Best Practices For Firewall Rules Configuration

When you change a firewall configuration, it’s important to consider potential security risks to avoid future issues.

Block By Default

Block all traffic by default and explicitly enable only specific traffic to known services.

- This strategy provides good control over the traffic and reduces the possibility of a breach because of service misconfiguration.

You achieve this behavior by configuring the last rule in an access control list to deny all traffic. You can do this explicitly or implicitly, depending on the platform.

Specify Source IP Address

If the service should be accessible to everyone on the internet, then any source IP address is the correct option.

- In all other cases, you should specify the source address.

It’s acceptable to enable all source addresses to access yout HTTP server, it’s not acceptable to enable all source addresses to access your server management ports or database ports.

- The list below is of common server management ports and database ports:
    - Server Management Ports:
    - Linux SSH: Port 22
    - Windows RDP: Port 3389
        - Database Ports:
        - SQL Server - Port 1433
        - Oracle: Port 1521
        - MYSQL: Port 2206

Be very, very specific about who can reach these ports.

Specify The Destination IP Address

The destination IP address is the server that runs the service to which you want to enable access.

- Always specify which server or servers are accessible.

- Configuring a destination value of any could lead to a security breach or server compromise of an unused protocol that might be accessible by default.

- However, destination IPs with a destination value of any can be used if there is only one IP assigned to the firewall.

Examples of Dangerous Configurations

Permit IP to any - Allows all traffic from any source on any port to any destination.

- This is the worst type of access control rule. It contradicts both of the security concepts of denying traffic by default and the principle of the least privilege.
    - The destination port should always be specified, and the destination IP address should be specified when practical. The source IP address should be specified unless the app is built to receive clients from the internet, such as a web server.
        - A good rule would be permit tcp any WEB-SERVER1 http.

Permit IP any any WEB-SEVER1 - Allows all traffic from any source to a web server.

- Only specific ports should be allowed; in the case of a web server, ports 80 (HTTP) and 443 (HTTPS). Otherwise, the management server is vulnerable.
    - A good rule would be Permit IP any WEB-SERVER1 http.

Example of Dangerous Configurations (Part 2)

Permit tcp any WEB-SERVER1 3389 - Allows RDP access from any source to the web server.

- It’s a dangerous practice to allow everyone access to your management ports. Be very specific about who can access the server management.
    - A good rule would be Permit tcp 12.34.56.78 administrator’s computer on the internet.

Permit tcp any DB-SERVER1 3306 - Allows MYSQL access from any source to the database.

- Database servers should never be exposed to the whole internet. If you need database queries to run across the public internet, specify the exact source IP address.
    - A good rule would be permit tcp 23.45.67.89 DB-SERVER1 3306 (where 23.45.67.89 is the IP address of the host on the internet that needs access to the database)
        - A best practice would be to allow database traffic over a VPN and not in clear text across the public internet.