Bomgar : Prise de contrôle contrôlée

Fabrice Prigent

Université Toulouse 1 Capitole

Jeudi 27 février 2014

Université en sciences sociales

- 20000 inscriptions
- 1100 personnels (permanents ou contractuels "présents")
- 3 sites sur 1 km de distance
  - L'Arsenal
  - Les anciennes facultés.
  - La Manufacture des tabacs
- Des délocalisations étrangères
  - Maroc
  - Vietnam
  - Vanuatu
  - etc.
- Des VIPs en déplacement permanent

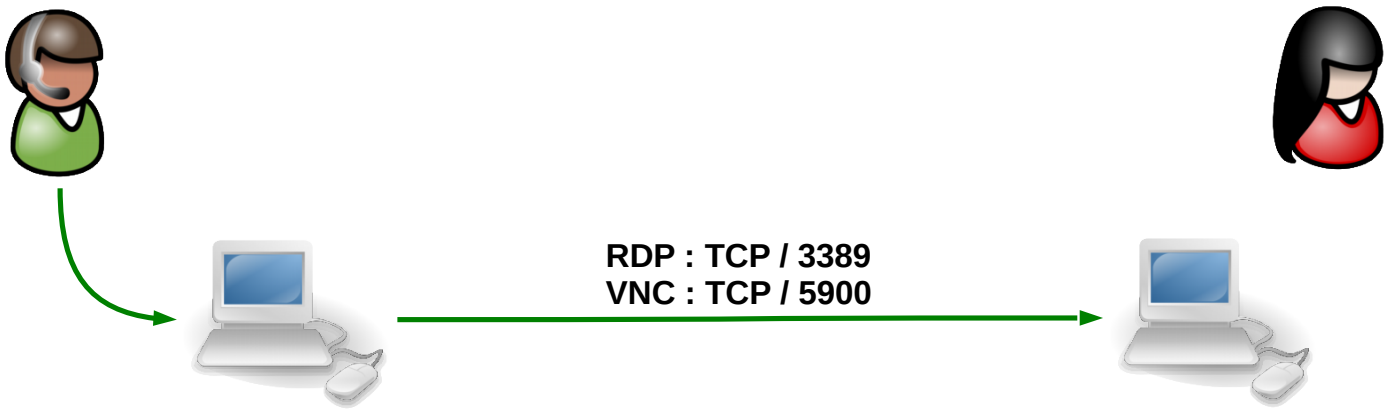
Le parc

- 1400 ordinateurs fixes
  - majoritairement pour les personnels et les étudiants
- 300 ordinateurs portables
  - majoritairement pour les responsables et les enseignants-chercheurs.
- Des postes "inventoriés non gérés" en progression
  - des Windows (version officielle +1, +2),
  - des Macs,
  - des Linux,
  - des smart/i/samsung/nimportenawak "phones" ou "tab".

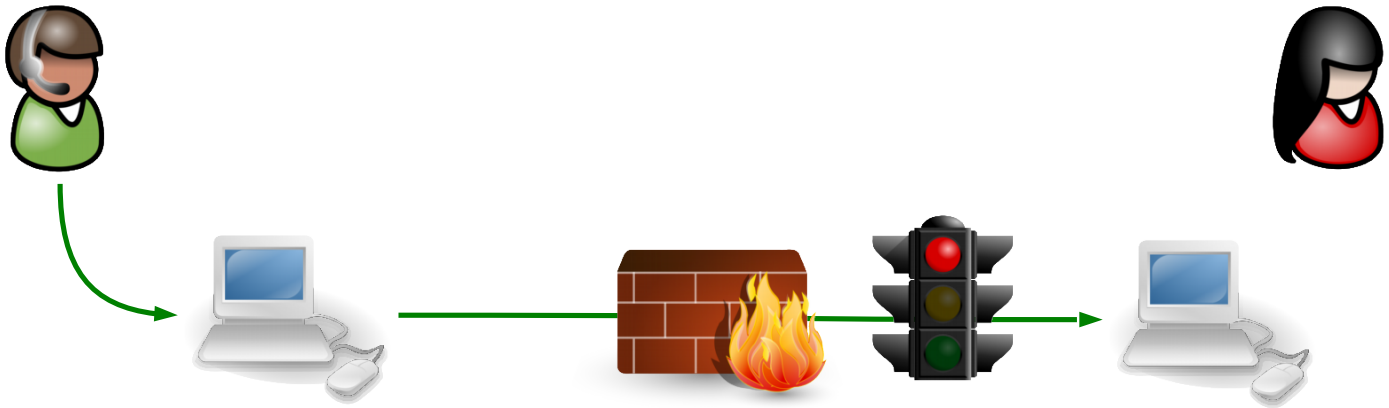
Les interventions

- Une structure centralisée (le 3636)
- 10 personnes pour le support
  - 2 personnes dédiées à l'accueil (niveau 0,1 ITIL)
  - 3 dédiées aux interventions (niveau 2 ITIL)
  - Déplacement sur place
  - Utilisation de VNC (UltraVNC)
  - 7000 interventions par an.

La prise de contrôle classique



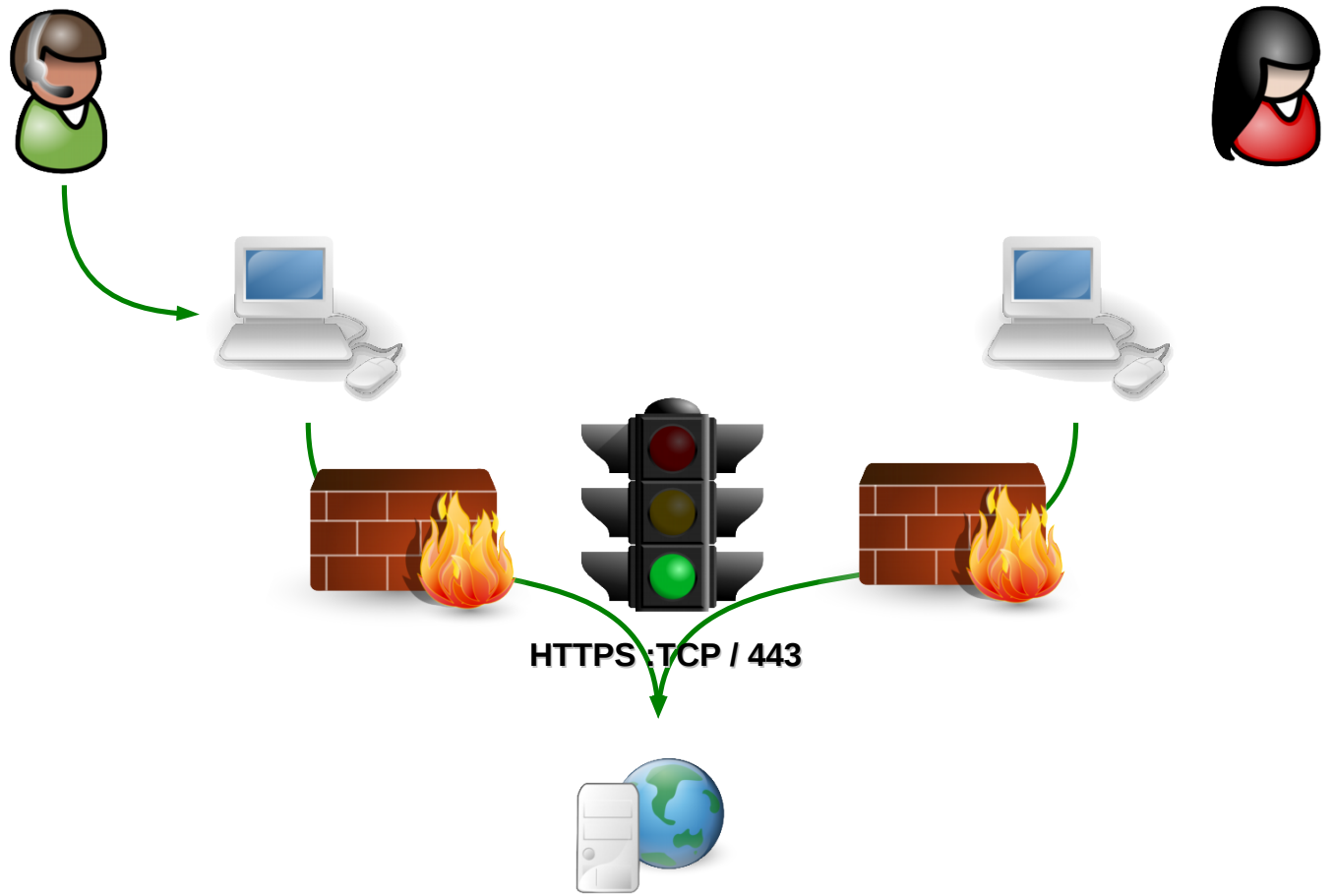
La prise de contrôle classique : avec firewall



