www.cnrs.fr

GESLAB
GESTION FINANCIÈRE

PRE-REQUIS

Référence	GESLAB_Pre-Requis_v2.0.doc
Date de la dernière mise à jour	12/01/2016
Statut	*Validé*
Rédigé par	*DSI*
Objet	*Pré-Requis*

Table de mise à jour du document		
Version	**Date**	**Objet de la mise à jour**
1.0	13/01/2012	Version initiale
1.1	23/01/2012	Ajout des caractéristiques matérielles
1.2	10/02/2012	Précision de la configuration réseau
1.3	20/03/2012	Ajout des ouvertures https
1.4	10/05/2012	Corrections concernant les ouvertures https
1.5	21/05/2012	Compléments ouverture réseau
1.6	05/09/2012	Changement logo GESLAB
1.7	21/12/2012	Aide sur les déconnexions intempestives
1.8	02/01/2013	Ajout d'un cas de déconnexion intempestive
1.9	18/01/2013	Complément sur les déconnexions intempestives
2.0	08/01/2016	Mise à jour des informations de configuration mini

SOMMAIRE

1 CLIENT LOURD 4

1.1 MATERIEL 4
1.2 CONFIGURATION RESEAU 4
1.3 OS 4
1.4 PROBLEMES DE DECONNEXIONS INTEMPESTIVES 6
1.4.1 PARE-FEU/IDS NETASQ 6
1.4.2 PARE-FEU CISCO 6
1.4.3 PARE-FEU FORTINET 7
1.4.4 PARE-FEU CHECKPOINT 7
1.4.5 PARE-FEU « JUNIPER » 8
1.4.6 PARE-FEU KASPERSKY AU NIVEAU DU POSTE UTILISATEUR 8
1.4.7 REGLAGE AU NIVEAU DU NAT 8

2 CLIENT WEB 9

2.1 JAVA 9
2.2 NAVIGATEURS 9

1 CLIENT LOURD

1.1 MATERIEL

RAM : 1 Go
CPU : minimum Pentium 4, conseillé Core 2
Espace disque disponible : 410 Mo

1.2 CONFIGURATION RESEAU

Port 1630 ouvert en TCP en sortie vers l'adresse ip : 193.49.3.101

Port 443 ouvert en sortie vers les adresses ip :

- geslab.dsi.cnrs.fr 193.55.86.39
- janus.dsi.cnrs.fr 193.55.86.7
- wayf.dsi.cnrs.fr 193.55.86.40

Une évolution de GESLAB va permettre de renvoyer les flux vers un éventuel serveur proxy http. La mise en place de cette évolution n'est pas encore planifiée.

