GAJSHIELD

Data Security Firewall

How to create firewall rules to access local server from the internet (destination NAT (DNAT) rule) or port forwarding

How to create firewall rules to access local server from the internet (destination NAT (DNAT) rule) or port forwarding

A destination NAT rule redirects traffic that is sent to a specified destination. There may be times you may want to allow access to your servers from the internet, without providing these servers with a valid internet address.

Prerequisites before starting:

Source IP Address: The IP address from where your server would be accessed from the WAN. This could be a single address, network address or any IP address from the internet.

From Interface: This interface is configured with the public IP address of the server.
To Interface: The interface on which your local server is connected.

Service: Port or service you want to allow access (specify the port no. on which your local server is listening)

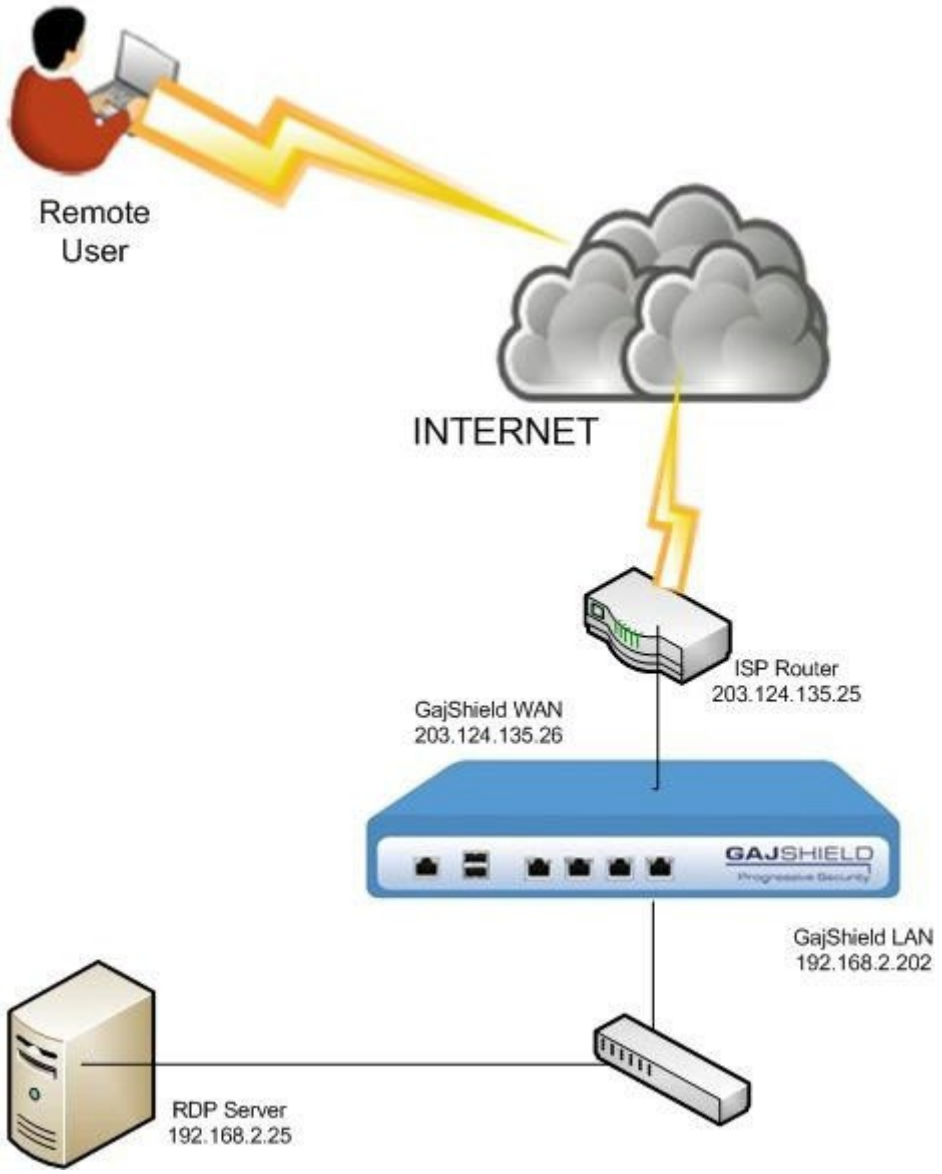
Note: If services not part of standard service list, create the service at Definitions -> Protocols and Services -> Services

Destination IP Address: This is the public address on which your server is accessed from the WAN.

Note: This IP address should belong to the firewall either on the firewall interface or through an alias IP address.