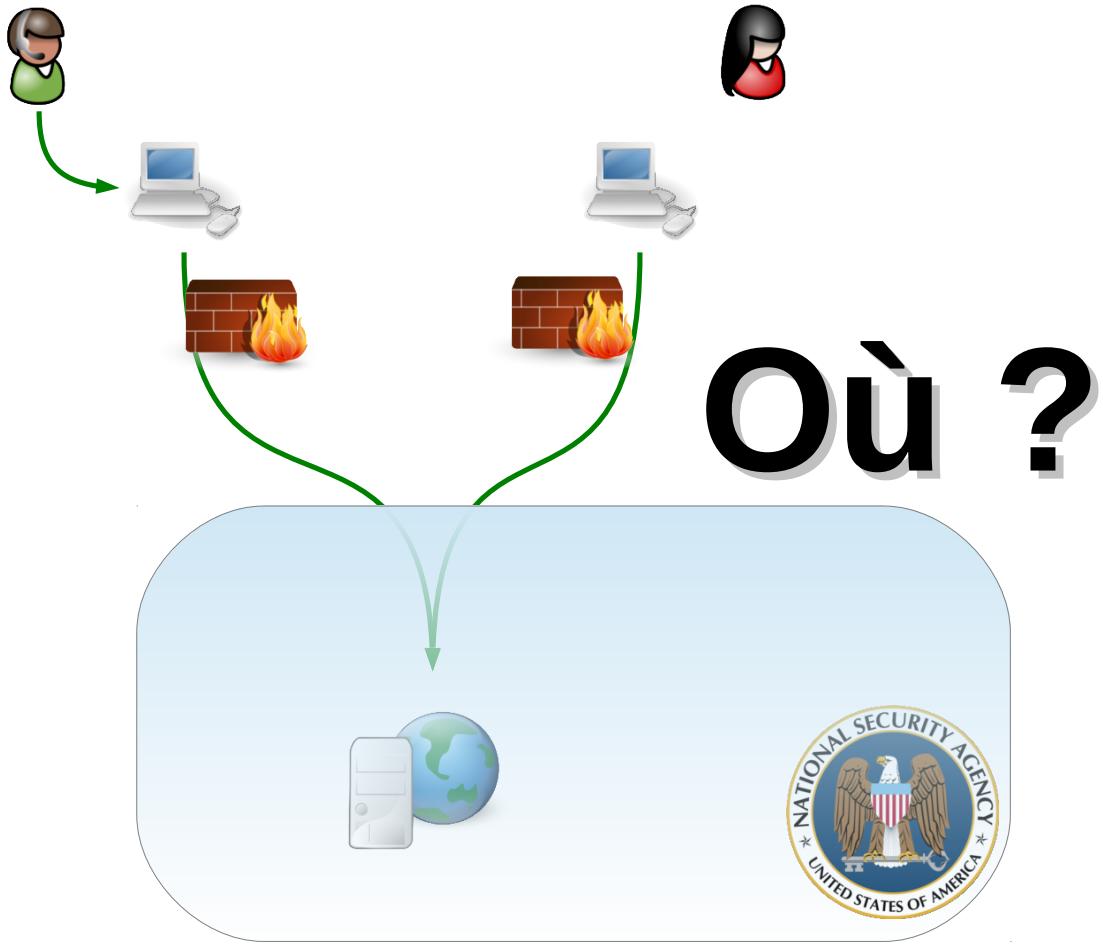
La prise de contrôle sans firewall

DNS	IP	Attaque	Nb
xxxxxx.powerhost.ro	93.114.46.160	Scan de port rdesktop	24492
adsl-98-71-245-112.jax.bellsouth.net	98.71.245.112	scan POP3	2998
richard.tcn.net	199.166.4.8	scan POP3	2604
41334f34.cst.lightpath.net	65.51.79.52	Scan de port rdesktop	2120
59.67.71.233	59.67.71.233	Scan de port rdesktop	1718
208.151.198.203.static.netvigator.com	203.198.151.208	scan POP3	1351
whitney.portmorgan.com	208.92.64.5	Scan de port rdesktop	1154
75-146-0-66-delmarva.hfc.comcastbusiness.net	75.146.0.66	Scan de port rdesktop	883
dsl-200-67-153-188-sta.prod-empresarial.com.mx	200.67.153.188	Scan de port rdesktop	565
188.212.152.4	188.212.152.4	Scan de port rdesktop	292
116.32.124.158	116.32.124.158	scan POP3	275
95-143-134-116.client.ltnet.cz	95.143.134.116	Scan de port actif telnet	136
ns1.mcsi.ro	80.96.196.3	Scan de port rdesktop	131
122-117-227-190.hinet-ip.hinet.net	122.117.227.190	Scan de port actif telnet	129
mom77-1-88-179-134-18.fbx.proxad.net	88.179.134.18	Scan de port actif telnet	115
acgr158.neoplus.adsl.tpnet.pl	83.9.245.158	Scan de port actif telnet	112
220-135-67-78.hinet-ip.hinet.net	220.135.67.78	Scan de port actif telnet	112
202-18-137-186.fibertel.com.ar	186.137.18.202	Scan de port actif telnet	111
server109-228-24-147.live-servers.net	109.228.24.147	Scan de port rdesktop	100
122.199.99.232	122.199.99.232	Scan de port actif telnet	99
sab57-4-88-164-211-233.fbx.proxad.net	88.164.211.233	scan POP3	94
220-134-182-16.hinet-ip.hinet.net	220.134.182.16	Scan de port actif telnet	78
host-92-26-192-174.as13285.net	92.26.192.174	Scan de port actif telnet	77
122-117-29-122.hinet-ip.hinet.net	122.117.29.122	Scan de port actif telnet	71
68-188-15-166.static.stls.mo.charter.com	68.188.15.166	Scan de port rdesktop	70
host68-171-149-62.serverdedicati.aruba.it	62.149.171.68	Scan de port rdesktop	60
fax.harboraccess.com	69.57.56.26	Scan de port rdesktop	55
pa42-241-22-24.pa.nsw.optusnet.com.au	42.241.22.24	scan POP3	51

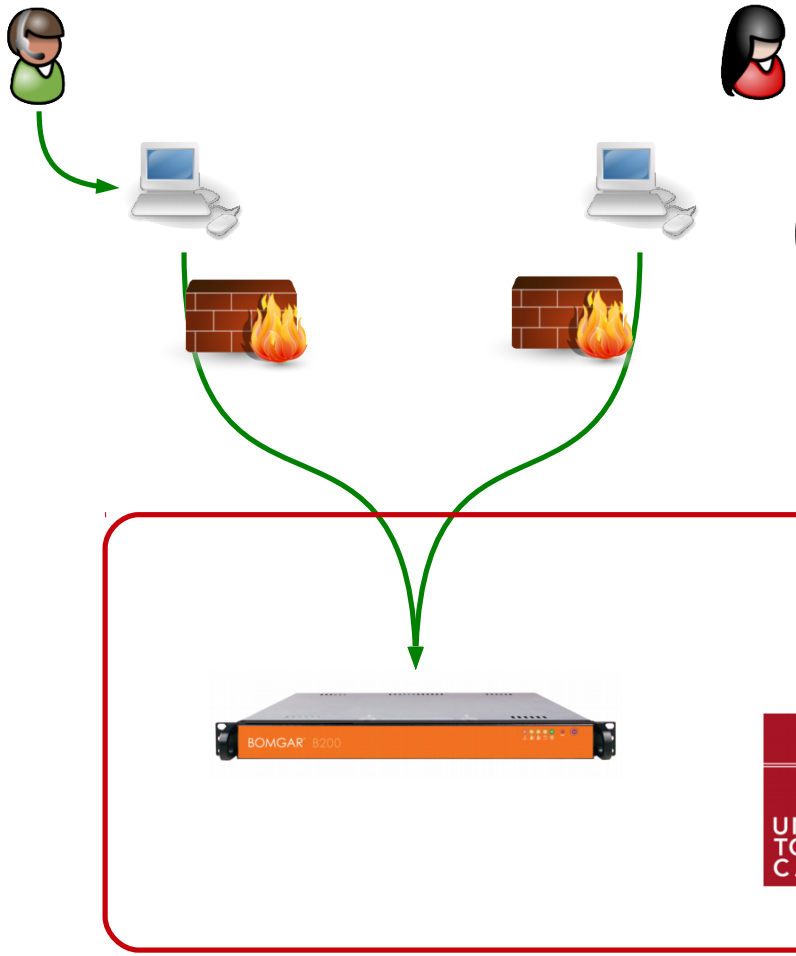
La prise de contrôle déportée



La prise de contrôle déportée : où ?



La prise de contrôle déportée : où ?



Chez Nous !

Des usages qui évoluent

- De plus en plus de portables
  - avec station d'accueil et écran de grand dimension (double écran)
  - avec une utilisation à la maison (par des lignes ADSL plus ou moins rapides)
- Généralisation des postes "non administrateurs"
  - installation de logiciels par la DSI
  - installation de composants par la DSI.

Des contraintes plus fortes

- Webification des applications
  - VNC gère très mal les navigateurs.
- Effet "PRISM"
  - Problématique de la prise de contrôle en passant par des serveurs étrangers.