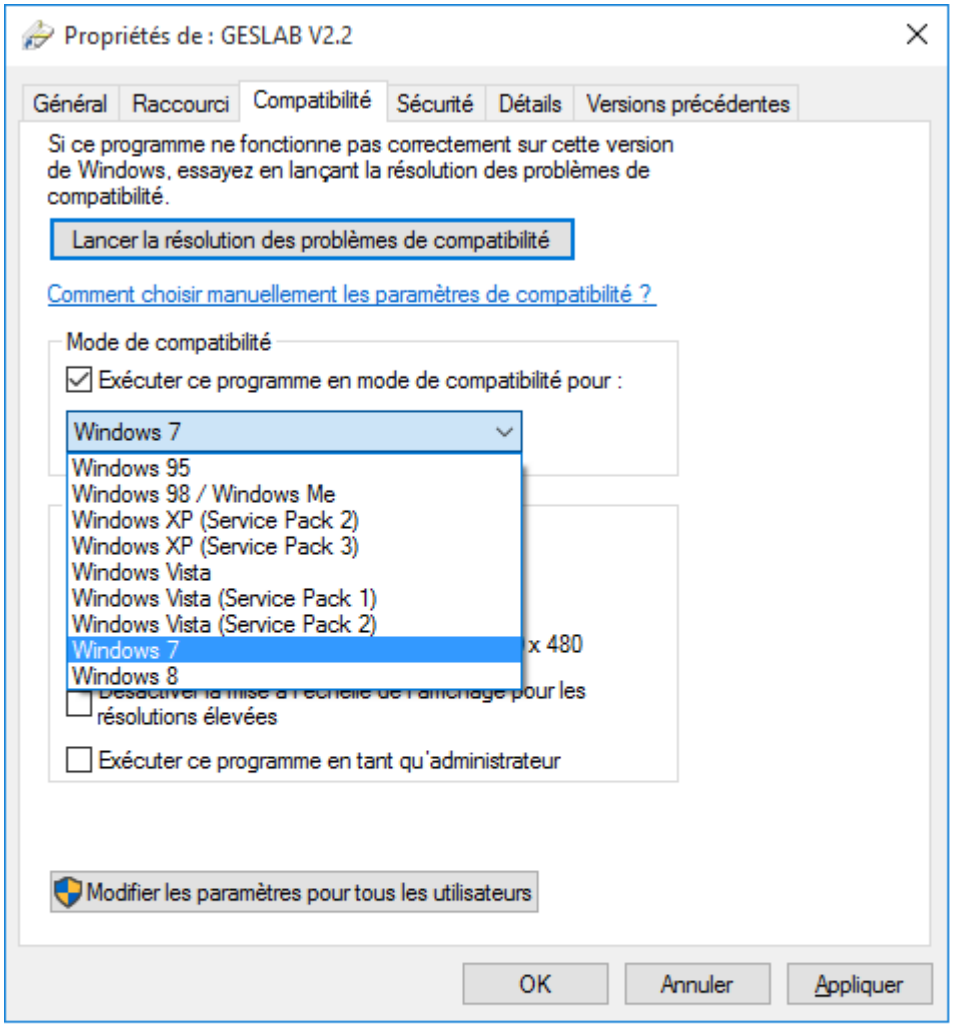
1.3 OS

Postes Microsoft :

- Windows XP SP3
- Windows Vista SP2
- Windows Seven SP1

- Windows 8 (avec modification ci-dessous)
- Windows 10 (avec modification ci-dessous)

Si l'installation est faite par l'installeur, omnis s'ouvre en mode « tablette » et les menus sont invisibles.
Pour éviter cela il faut faire une petite manipulation à réaliser sur le raccourci de lancement de GESLAB.



Postes MAC :

- De MAC OSX 10.6 (Snow Leopard) à MAC OSX 10.10 (yosemite)

Serveur Microsoft :

- Windows Terminal Server 2008
- Citrix XenDesktop 5

1.4 PROBLEMES DE DECONNEXIONS INTEMPESTIVES

Plusieurs gestionnaires de laboratoires se plaignent de déconnexions intempestives du client lourd GESLAB au bout d'un temps relativement court (en tout cas bien inférieur aux 8 heures configurées en central).

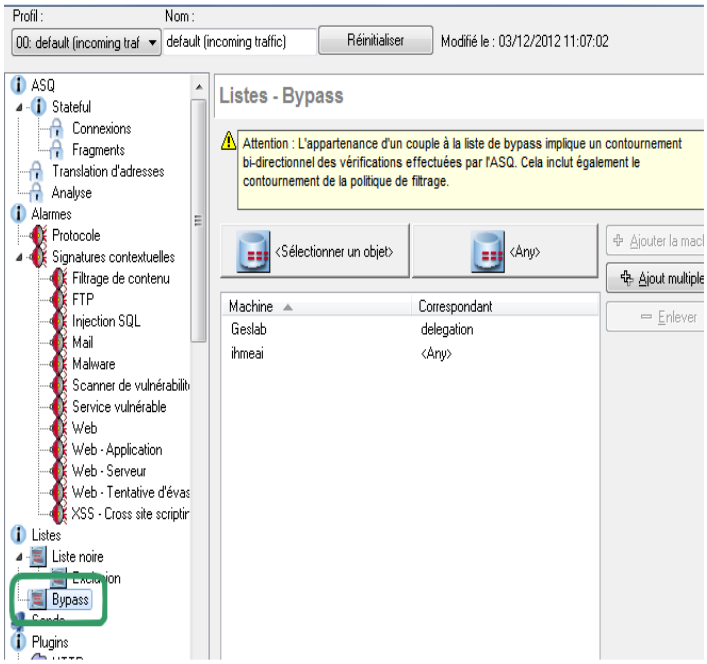
Explications sur ce problème données par la DELEGATION ALSACE à ses labos

Les déconnexions intempestives du client lourd GESLAB rencontrées par certain(e)s gestionnaires sont potentiellement dues aux équipements de détection et de prévention d'intrusions (IDS).
Les IDS gèrent des délais d'expiration de connexions TCP, une application connectée sans échange avec le client peut être déconnectée intempestivement par le pare-feu.
Solutions : augmenter globalement le time-out de déconnexion TCP, ou rajouter le serveur GESLAB (193.49.3.101) dans une liste blanche où les flux ne sont pas analysés/surveillés.

