmétrique des bâtiments très élaborée
- Une vidéosurveillance
- Un automatisme des remontées d'alarmes

A l'entrée du site, le personnel et les visiteurs font l'objet d'un premier filtrage, en effet, seules les personnes autorisées et les visiteurs attendus pourront entrer dans l'enceinte du site. L'accès aux bâtiments puis aux locaux n'est accordé qu'à un nombre restreint de collaborateurs d'Atos Worldline et aux visiteurs attendus. La séparation des bâtiments en zones permet de limiter le déplacement des individus aux seuls endroits nécessaires à leur activité.

Plus un local est sensible, plus il y a de contrôles à franchir pour y parvenir :

- aux grilles d'entrée du site,
- à l'entrée du bâtiment,
- à l'accueil des visiteurs

- à l'entrée des salles informatiques,
- à l'entrée des salles et espaces dédiés sécurisés dans les salles informatiques.
- A l'entrée des locaux techniques

Des mesures complémentaires s'ajoutent à ces contrôles :

- exigence de présentation d'une pièce d'identité pour les visiteurs,
- surveillance vidéo avec conservation des traces selon la réglementation pour tous les accès sensibles,
- contrôles visuels.
- L'accès à la zone de haute sécurité nécessite l'authentification obligatoire de deux personnes autorisées (dual control) via un système d'authentification forte intégrant de la biométrie

Par ailleurs, tout le périmètre du bâtiment principal est équipé entre autres, de détection « laser », afin de prévenir toute tentative d'intrusion. Le tout est doublé d'une surveillance vidéo pour lever les doutes et conserver des traces.

L'ensemble des plates formes de vote du MAEE bénéficient de la haute disponibilité du centre en matière énergétique, climatique et sécurité incendie.
Ces plates formes bénéficient d'un niveau complémentaire de sécurité physique puisque tous les serveurs sont installés dans des baies sécurisées et scellées préalablement au vote.

### 6.2.1 *Sécurité logique*

| **Durcissement des serveurs** | | **SYSTEM** |
|---|---|---|
| Protection antivirale à jour. | Non | Aucun antivirus actuellement installé sur les serveurs Linux |
| Désactivation des interfaces inutilisées. | Oui | Pas de cable. |
| Paramétrage du BIOS sécurisé. | Non | L'accès en salle est nécessaire pour accéder au BIOS. L'accès à la salle machine est sécurisé |
| Dispositif de contrôle d'intégrité des fichiers et des programmes. | Oui | AIDE |
| Sécurité physique assurée (baie fermée à clé ou coffre). | Oui | Cage serveur. |
| Ouverture de session sécurisée. | Oui | ISAAC3 |
| Derniers correctifs de sécurité pour leur système d'exploitation ainsi que les applications qui y sont installées. | Non | Mise à jour avant le vote des logiciels les + impactant (Apache, Tomcat, Java, …). Pas de mise à jour sur BDD car |

| | | |
|---|---|---|
| | | impact les versions Oracle/ASM |
| Liste des comptes mis en œuvre sous le contrôle du MAEE contrôlable par un auditeur externe et justifiée par rapport aux besoins. | Oui | Compte standard pour toutes les installations. |
| | | |
| Les personnels en charge de la configuration, de l'exploitation et de l'administration des serveurs ne doivent disposer d'aucun accès sur les pare-feux et sur les équipements réseaux constituant la machine de vote. | Oui | |
| | | |
| Les guides de durcissement publics doivent être utilisés : | | |
| Pour les serveurs Linux : | | |
| • Guide to the Secure Configuration of Red Hat Enterprise Linux 5 - Revision 4.1 - February 28, 2011 (auteur : National Security Agency) | Non | Ce sont des installations standards d'Atos Wordline qui sont mises en place. Ces versions sont validées par les équipes techniques transverses (Technical Services)<br>L'ingénieur Système en charge de l'installation désactive par script un ensemble de service / package inutilisés.<br>Pour la partie BDD, les pré-requis Oracle sont ajoutés.<br><br>Versions utilisées : « Red Hat Enterprise Linux Server release 5.6 (Tikanga) Kernel : 2.6.18-274.el5 » sur les Fronts et Middle, « 5.4 (Tikanga) Kernel : 2.6.18-164.el5 » sur les BDD |
| • Red Hat Enterprise Linux Benchmark, v1.1.2 (2009/06/17) (auteur : CIS - the Center of Internet Security) | Non | |
| • Linux Security Checklist SANS Institute - May 5th, 2011 (auteur : SANS Institute) | Non | |
| Pour les serveurs Windows : | | |
| • Windows Server® 2008 Security Guide - Version 3.0 February 2009 (auteur : Microsoft) | N/A | |
| • Security Configuration Benchmark For Microsoft Windows Server 2008 - Version 1.1.0 July 30th, 2010 (auteur : CIS - The Center for Internet Security) | N/A | |
| • Security Configuration Benchmark For Microsoft Windows 7 - Version 1.1.0 July 30th 2010 (auteur : CIS - The Center for | N/A | |