Des constantes

- Plus la technologie avance, et moins les utilisateurs comprennent
- Plus la technologie avance, et plus la simplification donne l'impression aux utilisateurs qu'ils comprennent.
  - donc, ils veulent faire plus de choses
  - donc, ils font plus de ... manipulations inappropriées.

Nos demandes

- Passer les firewalls "simplement" (HTTP/HTTPS),
- Etre en mesure de gérer des postes à distance sur des lignes bas débit,
- Simplicité de déploiement (pour les utilisateurs, y compris Tata Josette),
- Contrôler la chaine de prise de contrôle,
- Passage en mode administrateur,
- Gestion du double écran.

Tests

Nous avons testé longuement chacun des concurrents potentiels.

- Dans les conditions d'utilisation demandées (ADSL)
- Avec les produits définitifs (logiciels ou matériels)

And the Winner is

- Parce qu'il est au même niveau que les leaders (logiciels) du marché sur les fonctionnalités.
  - LogmeIn
  - TeamViewer
- Mais qu'il est le seul, distribué en europe, à le faire sous notre contrôle. Un autre logiciel (streamconnect), sur le marché américain semble être en mesure de le faire.
- Parce que les versions du client sont toujours adaptées à la version du matériel.

Principes de fonctionnement

- Principe d'appliance (possibilité de SaaS, et de VM)
- Connexions sortantes en HTTPS (compatibilité maximale avec les Pare-feu)
  - pour l'informaticien
  - pour l'utilisateur
- En "one-shot" non préparé
  - l'informaticien génère un code sur la plateforme
  - l'utilisateur va sur l'url `http://sos.ut-capitole.fr/`
  - il entre le code
  - il télécharge le client
- Si le poste est préparé
  - Installation d'un bouton d'appel
  - Installation transparente d'un lancement de client (notion de jump client).

Des clients

- Distribution des logiciels de prise en main
  - par HTTPS
  - depuis le boitier
  - pour l'informaticien et l'utilisateur
- Pour tous les OS (pour informaticien et utilisateur)
  - Windows
  - Mac/OS
  - Linux
  - Android (en lecture seule pour le client)
  - IOS (avec restrictions malgré tout)

Les fonctions

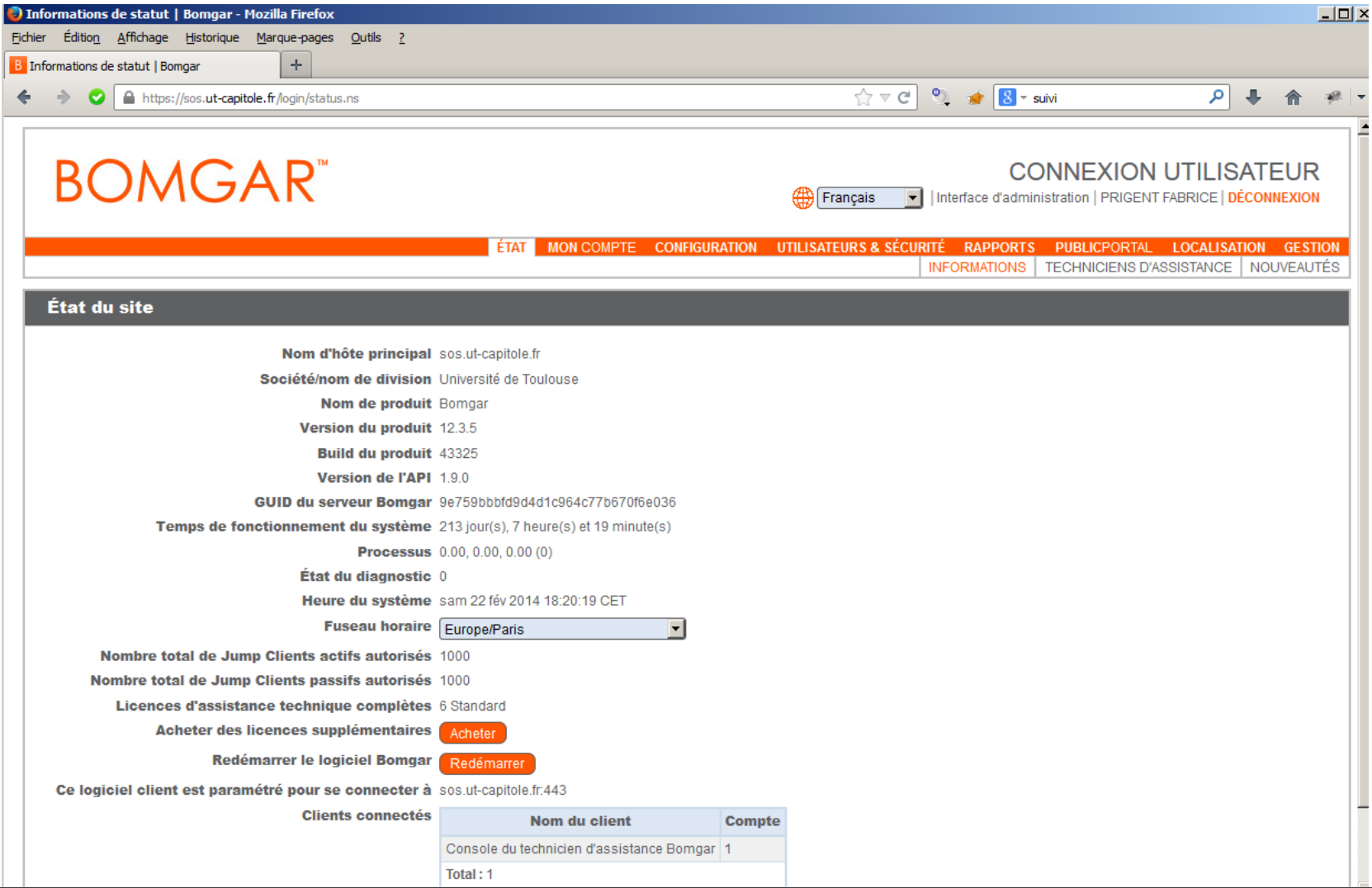
- Prise de contrôle
- Transfert de fichiers
- Informations système
- Chat
- Lancement de commandes en mode administrateur

La gestion des licences

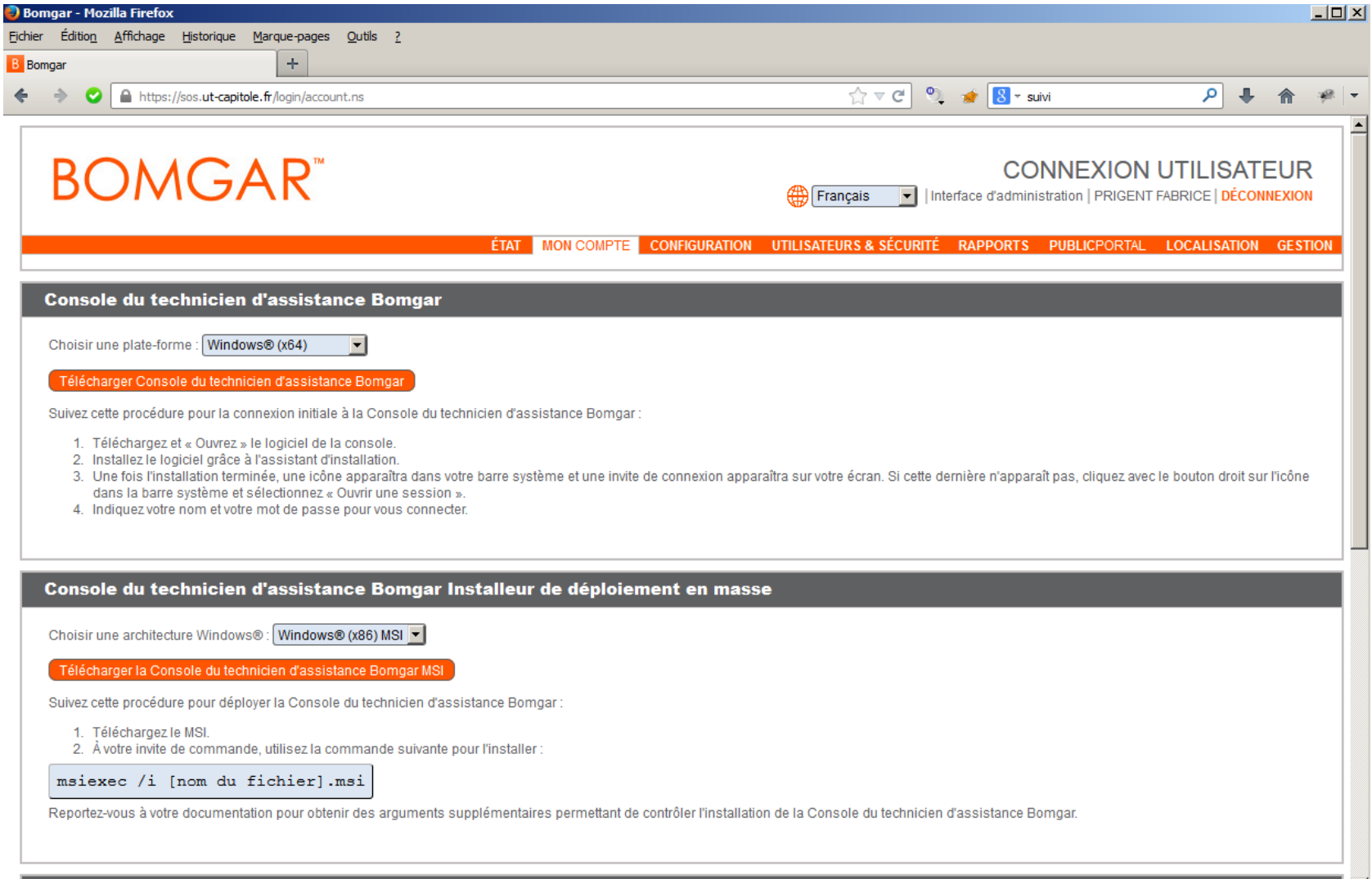
- Achat d'un boitier (B200 pour nous), moins de 2000 €.
- Achat de licences simultanées d'utilisation
  - suivant le mode (entreprise ou standard)
  - en gros le prix du boitier
- Maintenance
  - 15% par an
  - Elle n'est pas obligatoire (le client n'a pas d'upgrade forcé)
- En cours de validation par le "Groupe Logiciel" du MESR.

