

Bintec Solution – Stateful Inspection Firewall (3): Externer Verbindungsaufbau über vorgegebene Portnummer

Die Stateful Inspection Firewall (SIF) von Bintec bietet die Möglichkeit, alle von außen initiierten Verbindungen prinzipiell zu blockieren. Dies bietet zwar einen hohen Sicherheitsgrad, verhindert aber die Kommunikation mit externen Diensten, die von sich aus eine initiale Verbindung aufbauen müssen. Um dennoch mit solchen Applikationen kommunizieren zu können bietet die SIF die Funktion, diesen Diensten eine definierte Portnummer mitzuteilen, die für die Durchlassung solcher Anwendungen auf der Firewall konfiguriert ist. Dieses Verhalten soll am Beispiel des FTP Dienstes verdeutlicht werden (vgl. Abbildung 1): Die Clients des lokalen Netzes benötigen den Zugriff auf einen entfernten FTP Dienst. Für den eigentlichen Datentransfer müsste der FTP Server von sich aus eine Verbindung zum anfragenden Client aufbauen, die allerdings von der Firewall abgeblockt würde. Die SIF hingegen übermittelt nun dem FTP Server bei der ersten Anfrage des Clients die konfigurierte Portnummer, die der Server für den nachgelagerten Datentransfer zum Client zu benutzen hat. Hierdurch ist sichergestellt, dass diese Verbindung von der Firewall zum Client durchgelassen wird und der Download stattfinden kann.

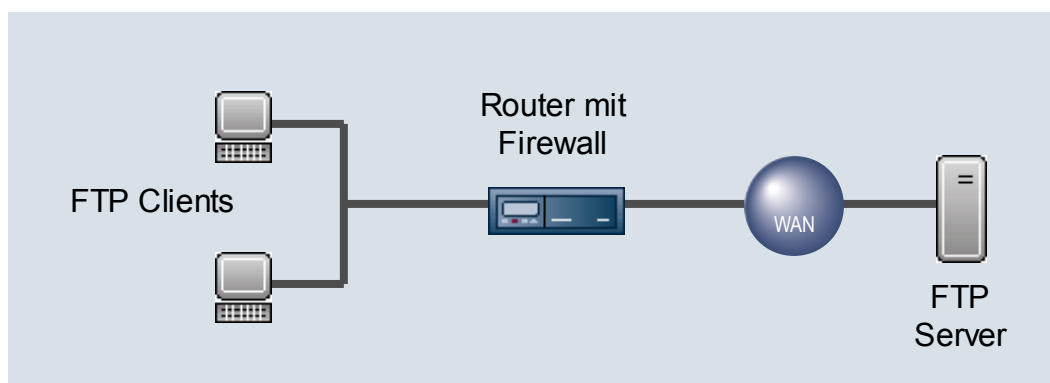


Abbildung 1: Verbindung zu einem externen FTP Server mittels SIF