| | | |
|---|---|---|
| Internet Security) | | |
| Pour le serveur Apache : | | |
| • Security Configuration Benchmark For Apache HTTP Server 2.2, Version 3.0.0 de May 18th, 2010, The Center for Internet Security | N/A | Nginx est utilisé en Front à la place d'Apache.<br>Version « nginx-1.0.9-3.rhel5.x86_64» |
| | | |
| **Administration des serveurs.** | | |
| L'administration des serveurs doit être effectuée par du personnel habilité au moyen de comptes nominatifs permettant d'assurer la traçabilité des actions. Ces actions doivent pouvoir être contrôlées par un auditeur externe ou par un membre du BVE. | Pas de compte nominatif mais traçabilité des accès. | ISAAC3 |
| | | |
| **Conformité des serveurs** | | |
| Les versions des systèmes d'exploitation utilisés doivent disposer d'un certificat CC. | | |
| Dans le cas de l'utilisation de la librairie OpenSSL, une version évaluée FIPS 140-2 doit être utilisée. Le serveur sur lequel la librairie est installée doit être conforme aux exigences sur le durcissement. | Non | Le changement de librairie, sous réserve de validation par les équipes transverses, nécessiterait la recompilation de nombreux composant l'utilisant.<br>La version Open SSL utilisée est « OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008 ». La dernière disponible pour RedHat 5.6 est la « 0.9.8o » |
| La taille des clés et le choix des algorithmes doivent être conformes au RGS : RSA 2048/4096, DH Groupe 14 ou plus, AES 128/256, SHA 256. | | Voir document Cryptographic Key Management |
| La génération des clés doit être conforme au RGS. | | Voir document Cryptographic Key Management |
| | | |
| Durcissement des équipements réseaux | | RESEAU |
| Les équipements réseaux mis en œuvre doivent comprendre les éléments suivants : | | |
| • Désactivation des interfaces inutilisées. | Oui | |

| | | |
|---|---|---|
| • Paramétrage du BIOS sécurisé. | N/A | |
| • Sécurité physique assurée (baie fermée à clé ou coffre). | Oui | Baies scellés |
| • Ouverture de session sécurisée. | | ISAAC2 |
| • Derniers correctifs de sécurité pour leur système d'exploitation. | Non | Les versions d'OS à utiliser sur ces composants sont définis par les équipes transverses d'AWL. Seuls les correctifs jugés nécessaires et validés par ces équipes sont installés |
| • Liste des comptes mis en œuvre sous le contrôle du MAEE contrôlable par un auditeur externe et justifiée par rapport aux besoins. | Oui | Compte standard. |
| | | |
| Les guides de durcissement publics doivent être utilisés : | | |
| - Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology, February 2007, NIST Special Publication 800-94 | Non | Ce sont les procédures standards AWL qui sont appliqués, |
| - Network Intrusion Detection/Prevention Systems & Content Scanning Appliances, Version 8, Release 1, Supplement of Network Infrastructure STIG, V8R1, 24 March 2010, Developed by DISA for the DoD. | Non | |
| - Cisco IOS Switch Security Configuration Guide, Switch Security Guidance Activity of the Systems and Network Attack Center (SNAC), 21 june 2004, Version 1.0. | Non | |
| - Router Security Configuration Guide, Principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco Systems routers Router Security Guidance Activity of the System and Network Attack Center (SNAC), December 15, 2005, Version 1.1c | Non | |
| Administration des équipements réseaux. | | RESEAUX |
| L'administration des équipements réseaux doit être effectuée par du personnel habilité au moyen de comptes nominatifs permettant d'assurer la traçabilité des actions. Ces actions doivent pouvoir être contrôlées par un auditeur externe ou par un membre du BVE. | Oui | |