Support : Portail

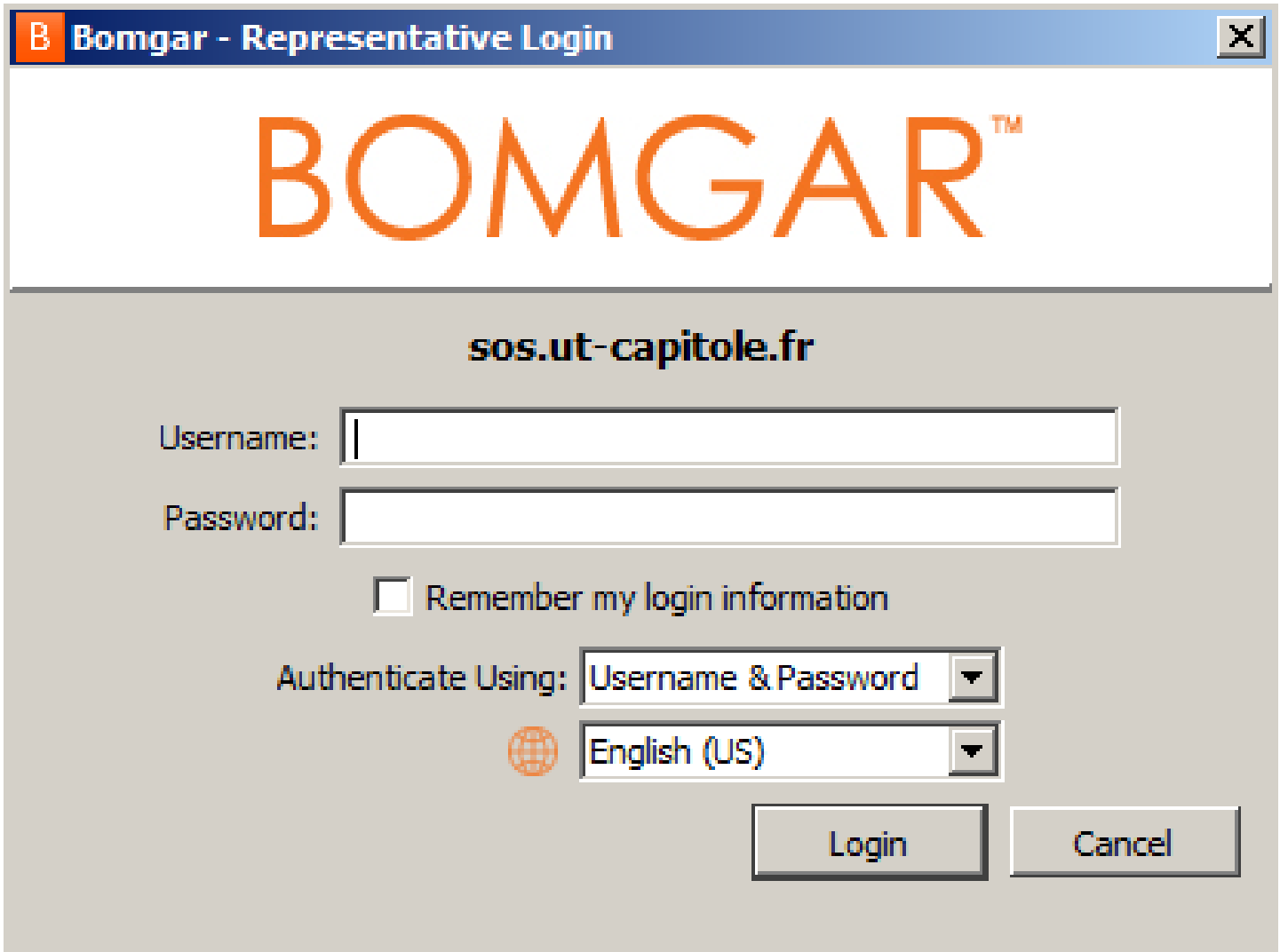
Support : Portail



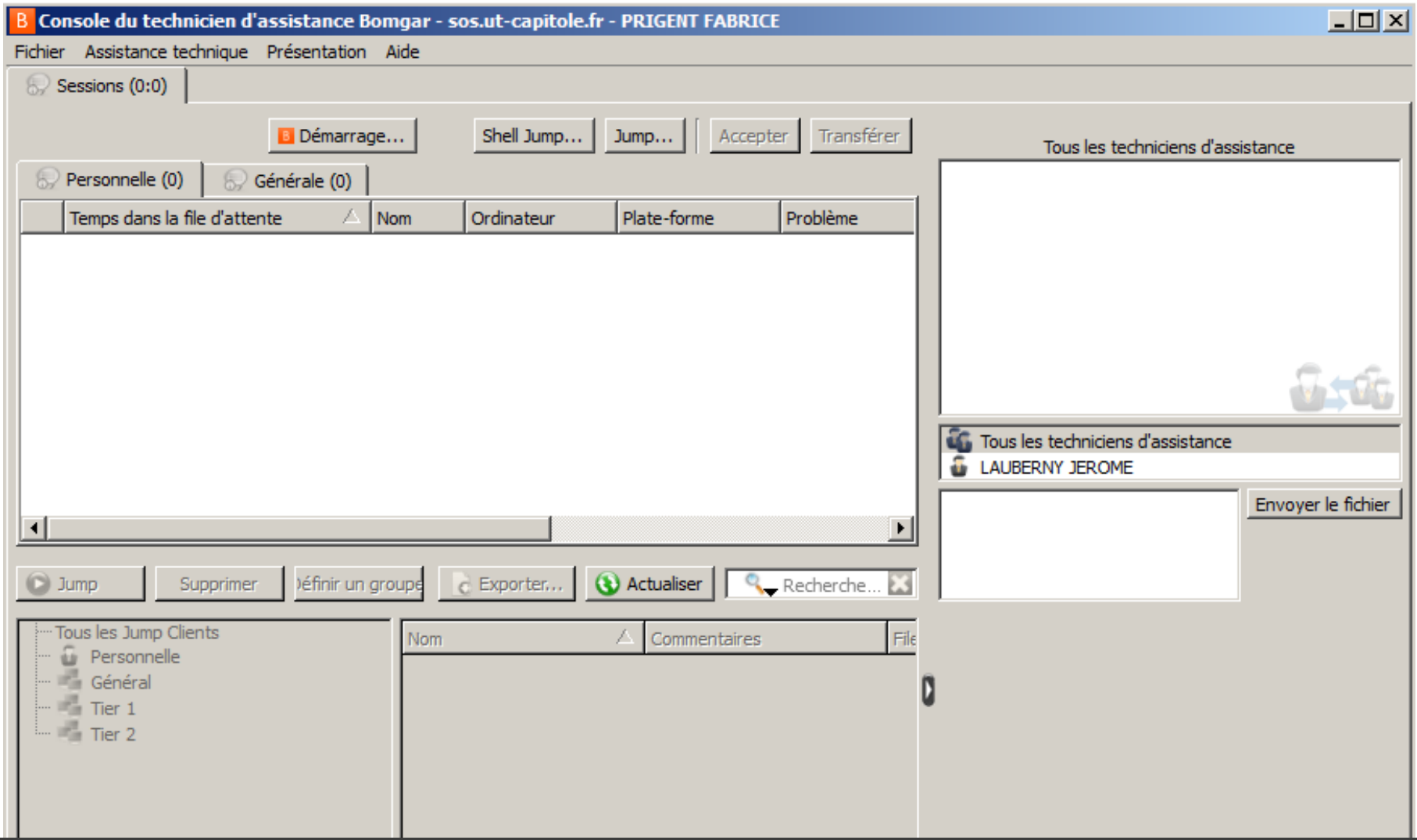
Support : Téléchargement