Nat Address: The IP address to the server you want to redirect traffic to. Note: Create hosts for all the required above IP addresses.

Example: This example creates a DNAT rule that allows Remote Desktop Server (RDP) traffic for a specific user from the internet to the local RDP server.



Pre-requisites in our example:

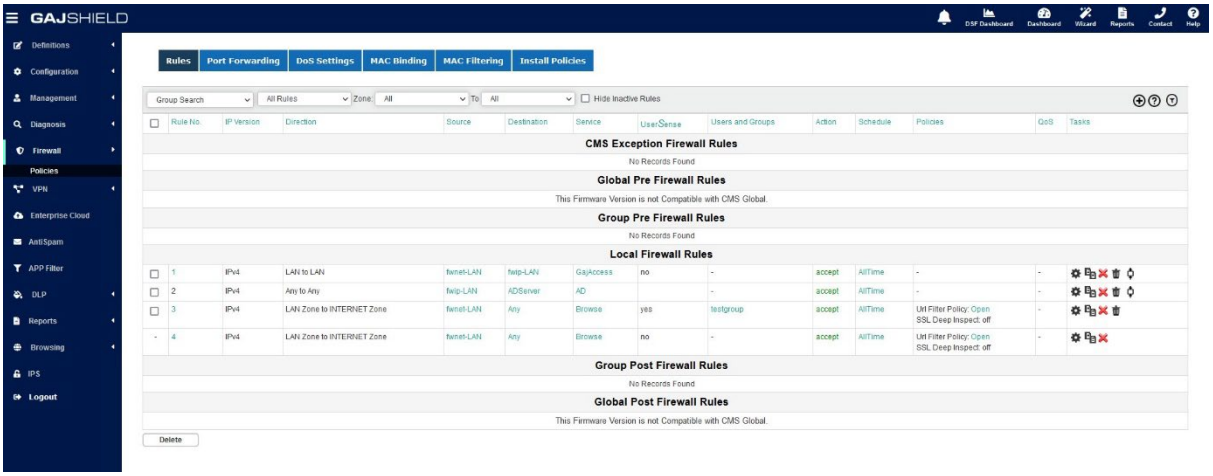
Source – ANY (because we want to allow access to anyone).
From interface – WAN
To interface – LAN
Service – remote-desktop (TCP port 3389)
Destination –

1) Public IP-203.124.135.26 used to access the RDP server for the Internet.
2) Private IP-192.168.2.25 of the RDP server to which the traffic is redirected.

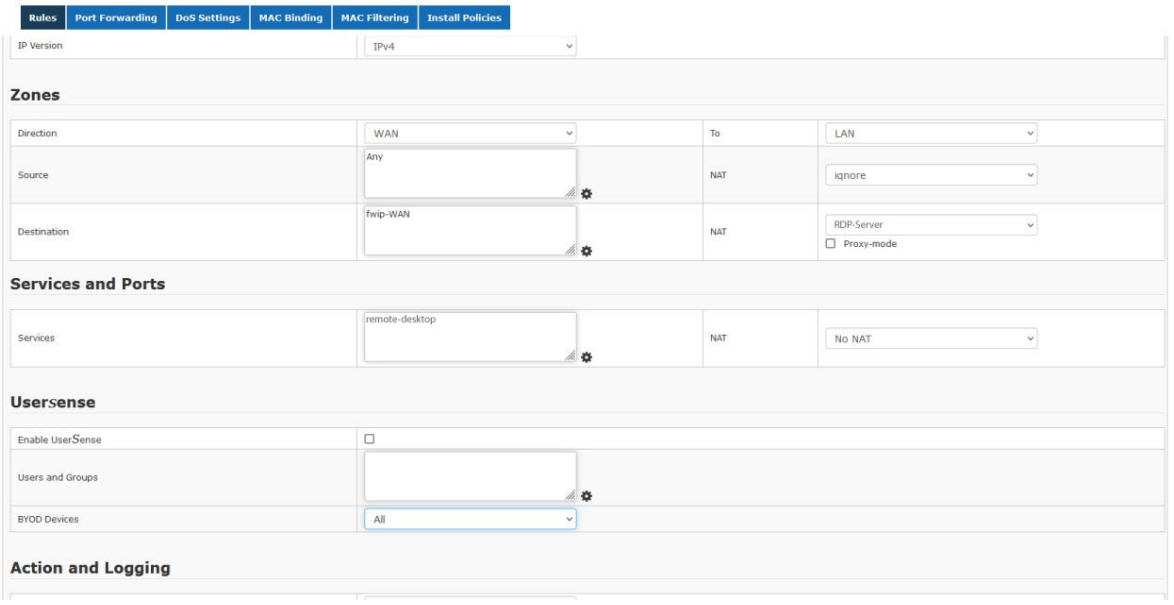
Configuration:
Step 1:
To allow remote user RDP access to local server, we need to create a firewall rule. Before