| **Conformité des équipements réseaux** | | |
|---|---|---|
| Les équipements réseaux utilisés doivent disposer d'un certificat CC. | Non | Tout comme pour le cote de 2009, ce sont des équipements standard AWL, validés par les équipes techniques réseau qui sont utilisés |
| La taille des clés et le choix des algorithmes doivent être conformes au RGS : RSA 2048/4096, DH Groupe 14 ou plus, AES 128/256, SHA 256. | Non | AES / SHA / DH Groupe 2 |
| La génération des clés doit être conforme au RGS. | Non | |
| **Filtrage des flux** | | |
| Aucun serveur ne doit être directement relié à Internet. Chaque liaison entre un serveur et Internet doit être filtrée par un pare-feu. | Oui | |
| Le pare-feu doit permettre de filtrer les types de flux entrants et sortants de la machine de vote, afin de n'autoriser que les types de flux nécessaires au fonctionnement de la machine de vote. | Oui | |
| Le pare-feu doit permettre le blocage de tous les types de flux non autorisés. | Oui | |
| Le pare-feu doit permettre la journalisation des tentatives de connexion au moyen de flux non autorisés à la machine de vote. Ces journaux doivent pouvoir être transmis au serveur de centralisation des traces. | Oui | Logs conservées sur syslog |
| La configuration du pare-feu doit être effectuée par du personnel habilité et validée par le MAEE. | Oui | |
| La configuration du pare-feu doit pouvoir être contrôlée par un auditeur externe ou par un membre du BVE. | Oui | Fourniture de la configuration actuelle du firewall. |
| Le fichier contenant les règles de filtrage doit pouvoir être extrait et fourni au BVE lors du scellement du système. | Oui | |
| Une fois la configuration du pare-feu validée, toute modification de cette configuration ne peut être effectuée sans l'accord du BVE. | Oui | |
| La configuration du pare-feu doit comprendre : | | |
| • La description des flux : équipement concerné, initiateur(s), destinataire(s), | Oui | |
| • Le protocole ou le numéro de port utilisé, | Oui | |
| • Le caractère « accepté » ou « refusé », | Oui | |
| Tous les accès et les actions effectués sur le pare-feu par le personnel en charge de sa | Oui | Demandes effectuées suite à |

| | | |
|---|---|---|
| maintenance et de son administration doivent être tracés depuis le scellement jusqu'à la fin de la période de vote. L'ensemble des traces doit être remis au BVE après la fermeture du scrutin. | | une demande de la BU. |
| Le pare-feu doit contenir un module de protection contre les attaques en déni de service. | Non | Pas de protection tout comme en 2009 |
| Le pare-feu doit permettre de n'autoriser les paquets faisant partie d'une connexion déjà établie (mode « stateful »). | Oui | |
| Les personnels en charge de la configuration, de l'exploitation et de l'administration des pare-feux ne doivent disposer d'aucun accès sur les serveurs constituant la machine de vote. | Non | La partie réseau des serveurs est administrée par l'équipe système. Pour les équipements réseau il s'agit des équipes réseau. En Standard AWL, l'accès pour test réseau est donné aux équipes réseau, sans droits system sur la machine. |
| La transmission d'informations de routage entre les équipements réseaux doit être réalisée après authentification mutuelle entre ces équipements. | Oui | Routage static |
| Une organisation permettant d'assurer le back-up des administrateurs réseaux, doit être mise en place. | Oui | |
| En cas de défaillance d'un pare-feu : | | |
| • Une alarme doit être générée. | Oui | |
| • L'équipement ne doit pas avoir un comportement remettant en cause les règles de filtrage. | Oui | |
| • La configuration des pare-feux doit pouvoir être accessible. | Oui | Sur CVS |
| • Les traces générées par le pare-feu doivent permettre l'analyse de l'origine de la défaillance. | Oui | Logs sur Syslog |
| | | |
| **Cloisonnement des flux** | | |
| La machine de vote doit être positionnée dans un sous réseau dédié cloisonné logiquement au sein du réseau d'ATOS. | Oui | |
| La configuration des équipements réseaux mettant en œuvre le cloisonnement doit être effectuée par du personnel habilité et validée par le MAEE. | Oui | |
| La configuration des équipements réseaux mettant en œuvre le cloisonnement doit doit pouvoir être contrôlée par un auditeur externe ou par un membre du BVE. | Oui | |
| Le fichier contenant les règles de cloisonnement doit pouvoir être extrait et fourni | Oui | |