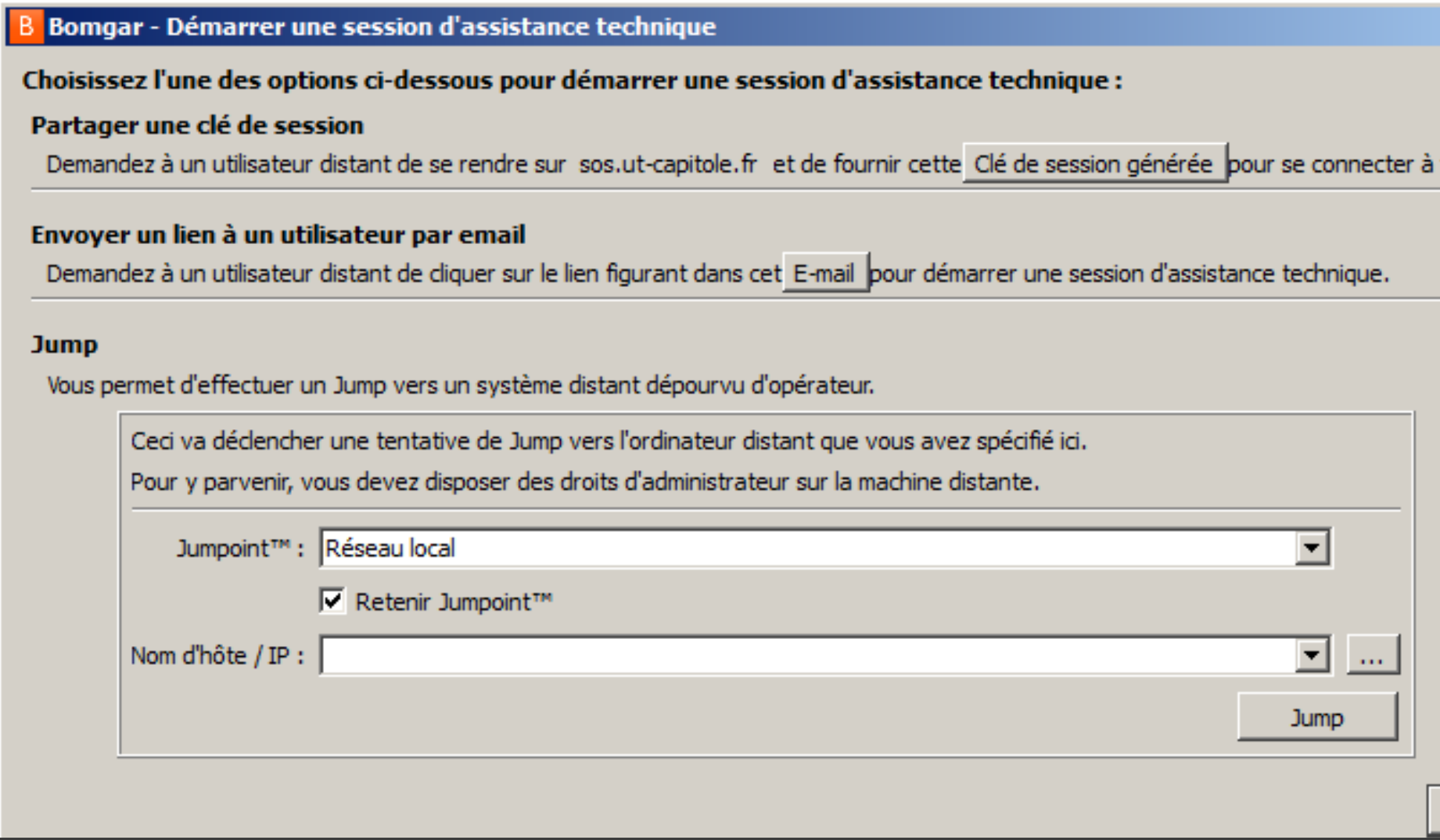
Support : Lancement du logiciel



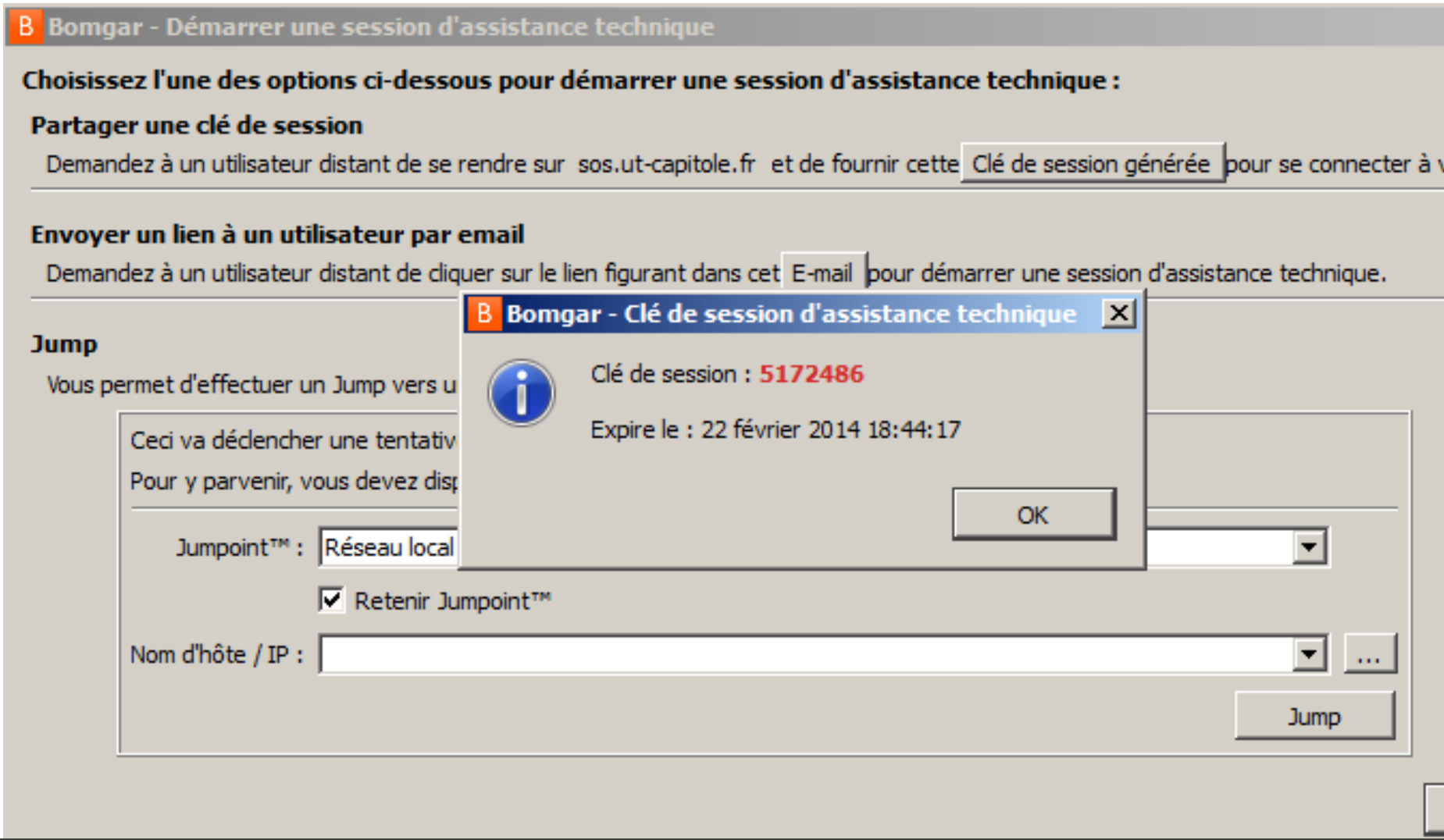
Support : Lancement du logiciel