Un travail a été réalisé avec les équipes SI des délégations et les équipes réseaux des universités.
Voici des exemples de solutions apportées sur quelques sites, en fonction des matériels utilisés.

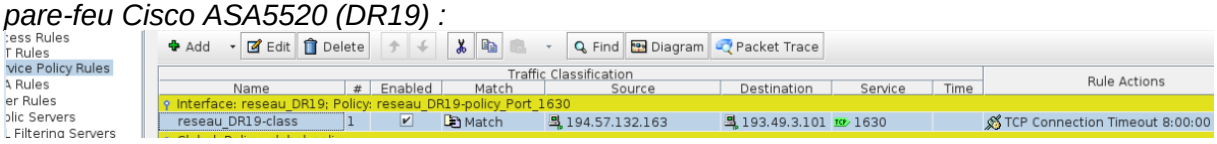
1.4.1 PARE-FEU/IDS NETASQ

Délégation Alsace
Il suffit de rajouter le serveur GESLAB dans le « Bypass » du module ASQ. Du coup seuls les flux entre le serveur GESLAB et les postes du LAN ne seront pas traités par le module ASQ.



1.4.2 PARE-FEU CISCO

pare-feu Cisco ASA5520 (DR19) :



1.4.3 PARE-FEU FORTINET

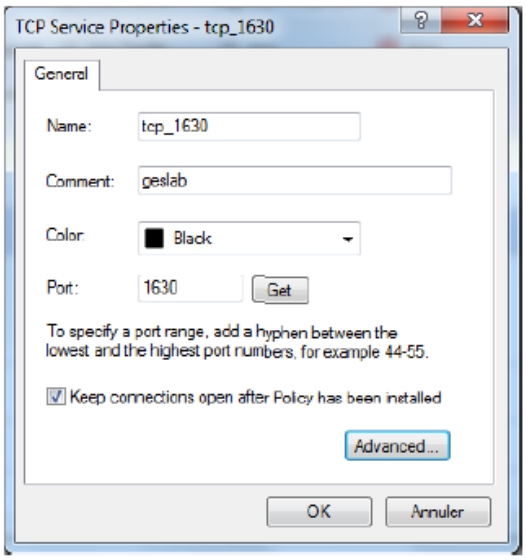
Configuration sur un Fortigate 310B (DR20, FortiOS 4.0 MR3)
La configuration est dans un virtual domaine « DR20 ».
Le timeout par défaut est de 3600s (1H) on la pousse à 28800 (8 H) pour le port 1630/tcp.

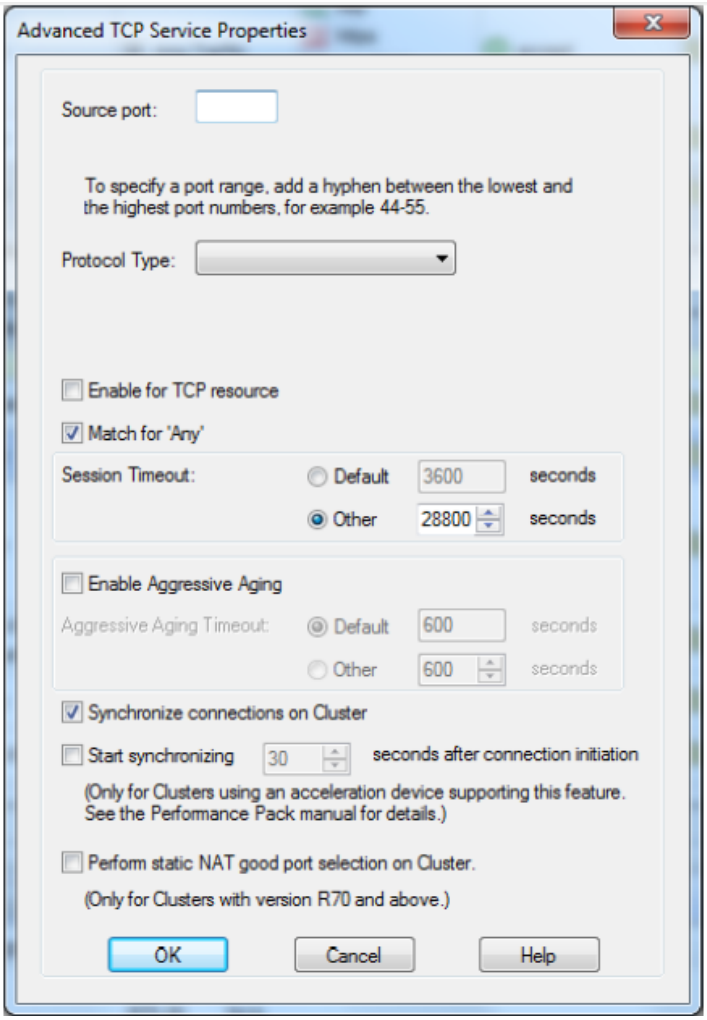
```
fg # config vdomfg (vdom) # edit DR20current vf=DR20:1
fg (DR20) # config system session-ttl
fg (session-ttl) # set default 3600
fg (session-ttl) # config port
fg (port) # edit 1630
new entry '1630' added
fg (1630) # set timeout 28800
fg (1630) # set protocol 6
fg (1630) # set start-port 1630
fg (1630) # set end-port 1630
fg (1630) # end
fg (session-ttl) # end
```

