

La sécurité englobant l'utilisation du WebAgent.

Geocom France Informatique

SOMMAIRE:

- **Installation du logiciel webAgent**
- **Les accès utilisateurs**
- **Schéma**
- **Sécurité en cas d'intrusion**
- **Certificats**
- **Directives d'accès au logiciel WebAgent de l'extérieur**

❖ Installation du logiciel webAgent

Geocom WebAgent est installé en tant que page autonome dans IIS. La communication avec le serveur d'application Geocom se fait via des sockets et trois ports (port système, port données, port fichier), qui sont définis dans les paramètres de configuration du serveur d'application Geocom.

Par défaut, nous réalisons l'installation du WebAgent uniquement pour le réseau interne du client

IIS: Internet Information Server

❖ Les accès utilisateurs

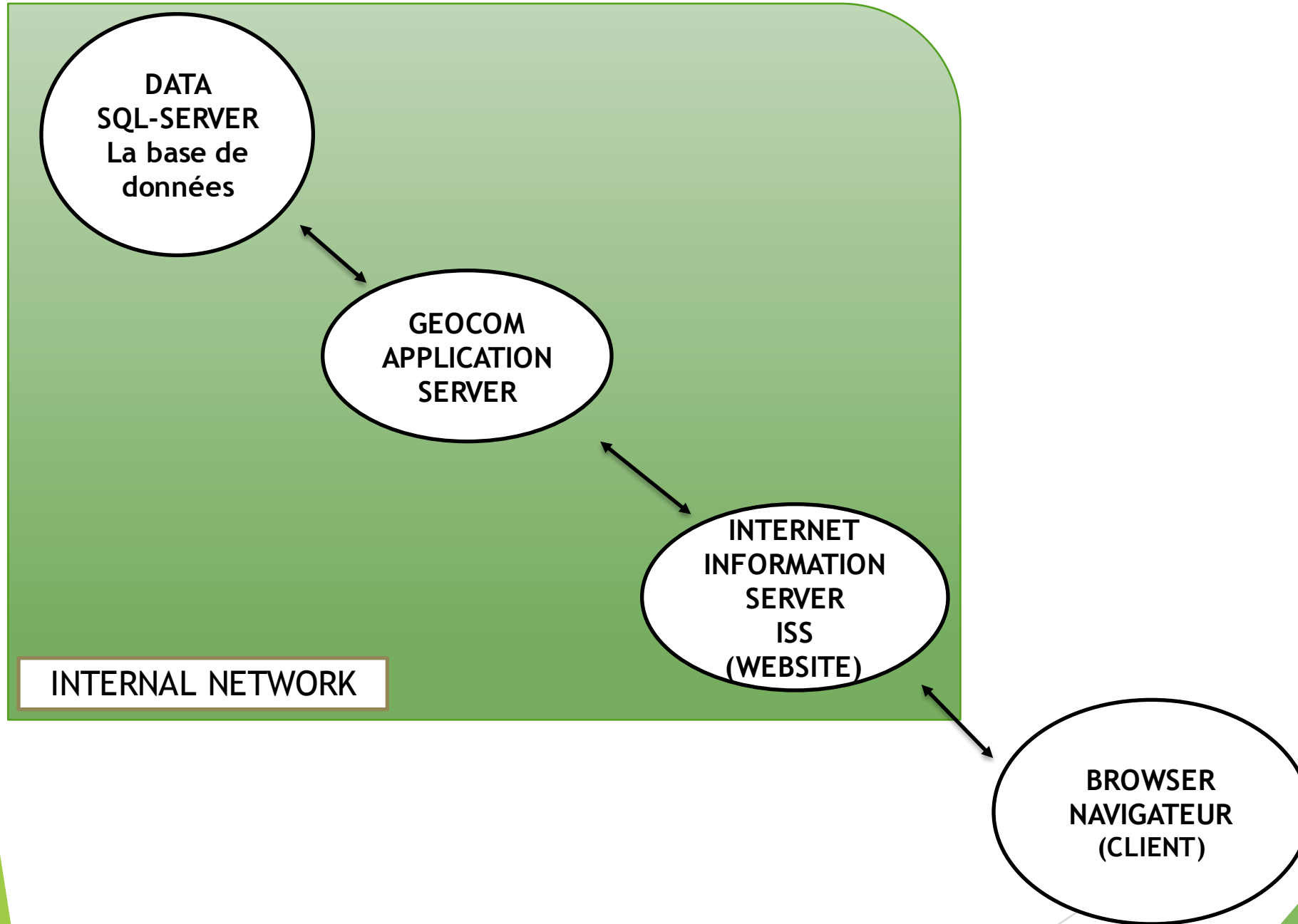
L'utilisation des fonctions Geocom WebAgent n'est accessible qu'aux utilisateurs autorisés après une authentification réussie.

Seuls les utilisateurs authentifiés sont autorisés à communiquer avec le serveur d'application Geocom. Et le Geocom WebAgent est stocké en permanence dans le programme en tant qu'utilisateur.

Cela garantit que seuls les utilisateurs autorisés peuvent accéder aux données sur le serveur d'application Geocom. De même, les ports ouverts ne peuvent pas être utilisés pour accéder au réseau en général.

Il est cependant possible, d'accéder au WebAgent de l'extérieur, si l'on suit une ou plusieurs des directives suggérées (voir page 8)

❖ Schéma



❖ Sécurité en cas d'intrusion

Contrairement à la plupart, notre site Web donne AUCUN ACCÈS DIRECT aux données. Donc même si le site Web est piraté de l'extérieur, le pirate n'aura pas accès aux données. Le site Web ne le fait même pas «savoir» où les données sont stockées, car la communication du site Web se fait uniquement avec le serveur d'application Geocom (voir le schéma).

Ainsi, même en cas de piratage du site Web, les intrus n'obtiendront pratiquement aucune information de la base de données Geocom

La responsabilité principale de la sécurité et de la protection contre le piratage de ce site Web incombe donc au service informatique du client

❖ Les Certificats

La plus importante est en fait une mesure obligatoire que IIS doit être exécuté avec un certificat SSL (connexion https), de sorte que la communication entre le navigateur et le site Web soit cryptée.

Logiciels utilisés:

- Microsoft Internet Information Services (IIS) version 7.0 ou supérieure
- Geocon Roster Pro Server (serveur d'application Geocon)
- Crystal Reports Runtime Version 13

Technologies:

- ASP.NET - Technologie de Microsoft
- Geocon WebClient représente une application Web.



Directives d'Accès au logiciel WebAgent de l'extérieur

- Avoir un certificat générique pour le domaine du client (par exemple, *.geocon.de qui comprend également www.geocon.de)
- créez un sous-domaine et laissez-le pointer vers l'adresse IP externe / publique de l'endroit où le client héberge son client Web. Utiliser le port standard 443 pour **https**. ou un port exotique.
- créer une règle de mappage de port sur le pare-feu externe ou (routeur DSL) qui pointe vers le serveur et le port sur lesquels s'exécute le client Web
- importer le certificat dans l'IIS
- Dans IIS, créez une liaison nouvelle / supplémentaire (443 ou un autre port exotique) pour le site Web du WebClient et sélectionnez le certificat à utiliser avec lui (celui importé)

La communication entre le navigateur et WebClient est alors sécurisée via le protocole https.