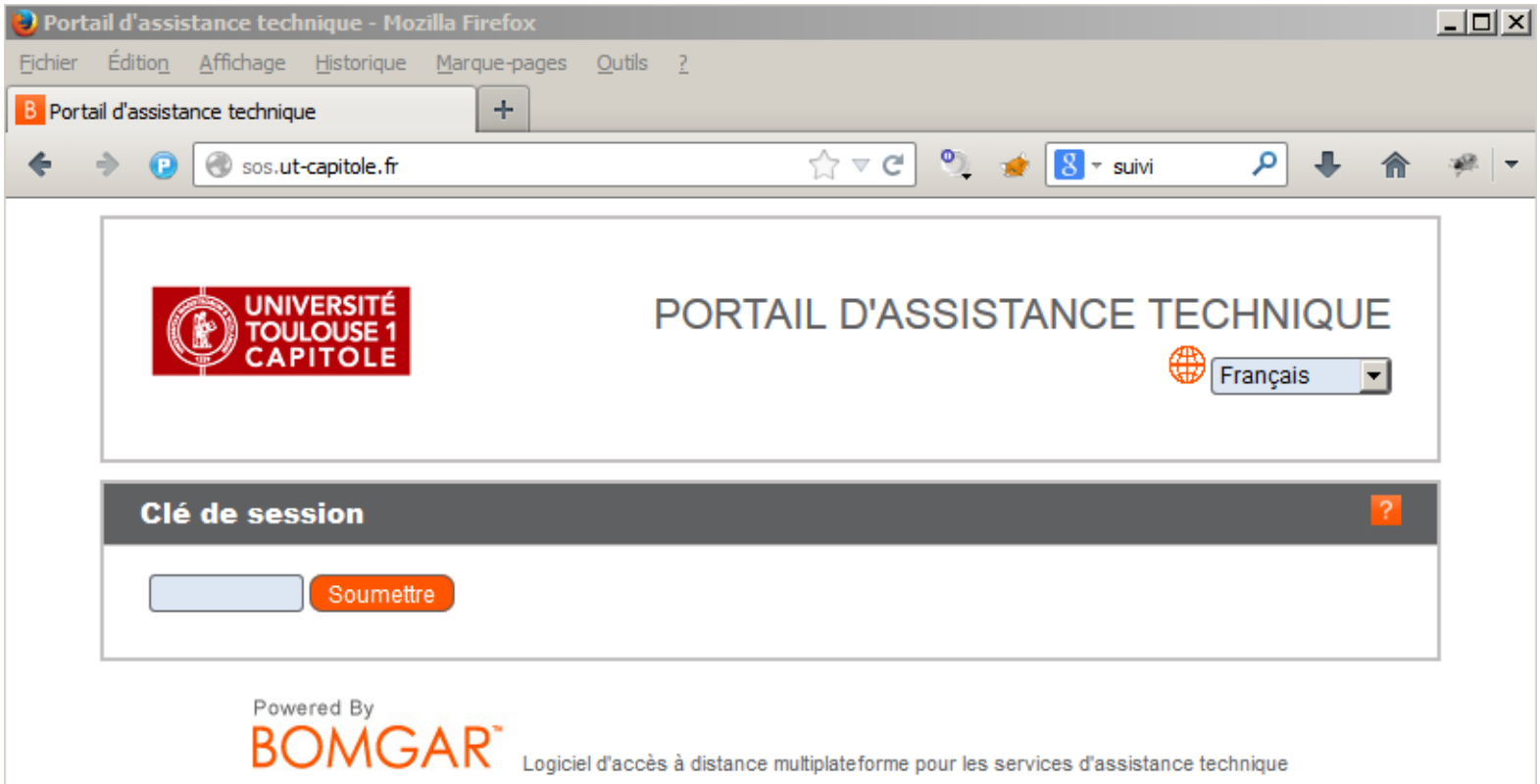
Support : Choix d'une prise de contrôle



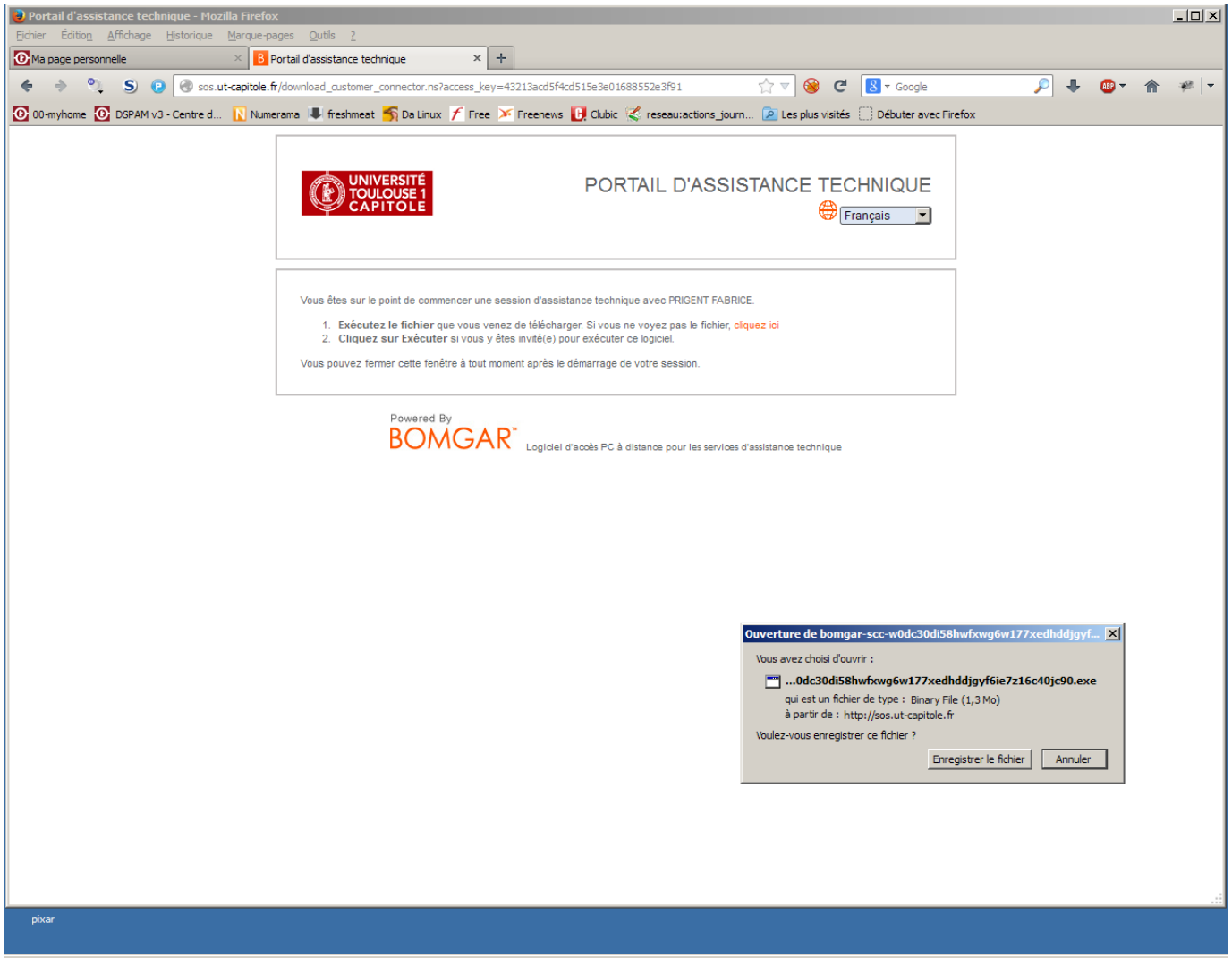
Support : Création d'un numéro de session



