Sécurité Réseau

Utilisation de Différents Ports

Si une requête est envoyée, celle-ci passe par une Adresse IP et un port particulier (il y a 65535 ports différents). Pour utiliser l'authentification Windows, plusieurs ports doivent être ouverts. Pour une authentification de base, seul un port est nécessaire.

Le port 80 est le port standard utilisé. Si une connexion via SSL est établie, le port 443 est utilisé par défaut. Si plusieurs serveurs dans le réseau local doivent être appelés de l'extérieur en utilisant la même adresse IP, différents ports doivent être utilisés pour chaque serveur (exemple ci-dessus : port 80 pour le site Web de l'entreprise et le port 88 pour FileDirector). Si des requêtes sont envoyées sur les adresses IP externes (e.g. 212.17.9.50:88), elles sont distribuées par le firewall vers les adresses IP internes.

Dans l'illustration ci-dessus, une adresse IP externe avec différents ports est configurée. Si le port 80 doit être utilisé pour toutes les applications, différentes adresses IP externes IP peuvent être utilisées. Ceci peut être configure en utilisant différentes cartes réseaux.

FileDirector avec un firewall

Connexion Interne : Authentification Windows :

Pour un réseau interne, l'authentification Windows est normalement utilisée. Pour l'authentification Windows plusieurs ports sont utilisés. Si les requêtes venant de l'extérieur accèdent au système, un seul port est normalement activé. Par ce port, l'authentification de base doit avoir lieu.

Connexion Externe : Authentification de base

Une connexion externe est effectuée via une authentification de base, car un seul port est nécessaire et, via le pare-feu, seuls les ports utilisés pour la communication doivent être ouverts. L'utilisateur doit se connecter avec son nom d'utilisateur et son mot de passe sur la page web demandée. Le compte de l'utilisateur doit être connu dans le RESEAU LOCAL.

Accès Externe avec connexion en authentification de base :

Si un utilisateur se connecte de l'extérieur pour accéder aux données du serveur FileDirector, le compte doit être connu dans le RESEAU LOCAL et doit être dans un des groupes FileDirector (fd-scan). (Comptes sur le contrôleur de domaine [6])

L’utilisateur appelle FileDirector en utilisant le WinClient [1] ou le WebServer [2] via Internet [3] et obtient une fenêtre de connexion.

Le Firewall [5] n’a qu’un port (80) ouvert [4], qui autorise seulement l’authentification de base. Dans IIS [7] l’authentification de base doit être permise.

L’authentification Windows peut être utilisée pour la connexion de clients internes [8] et [9]. Elle doit être aussi activée dans IIS [7].

Accès Externe sans connexion :

Si un utilisateur accède aux données du serveur FileDirector de l’extérieur sans s’être connecté ou sans avoir son propre compte dans le réseau, il peut utiliser une authentification anonyme. Un utilisateur Windows spécial pour l’accès anonyme est configuré. IIS fournit un compte par défaut ***IUSR_Servername*** pour l’accès anonyme.

Si ***IUSR_Servername*** doit être en mesure d’accéder aux données FileDirector, le compte doit être membre d’un des groupes FileDirector sur le domaine [6], par exemple fd-scan.

Dans IIS [7] l’accès anonyme est permis pour ce compte dans l’application FileDirectorWeb.

Si un utilisateur inconnu se connecte au WebServer [7], il doit se connecter avec le compte IUSR. Cet utilisateur anonyme est stocké dans le web.config par le ConfigUtility de sorte que le WebServer peut automatiquement l’utiliser.

Le Firewall [5] offre seulement un seul port ouvert (80) [4], qui autorise seulement l’authentification de base. Par conséquent l’authentification de base doit être permise dans IIS [7] pour l’application FileDirectorWeb.

Configuration en DMZ

Connexion via Internet (WebServer)

[1] L’utilisateur appelle le WebServer avec http://[external IP]/filedirector/web et obtient une fenêtre de connexion.

[2] Le Firewall a un seul port ouvert (80), permettant l’authentification de base.

[3] Dans IIS, pour l’application ‘FileDirectorWeb’, seule l’authentification de base est autorisée. Sur le serveur [3] un compte local ‘fd-server’ avec le même mot de passe que sur le serveur FileDirector [on 6] doit être créé pour s’assurer que le cache local du WebServer externe [4] peut être contrôlé.

[4] Puisque l’utilisateur doit se connecter avec un compte connu de FileDirector, aucun compte ne devrait être spécifié dans le WebServer.

[5] Le Firewall est configuré avec le port 80 pour l’authentification de base.

[6] Sur l contrôleur de domaine, le compte connecté doit être connu et être membre d’un des groupes FD (par exemple fd-scan).

[7] Le serveur FD connaît l’utilisateur connectée car il est membre d’un groupe FileDirector. Dans IIS, l’authentification de base doit être activée.

[8] Pour la connexion d’un client interne, l’authentification Windows peut être utilisée. Elle doit aussi être activée dans IIS [7] pour l’application ***FileDirector***.

[10] Pour l’utilisation interne du WebServer, un WebServer interne [10] devrait être paramétré. Pour une option de connexion interne à Windows, l’***authentification Windows*** peut être définie dans IIS [7] pour l’application ***FileDirectorWeb***.

Réglages DMZ dans Enterprise Manager

Lors de la transmission de données, seules les commandes spécifiques à exécuter devraient être permises. Pour permettre cela dans FileDirector, le mode DMZ peut être activé où juste les commandes sélectionnées peuvent être autorisées.

Les réglages peuvent être configurés dans Enterprise Manager :

Configuration Système → serveur → actif → sélectionnez le serveur → réglages → Réglages DMZ