

Utilisation de DataConf avec un Firewall et un Proxy Web

1 - Pourquoi DataConf peut être considéré dangereux par les *firewalls* ou les *proxys* ?

Le système DataConf utilise le protocole RFB/TCP pour l'échange des données d'information qui permettent de retransmettre l'écran du conférencier. Il s'agit du protocole standard utilisé entre autre par les programmes d'administration de machines distantes tel que VNC. Ce genre de programmes permet de voir un écran et de connaître tous les événements clavier et souris d'une machine distante. C'est pourquoi les *firewalls* considèrent généralement les programmes utilisant ce protocole comme dangereux pour la sécurité.

2 – Pourquoi DataConf est sûr d'utilisation ?

DataConf protège la confidentialité de votre conférence et la sécurité de votre machine par plusieurs dispositifs :

- Un code de session est calculé aléatoirement à chaque conférence. Cela vous assure que seules les personnes ayant ce code peuvent accéder à votre conférence.
- Si un niveau de sécurité supplémentaire est nécessaire, vous pouvez crypter vos conférences. Cela vous assure qu'une personne malveillante ne peut pas accéder à votre machine même en espionnant ce qui circule sur le réseau.

Pour une utilisation transparente de votre part, nous utilisons le *tunneling* pour faire transiter les données de votre conférence. En effet un tunnel est créé entre votre machine, notre serveur et les participants à la conférence (cf. figure 1).

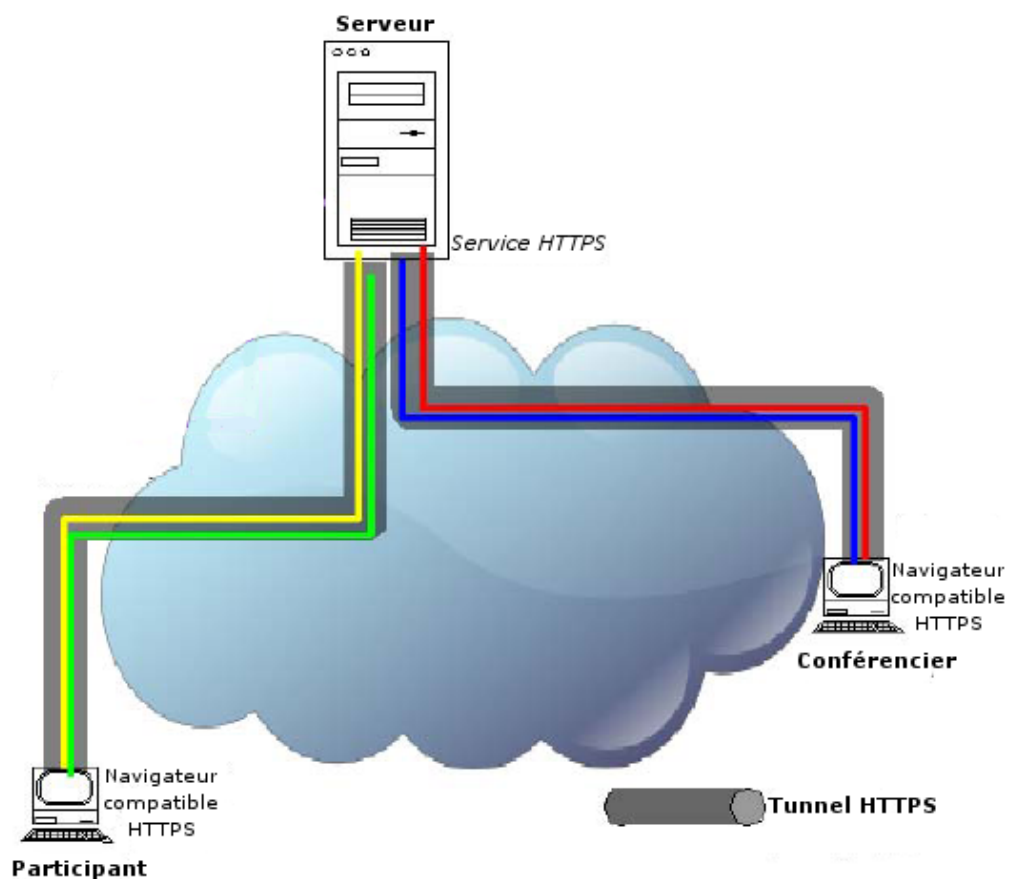


Fig 1 : Schéma du *tunneling* DataConf.