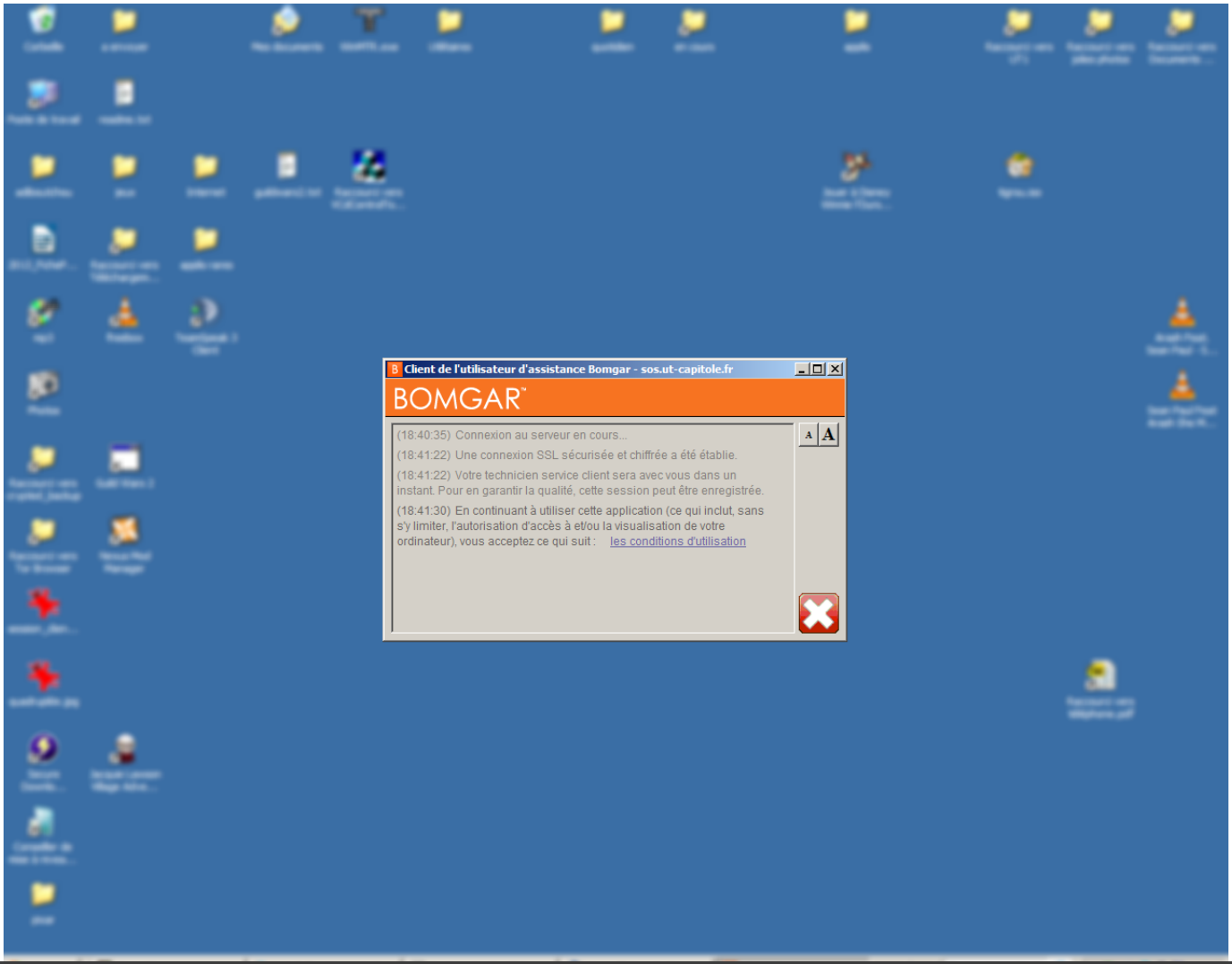
Utilisateur : Portail



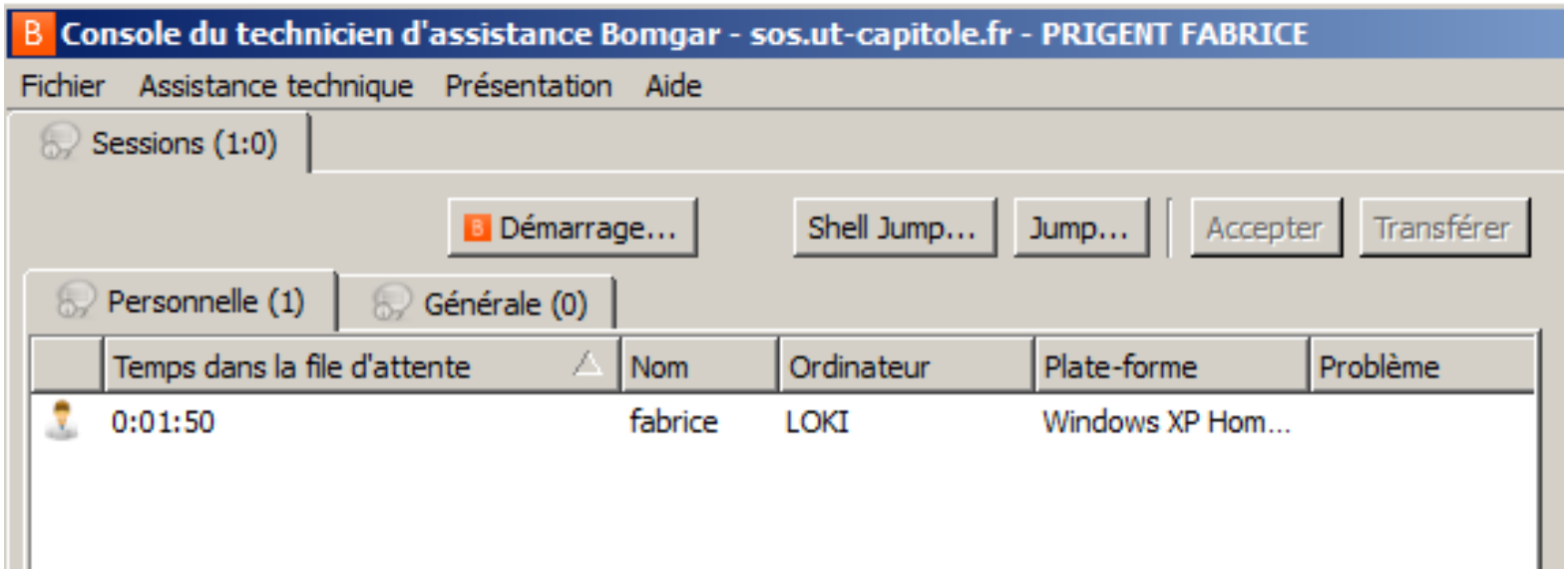
Utilisateur : Rapatriement du client spécifique