1.4.4 PARE-FEU CHECKPOINT

Exemple à Brest

Ajout d'une règle portant le timeout sur le port tcp 1630 à 28800s (8h) et on décoche l'onglet "Enable Agressive Aging" :





1.4.5 PARE-FEU « JUNIPER »

Exemple à l'Université Paris 10 (liste ASR)
Nous avons réglé le problème coté CRI de l'université en créant sur le juniper d'abord un service définissant un time out de 8 heures pour les sessions sur le port 1630. Ensuite nous avons créé une règle utilisant ce service pour l'adresse de destination 193.49.3.101. Cette a été placée en première afin d'être matchée avant les autres.

1.4.6 PARE-FEU KASPERSKY AU NIVEAU DU POSTE UTILISATEUR

Exemple à l'Université Paris 11 (liste ASR)

Le problème était dû au firewall intégré à l'antivirus des postes de travail de nos gestionnaires.

Avec Kaspersky 6.0 :

- Configurer le pare-feu.
- Ajouter une règle pour l'application omnis.exe V 5.0.1.0.
- Autoriser toute activité TCP et UDP.

1.4.7 REGLAGE AU NIVEAU DU NAT

Exemple à l'Université de Toulouse : il y avait une déconnexion au niveau du NAT au bout de 10 mn (sur un Netasq : il s'agissait de modifier le délai du NAT : Prévention d'intrusion > ASQ > Translation d'adresses > Expiration du NAT (passé à 60 mn au lieu de 20mn). Après redémarrage du FW, c'est OK)

Voici la piste suivie pour localiser le problème :
Constat depuis le poste de travail qui se connecte sur le serveur 193.49.3.101 : a priori, une action sur le logiciel, passé une dizaine de minutes d'inactivité de la connexion (TCP-1630), tombe en erreur.
À l'aide de TCPView, on remarque que le processus qui gère la connexion TCP-1630 (en question) s'ouvre, fonctionne correctement, reste en état "établi" au-delà de 10min… mais se ferme dès l'action (la requête vers silab) après l'inactivité de 10 min.
L'analyse des paquets, via wireshark, confirme tout cela : la première requête après le temps d'inactivité n'obtient pas de réponse, est retransmise 7 fois et se conclue par un RST de la connexion

Autre piste autour du NAT (LMGM – Toulouse, routeur Netasq) : il fallait modifier le délai du NAT dans *Prévention d'intrusion > ASQ > Translation d'adresses > Expiration du NAT*. Paramètre passé à 60 mn au lieu de 20mn, après redémarrage du FW c'est OK.

2 CLIENT WEB

2.1 JAVA

Le javascript doit être activé

2.2 NAVIGATEURS

Postes Microsoft :

- Mozilla Firefox 7 (minimum)
- Internet Explorer 8 (minimum)
- Chrome (pas de version minimum)

Postes MAC :

- Mozilla Firefox 7 (minimum)
- Safari 5.1 (minimum)

Postes Linux :

- Mozilla Firefox 7 (minimum)