| | | |
|---|---|---|
| au BVE lors du scellement du système. | | |
| Une fois la configuration des équipements réseaux mettant en œuvre le cloisonnement validée, toute modification de cette configuration ne peut être effectuée sans l'accord du BVE. | Oui | |
| Tous les accès et les actions effectués sur les équipements réseaux mettant en œuvre le cloisonnement par le personnel en charge de leur maintenance et de leur administration doivent être tracés depuis le scellement jusqu'à la fin de la période de vote. L'ensemble des traces doit être remis au BVE après la fermeture du scrutin. | Oui | Via CVS |
| Les personnels en charge de la configuration, de l'exploitation et de l'administration des équipements réseaux mettant en œuvre le cloisonnement ne doivent disposer d'aucun accès sur les serveurs constituant la machine de vote. | Non | La partie réseau des serveurs est administrée par l'équipe système. Pour les équipements réseau il s'agit des équipes réseau. En Standard AWL, l'accès pour test réseau est donné aux équipes réseau, sans droits system sur la machine. |
| En cas de défaillance d'un des équipements réseaux mettant en œuvre le cloisonnement : | | |
| • Une alarme doit être générée. | Oui | |
| • L'équipement ne doit pas avoir un comportement remettant en cause les règles de filtrage. | Oui | |
| • La configuration de l'équipement doit pouvoir être accessible. | Oui | Sur CVS |
| • Les traces générées par l'équipement doivent permettre l'analyse de l'origine de la défaillance. | Oui | Logs sur Syslog |
| | | |
| **Paramétrage des équipements réseaux** | | **RESEAU** |
| Les services à désactiver sont les suivants : | | |
| • Activation de DHCP SNOOPING | Non | Si pas de DHCP dans la bulle, peux être activé sans impact et aucun port à passer en trust |
| • Activation de DYNAMIC ARP INSPECTION | Non | - Dépend de DHCP snooping<br>- Quels sont les ports à passer en trust ?<br>A l'installation d'une machine, on le passe en trust et les autres restent untrust ? |
| | | |

| Les services à désactiver sont les suivants | | |
|---|---|---|
| • Désactivation de STP | Non | La désactivation aura un impact sur la prod. |
| • Désactivation de UDLD | Oui | |
| • Désactivation de VTP | Oui | Non Applicable car il ne s'applique pas pour le matériel utilisé de la bulle AFE |
| • Désactivation des COMMUNITY STRINGS par défaut | Oui | |
| • Désactivation des messages ICMP pour les interfaces | Non | - Problème pour la supervision<br>- Possibilité de filtrage pour ne laisser passer que les ICMP echo Reply et echo Request. |
| • Désactivation des services TCP et UDP small servers | Non | Non Applicable car il ne s'applique pas pour le matériel utilisé de la bulle AFE |
| • Désactivation du mécanisme FLOW CONTROL | Oui | |
| • Désactivation du protocole MOP | Non | Non Applicable car il ne s'applique pas pour le matériel utilisé de la bulle AFE |
| • Désactivation du serveur http (si pas d'utilisation de l'interface web) | Oui | |
| • Désactivation du service BOOTP SERVER | Oui | Non Activé |
| • Désactivation du service CDP | Oui | Non Applicable car il ne s'applique pas pour le matériel utilisé de la bulle AFE |
| • Désactivation du service CONFIGURATION AUTOLOADING | Oui | |
| • Désactivation du service DTP | Oui | Non Applicable car il ne s'applique pas pour le matériel utilisé de la bulle AFE |
| • Désactivation du service FINGER | Oui | Non Applicable car il ne s'applique pas pour le matériel utilisé de la bulle AFE |
| • Désactivation du service NTP ou contrôle des accès à ce service | Oui | Filtré par Firewall |
| • Désactivation du service PAD | Oui | Non Applicable car il ne s'applique pas pour le matériel utilisé de la bulle AFE |
| • Désactivation du service TFTP et activation seulement lors de l'usage | Non | Utilisé pour les sauvegardes de |