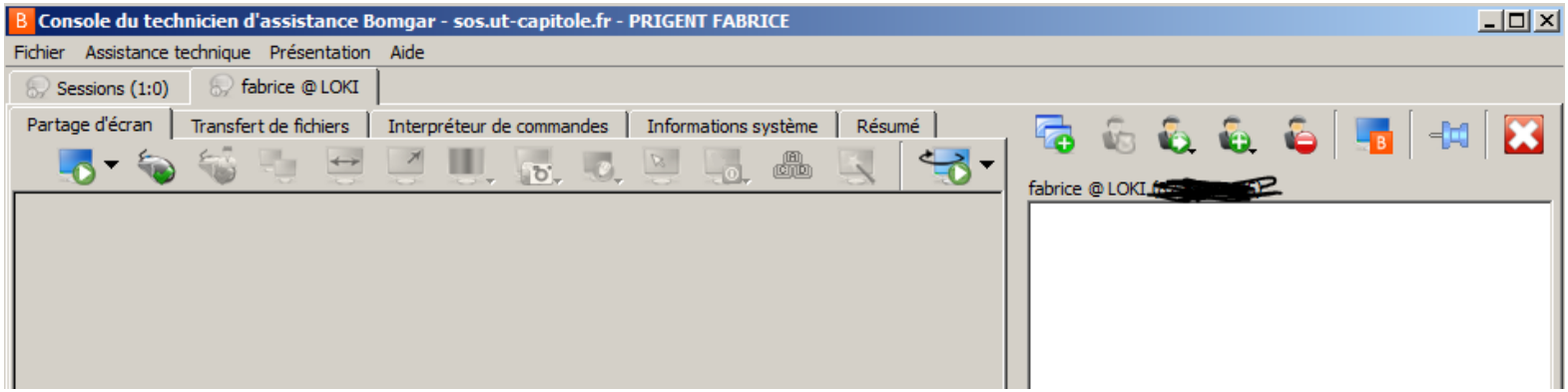
Utilisateur : Lancement du client



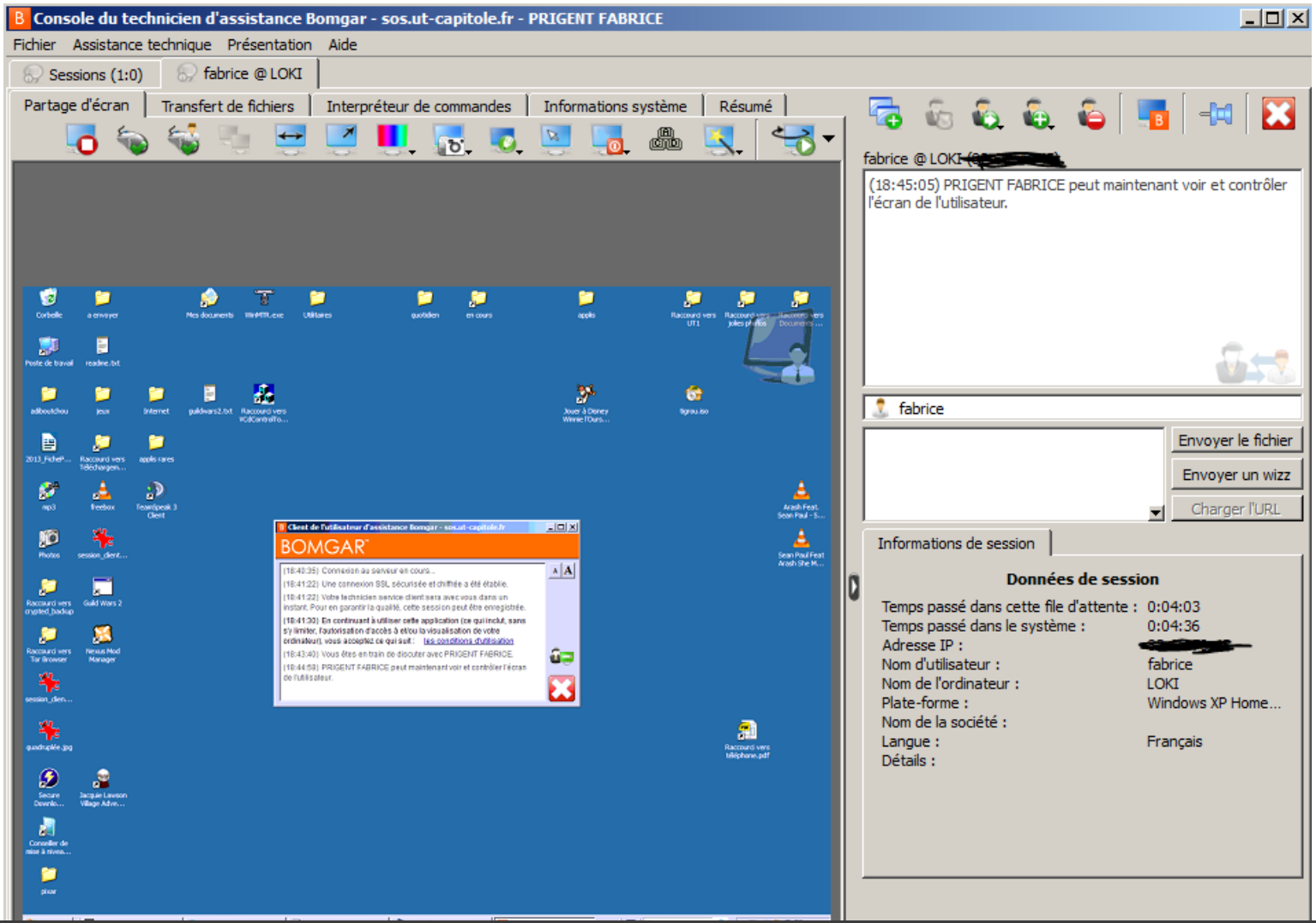
Support : visualisation de la session



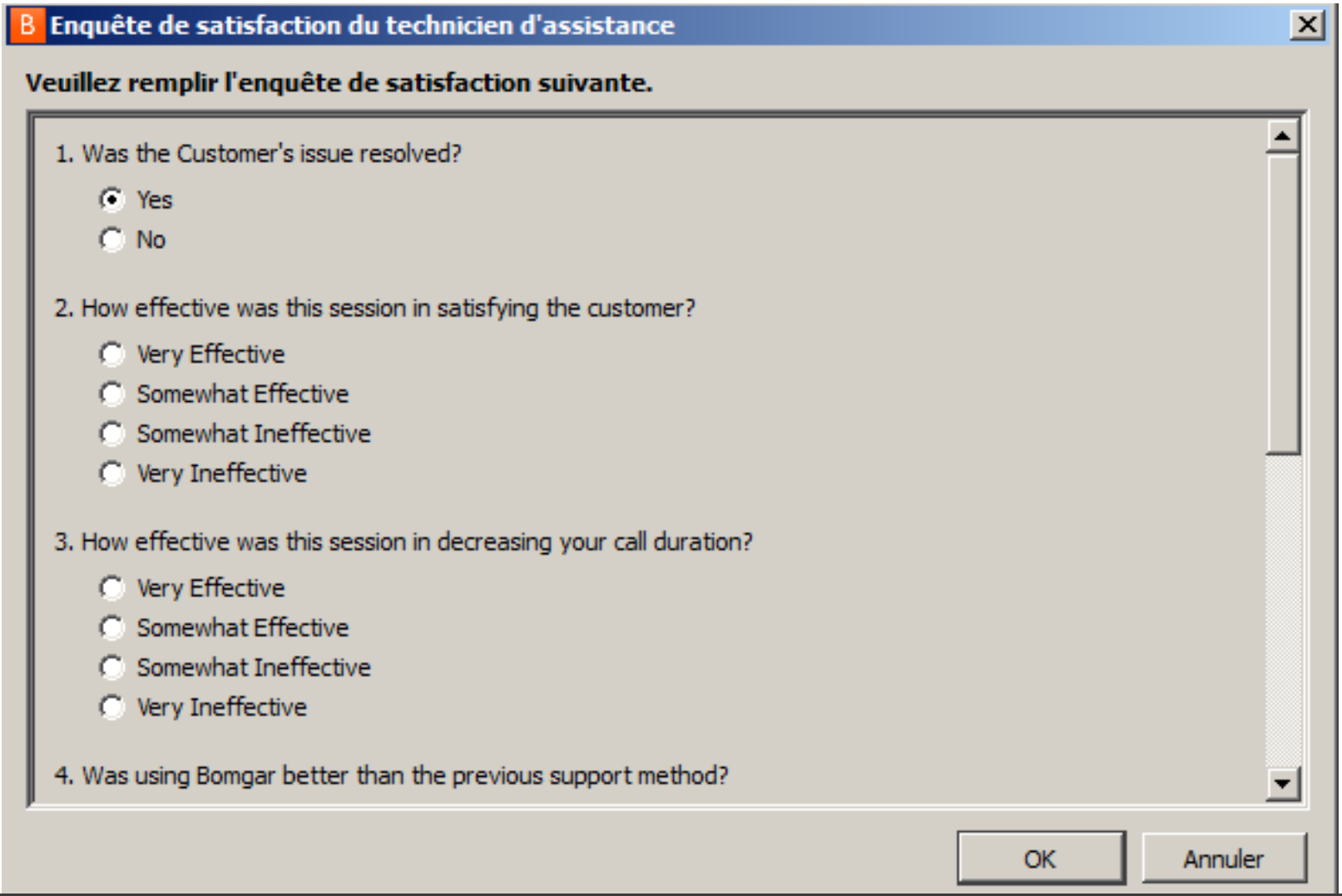
Session utilisateur



Session utilisateur



Session utilisateur



Les modes de connexions

5 modes principaux :

- One-shot
- Bomgar Button
- Jump client passif
- Jump client actif
- JumpPoint

One-Shot

Présenté ci-dessus, en général pour un poste inconnu ou jamais traité

Bomgar Button

- C'est une "icone" placée soit par déploiement, soit "épinglée" lors d'un "one-shot"
- Quand on clique, il met dans la file d'attente d'un informaticien ou d'un groupe d'informaticiens, la demande d'intervention.
- Le bouton peut-être personnalisé par les administrateurs bomgar
  - pour un informaticien particulier
  - avec une icone particulière
  - pour une durée particulière
    - une heure
    - une semaine

    ...
    - 5 ans

JumpClient

- C'est un "service" qui est déployé et lancé automatiquement
- L'informaticien prend directement la main sur le poste de l'utilisateur sans intervention de celui-ci
- Le jumpclient peut-être personnalisé par les administrateurs bomgar
  - pour un informaticien particulier (ou un groupe)
  - pour une personne particulière ou pour tous les utilisateurs
- Il existe en 2 modes
  - le mode actif
  - le mode passif

JumpClient Actif

- Le client se connecte automatiquement au serveur Bomgar
- Le nombre de sessions simultanées est limité par le serveur
  - 1.000 pour un B200
  - 5.000 pour un B300
  - 10.000 pour un B400
- Les sessions consomment de la CPU
- Le client peut-être n'importe où dans le monde
- Utile pour les informaticiens qui veulent, de chez eux, prendre le contrôle de leur PC de bureau (ne contourne pas les screensavers, mais attention à l'ouverture de l'accès ! !)

JumpClient Passif

- Le client se signale automatiquement 1 fois par jour au serveur Bomgar
- Il faut contacter le client sur un port particulier pour déclencher la prise de contrôle
- Le nombre de sessions simultanées est limité par le serveur
  - 1.000 pour un B200
  - 5.000 pour un B300
  - 10.000 pour un B400
- Les sessions ne consomment quasiment pas de CPU

JumpPoint

- Nécessite des licences "entreprises".
- C'est un proxy, qui doit être installé sur une machine dédiée.
- Le jumpoint permet de prendre le contrôle des postes sur le broadcast.

Des précautions

Le logiciel est particulièrement paramétrable, surtout en terme de permissions. Les rôles sont les suivants :

- L'administrateur Bomgar : il peut tout et voit tout
- L'informaticien : un compte lui est associé et peut éventuellement
  - consulter,
  - manipuler,
  - déployer.
- La granularité
  - la totalité,
  - le groupe,
  - l'informaticien.

Des précautions

- Gérer des postes au Vanuatu avec 12 heures de décalage horaire ne signifie pas 24/24H !
- Bien choisir son mode d'intervention.
- Il peut faire beaucoup de choses, mais il faut choisir un périmètre :
  - SCCM permet la prise de contrôle de postes fixes locaux.
  - Bomgar peut faire du lancement automatique de scripts.
  - Bomgar fait de l'enquête de satisfaction.

Des avantages périphériques

- L'utilisateur sait QUI se connecte.
- Prise de contrôle par des sociétés extérieures avec enregistrement des sessions.
- Possibilité de "pousser" des prises de contrôle vers un "expert".
- Liaison avec le LDAP, un AD, mais aussi une base locale.
- Les clients sont disponibles sur le serveur.
- On peut faire des présentations 1 vers n (50) facilement.
- On peut "retourner" la session (le client voit l'écran de l'informaticien).
- Quasiment tout est paramétrable.
- Des API sont disponibles.

Conclusion

Bomgar

- est un des (rares) projets qui s'est déroulé sans difficulté,
- fait exactement ce qu'on lui demande,
- fait facilement ce qu'on lui demande,
- fait tellement de choses, que l'on ne peut tout mettre en place,
- permet de bloquer par filtrage url les autres services de prise de contrôle,
- a un bon ROI (estimation : 2 ans à condition que votre direction connaisse la notion de coût complet).

Mais

- il nécessite de bien réfléchir aux périmètres des divers outils de gestion de parc,
- il faut choisir correctement les modes de déploiement,
- la gestion des smartphones est perfectible,

Merci de votre attention

Des questions ?