Trong phần này, bạn sẽ được tìm hiểu về các tùy chọn cấu hình cụ thể cho từng loại dịch vụ lưu trữ dữ liệu trong Azure relational data services. Nguyên tắc chung cho bảo mật mạng của các dịch vụ cơ sở dữ liệu Azure sequel là chỉ cho phép kết nối và giao tiếp cần thiết để dịch vụ hoạt động. Tất cả các cổng, giao thức và kết nối khác đều bị chặn mặc định. Các mạng cục bộ ảo, hay VLANs, và danh sách kiểm soát truy cập, hay ACLs, được sử dụng để hạn chế giao tiếp mạng theo nguồn và đích, giao thức và số cổng. Một ACL chứa một danh sách các tài nguyên và các đối tượng, người dùng, máy tính và ứng dụng được phép truy cập vào các tài nguyên đó. Khi một đối tượng cố gắng sử dụng một tài nguyên được bảo vệ bởi một ACL, nếu nó không có trong danh sách, nó sẽ không được truy cập. Các mục triển khai ACL dựa trên mạng bao gồm các router và cân bằng tải. Bạn kiểm soát luồng dữ liệu thông qua các mục này bằng cách xác định các quy tắc tường lửa.

Bước tiếp theo mô tả cách thiết lập kết nối đến một cơ sở dữ liệu Azure SQL. Các client kết nối đến một cổng thông tin có địa chỉ IP công cộng và lắng nghe trên cổng 1433. Tùy thuộc vào chính sách kết nối hiệu quả, cổng thông tin này sẽ chuyển hướng lưu lượng tới cụm cơ sở dữ liệu hoặc hoạt động như một proxy cho cụm cơ sở dữ liệu. Lưu ý rằng Azure SQL database sử dụng mô hình cụm để cung cấp khả năng sẵn có cao. Mỗi máy chủ và cơ sở dữ liệu được sao chép một cách minh bạch để đảm bảo rằng một máy chủ luôn có sẵn ngay cả khi có sự cố với cơ sở dữ liệu hoặc máy chủ. Bên trong cụm cơ sở dữ liệu, lưu lượng được chuyển tiếp đến cơ sở dữ liệu Azure SQL phù hợp.

Nếu bạn kết nối từ bên ngoài Azure, chẳng hạn như một ứng dụng trên nền tảng, kết nối của bạn mặc định sẽ là thông qua proxy. Mỗi yêu cầu sau đó có thể được phục vụ bởi một cơ sở dữ liệu khác nhau trong cụm. Các cuộc tấn công từ chối dịch vụ hoặc DoS được giảm bớt bằng một dịch vụ Gateway SQL database gọi là DoSGuard. DoSGaurd theo dõi hoạt động đăng nhập thất bại từ các địa chỉ IP. Nếu có nhiều lần đăng nhập thất bại từ một địa chỉ IP cụ thể trong một khoảng thời gian, địa chỉ IP đó sẽ bị chặn khỏi việc truy cập bất kỳ tài nguyên nào trong dịch vụ trong một thời gian ngắn.

Ngoài ra, Gateway SQL database Azure thực hiện các nhiệm vụ sau:

* Xác thực tất cả các kết nối đến máy chủ cơ sở dữ liệu để đảm bảo rằng chúng đến từ các client thực sự.
* Mã hóa tất cả các giao tiếp giữa một client và các máy chủ cơ sở dữ liệu.
* Kiểm tra từng gói mạng được gửi qua một kết nối client.

Khi bạn tạo máy chủ cơ sở dữ liệu Azure cho PostgreSQL, một cơ sở dữ liệu mặc định có tên là Postgre được tạo để kết nối đến máy chủ cơ sở dữ liệu của bạn. Bạn cần tên máy chủ đầy đủ và thông tin đăng nhập quản trị viên. Bạn có thể dễ dàng tìm thấy thông tin máy chủ và thông tin đăng nhập trên trang tổng quan máy chủ trong cổng thông tin.

Kết nối đến máy chủ cơ sở dữ liệu Azure cho PostgreSQL của bạn truyền qua cổng 5432. Khi bạn cố gắng kết nối từ bên trong một mạng doanh nghiệp, lưu lượng ra cổng 5432 có thể không được phép bởi tường lửa mạng của bạn. Trong trường hợp này, bạn không thể kết nối tới máy chủ của mình trừ khi bộ phận CNTT mở cổng 5432.