| | | |
|---|---|---|
| | | configuration |
| • | | |
| • Les mesures de sécurité à paramétrer sont les suivantes | | |
| • Activation du chiffrement des mots de passe (ENABLE-SECRET) | Oui | |
| • Configuration explicite du DNS ou désactivation du DNS LOOKUP | Oui | |
| • Dédier un port physique à l'administration out-band | Oui | |
| • Mise en place d'un mot de passe pour l'ouverture d'une session console | Oui | |
| • Pas d'utilisation du VLAN 1 pour l'administration | Oui | |
| • Utilisation du mécanisme PORT SECURITY | Non | Comme en 2009. L'upgrade d'infra demandé cet été porte sur les serveurs, pas sur les équipements réseaux. |
| • Utilisation du service SSH au lieu de TELNET | Oui | |
| | | |
| Les messages interdits sont les suivants : | | |
| - Interdiction des BROADCAST internes | Oui | |
| - Interdiction des masques ICMP | Non | Comme en 2009. L'upgrade d'infra demandé cet été porte sur les serveurs, pas sur les équipements réseaux. |
| - Interdiction des notifications en cas d'adresse IP incorrecte | Oui | |
| - Interdiction des redirections ICMP | Non | Comme en 2009. L'upgrade d'infra demandé cet été porte sur les serveurs, pas sur les équipements réseaux. |
| - Interdiction du relais de trames ARP | Non | |
| - Interdiction du routage par la source | Non | |
| | | |
| **Disponibilité de service** | | |
| L'ensemble des équipements doit être dimensionné pour supporter la charge maximale prévue. Les justifications des choix effectués doivent être fournies par les maîtres d'œuvre. | ??? | A voir lors des tests de performances |
| La chaîne de traitement des bulletins de vote doit être redondée. | Oui | |
| Les fonctions de sécurité réseau doivent être mises en œuvre sur les deux chaînes de | Oui | |

| | | |
|---|---|---|
| manière à éviter les points de panne unique. | | |
| Toute défaillance d'un équipement mettant en œuvre les fonctions de sécurité réseau (filtrage, cloisonnement) doit entraîner le basculement de ces fonctions de sécurité réseau sur la seconde chaîne. | Oui | |
| | | |
| **Surveillance** | | |
| L'ensemble des équipements doit être sous surveillance 24/24. | Oui durant la période de vote | |
| Tout événement de sécurité (cf. tableaux suivants dans le paragraphe « gestion des traces ») doit faire l'objet d'une alarme. | Non | Voir paragraphe « gestion des traces » |
| | | |
| **Gestion des traces** | | |
| La synchronisation horaire des équipements réseaux doit être assurée. | Oui | |
| ATOS doit mettre en place un dispositif de centralisation des traces en provenance de l'ensemble des équipements constituant la machine de vote (équipements réseaux / serveurs). | Non | Pas de serveur de centralisation des logs system et applicatif. |
| Les traces applicatives doivent également être centralisées sur ce dispositif. | Non | Pas de serveur de centralisation des logs system et applicatif. |
| Les événements de sécurité suivants doivent être collectés | | Pas de serveur de centralisation des logs system et applicatif |
| Les traces doivent contenir les informations suivantes : | | |
| - La date et l'heure de l'événement. | | |
| - L'identification de la machine ou de l'application de provenance de l'événement. | | |
| - L'adresse source et destination du flux. | | |
| - Le port source et destination du flux. | | |