3 – Utilisation en pratique de DataConf avec un *firewall*.

3 – 1 Cas du conférencier.

Lors du lancement de la conférence, le conférencier doit cliquer sur la case à cocher « Etes-vous derrière un pare-feu (Firewall) ? » (cf. figure 2).

Dans le cas où le conférencier possède un *firewall* logiciel sur sa machine, il est possible que le *firewall* déclenche une alerte lors du lancement de la conférence. Le conférencier doit alors désactiver son *firewall* pour les services DataConf (se rapporter à la notice du *firewall*).

Paramètres de connexion	
Voulez-vous une connexion sécurisée (SSL) ? <input type="checkbox"/>	Etes-vous derrière un pare-feu (Firewall) ? <input type="checkbox"/>
Utilisez-vous un proxy ? <input type="checkbox"/>	Hôte Proxy : <input type="text"/>
	Port Proxy : <input type="text"/>
	Proxy Username : <input type="text"/>
	Proxy Password : <input type="text"/>

Paramètres de la conférence	
Port de la conférence : <input type="text"/>	Pseudo : <input type="text"/>
Code de la conférence : <input type="text"/>	Email : <input type="text"/>

Fig 2 : Copie de l'interface DataConf : utilisation d'un *firewall*.

3 – 2 Cas d'un invité à la conférence.

Lors de l'accès à la conférence, l'invité doit cliquer sur la case à cocher « Etes-vous derrière un pare-feu (Firewall) ? » (cf. figure 2).

4 – Utilisation en pratique de DataConf avec un *proxy*.

4 – 1 Cas du conférencier.

Lors du lancement de la conférence, le conférencier doit cliquer sur la case à cocher « Utilisez-vous un proxy ? » (cf. figure 3, étape 1).

Puis il doit remplir les champs : « Hôte Proxy », « Port Proxy », « Proxy Username », « Proxy Password ». Ceux –ci correspondent à la machine qui héberge le *proxy*, le port d'utilisation, le nom d'utilisateur et le mot de passe du *proxy*. Dans le cas où il n'y a pas d'utilisateur et mot de passe pour accéder au *proxy*, le conférencier doit laisser ces champs vides (cf. figure 3, étape 2).

Paramètres de connexion	
Voulez-vous une connexion sécurisée (SSL) ? <input type="checkbox"/>	Etes-vous derrière un pare-feu (Firewall) ? <input type="checkbox"/>
Utilisez-vous un proxy ? <input checked="" type="checkbox"/> 1	Hôte Proxy : Machine_Proxy
	Port Proxy : 8080
	Proxy Username : <input type="text"/>
	Proxy Password : <input type="text"/>

Paramètres de la conférence	
Port de la conférence : <input type="text"/>	Pseudo : <input type="text"/>
Code de la conférence : <input type="text"/>	Email : <input type="text"/>

Fig 3 : Copie de l'interface DataConf : configuration du proxy.

4 – 2 Cas d'un invité à la conférence.

Lors de l'accès à la conférence, l'invité doit cliquer sur la case à cocher « Utilisez-vous un proxy ? » (cf. figure 3, étape1).

Puis il doit remplir les champs : « Hôte Proxy », « Port Proxy », « Proxy Username », « Proxy Password ». Ceux –ci correspondent à la machine qui héberge le *proxy*, le port d'utilisation, le nom d'utilisateur et le mot de passe du *proxy*. Dans le cas où il n'y a pas d'utilisateur et mot de passe pour accéder au *proxy*, l'invité doit laisser ces champs vides (cf. figure 3, étape 2).