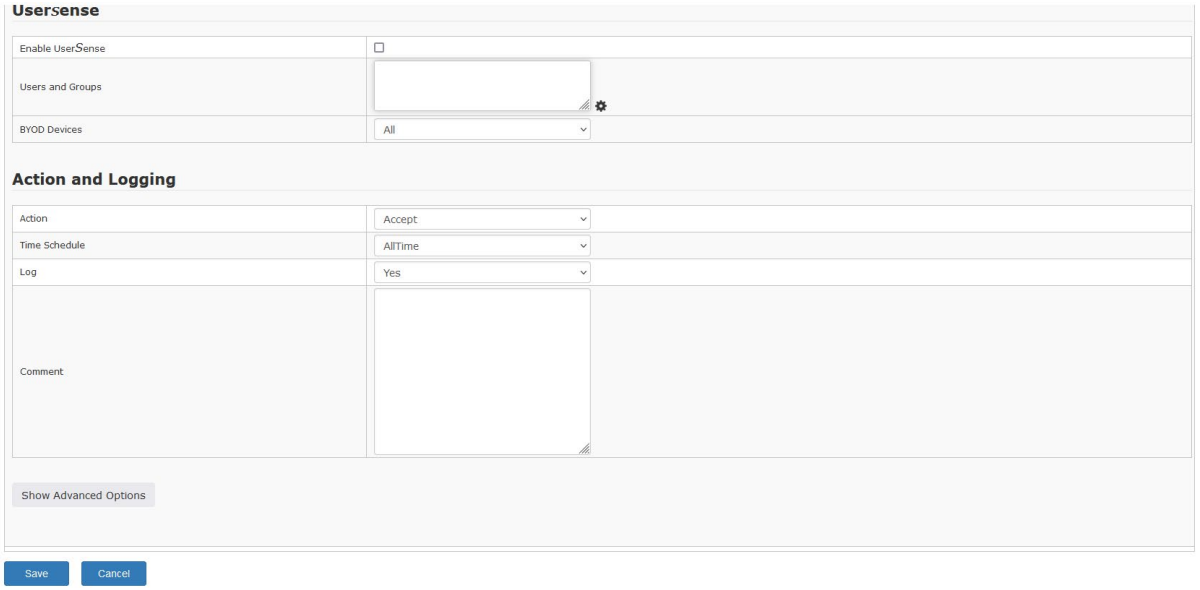
creating a firewall rule, it is important to define the required network objects. These can be added at Definitions -> Hosts
Refer to the following steps to know how to create a network object in GajShield firewall.

Step 2:
Add the required firewall rule.
To ADD firewall rule, go to Firewall –> Policies –> Rules –> Click on + button to add new firewall rule.



Step 3:
As per the pre-requisite in our example, you must add the firewall rule as specified in the below snapshot.





Configure the above rule as follows:

Direction: From WAN (Interface on which the public IP address is configured) To LAN (Interface to which the RDP server is connected)

Note: Servers should be kept in DMZ instead of your Private Network for better security

Source: We have selected ANY since we need to provide access from the Internet

Destination: Public Address used to access RDP server from the Internet

Destination-NAT: Address to which the traffic is directed (configured on the RDP Server)

Services: The service or port access from the Internet. In this case, it is configured as remote-desktop

Step 4: Once the rule is configured, to apply it, we need to install firewall policy. To do so, go to Firewall – >Policies – >Install Policies.

Trouble-Shooting

Even after creating the above rule, if you are unable to access your internal server on the required port, check the following,
Go to Live firewall logs and check whether the relevant traffic shows 'pass' or 'dropped' in the action column. If the packet gets dropped, check the following,

Is the direction of the rule properly defined? The 'From' direction should be the interface to which your ISP is connected and the 'To' direction should be the interface on which your server or application is connected.

Destination address should be the mapped to the internet IP address of your server and the Destination Nat should be the local IP address of your server.

Check other parameters like service
If the packet is passed, check the following:
Does the destination address shown in the Live Firewall Log correspond to your Internal server address? if not, check the rule again and correct it.

The default gateway of the internal server must be the firewall address. If not, set the default gateway to the firewall.

If a firewall is enabled on your server, ensure that it allows the packets, on the port forwarded, from the internet.

You have successfully created firewall rules to access local server from the internet.