*Table 6-1 Infrastructure – Sécurité Logique*

### 6.2.2 *Mesures de sécurité physique*

| | | |
|---|---|---|
| **Contrôle d'accès** | | |
| Les zones hébergeant les composants de la machine de vote doivent être physiquement protégées. | Oui | |
| L'accès doit être strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. Toute détection d'accès physique doit être remontée au BVE. | Oui | |
| | | |
| **Services essentiels** | | |
| Les serveurs composant la machine de vote doivent être arrêtés électriquement lorsque non utilisés. | Oui | |
| Les locaux hébergeant le système de vote à Vendôme doivent être climatisés. | Oui | |
| Les caractéristiques des équipements d'alimentation électrique et de climatisation doivent permettre de respecter les conditions d'usage des composants de la machine de vote telles que fixées par leurs fournisseurs. | Oui | |
| | | |
| **Marquage des matériels** | | |
| Les matériels utilisés doivent comporter un marquage physique les identifiant. | Oui | |
| Le marquage des matériels doit permettre d'identifier la fonction du matériel dans la machine de vote. | Oui | |
| | | |
| **Inventaire des matériels** | | |
| Un inventaire de l'ensemble des matériels utilisés dans le système de vote doit être maintenu par ATOS. | Oui | |
| Cet inventaire doit intégrer les marquages et intégrer les numéros de série des équipements. | Oui | |
| | | |
| **Intégration des matériels dans la machine de vote** | | |
| Toute intégration d'un matériel dans la machine de vote doit être signifiée au MAEE. | Oui | |
| Toutes les opérations effectuées entre la réception d'un matériel et son intégration dans la machine de vote doit être tracée. | Oui | |
| L'ensemble de ces traces doit être communiqué au MAEE. | Oui | |
| | | |

| | | |
|---|---|---|
| **Maintenance des matériels** | | |
| Les opérations de maintenance sur les matériels intégrés à la machine de vote doivent être tracées. | Oui | |
| L'ensemble de ces traces doit être communiqué au MAEE. | Oui | |
| | | |
| **Médias amovibles et terminaux mobiles** | | |
| Les médias amovibles et les terminaux mobiles utilisés dans le cadre des opérations de vote doivent être dédiés à ces opérations. | Oui | CD de scellement |
| Une table contenant l'ensemble des numéros de série des médias amovibles et des terminaux mobiles doit être maintenue par ATOS. | Oui | CD de scellement |
| Avant toute écriture de données sur un média amovible, un formatage du média doit être effectué. | Oui | CD de scellement |
| A l'issue de l'écriture de données, le média amovible doit être protégé en écriture. | Oui | CD de scellement |
| Les médias amovibles de type CD-ROM ou DVD doivent être non réinscriptibles. | Oui | CD de scellement |
| Les médias amovibles et les terminaux mobiles utilisés dans le cadre des opérations de vote doivent disposer d'un marquage physique. | Oui | |
| Les médias amovibles et les terminaux mobiles doivent être conservés dans un coffre-fort dédié au vote lorsqu'ils ne sont pas utilisés. | Oui | Coffre Vendome. |
| L'accès doit être strictement limité aux seules personnes autorisées à ces postes et supports et la traçabilité des accès doit être assurée. | Oui | |
| | | |
| **Matériel dédié** | | |
| Le matériel utilisé doit être dédié au vote et à chaque tour de scrutin. | Oui | Attention au réacheminement |
| | | |
| **Secours** | | |
| Chaque matériel utilisé dans le cadre des opérations de vote doit disposer d'un secours ayant la même configuration que le matériel nominal. | Oui | |
| Le matériel de secours doit être conservé et manipulé dans les mêmes conditions que le matériel nominal. | Oui | |
| | | |
| **Transfert du matériel** | | |
| Le transfert du matériel (terminaux mobiles, supports de données) entre le MAEE et le site d'hébergement à Vendôme doit être effectué par du personnel de confiance. | Oui | Récupération par MAEE. |
| Le transfert du matériel (terminaux mobiles, supports de données) entre le site de SCYTL et le MAEE ou entre le site de SCYTL et le site d'hébergement à Vendôme doit être effectué par du personnel de confiance. | N/A | Pas de transfert AWL-SCYTL. |
| | | |
| **Sauvegarde de la machine de vote** | | |
| Les composants de la machine de vote doivent permettre la sauvegarde de ses composants logiciels et matériels. | | |
| En cas de perte d'un composant, la restauration des données doit | | |

| | | |
|---|---|---|
| être effectuée conformément aux besoins de continuité du service. | | |
| | | |
| **Scellement physique** | | |
| Les équipements utilisés dans la machine de vote doivent faire l'objet d'un scellement physique garantissant que toute manipulation de ces composants est détectée. | Oui | |
| Les recommandations décrites dans le guide de l'ANSSI doivent être respectées. | Non | A vérifier. |

*Table 6-2 Infrastructure – Sécurité Physique*