DNS forwarding for clusters with and without NAT

When using TightGate-Pro, the TightGate-Viewer establishes a connection to the TightGate server. It does this by attempting to establish a connection via the name of the TightGate server. The request is first sent to the name server in the network. This resolves the requested name to the IP address of TightGate-Pro, gives this IP to the TightGate-Viewer he can establish the connection. To make this possible, a number of prerequisites must be met in the infrastructure. The following instructions explain how the interaction between TightGate-Viewer, DNS server and TightGate-Pro server works.

DNS for individual systems

The DNS query is easily answered for TightGate-Pro single systems, as there is a simple 1:1 conversion from the requested name to the IP address.

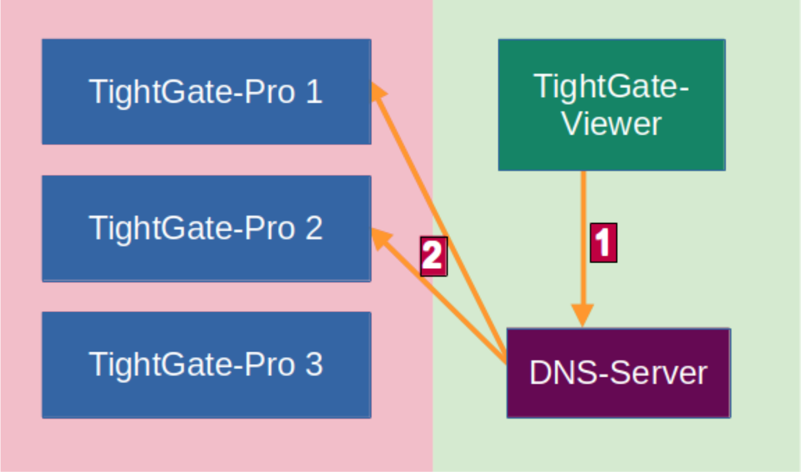
DNS for clusters

For cluster systems, things get a little more complicated, as there are several servers behind the requested name from TightGate-Pro. At this point, the requested name server must enquire in advance which TightGate-Pro servers are available for the requested name. For this purpose TightGate-Pro clusters use DNS zone forwarding for this purpose. DNS zone forwarding ensures that the DNS server receives feedback from the TightGate-Pro cluster at all times as to which TightGate-Pro servers are currently available for connection requests.

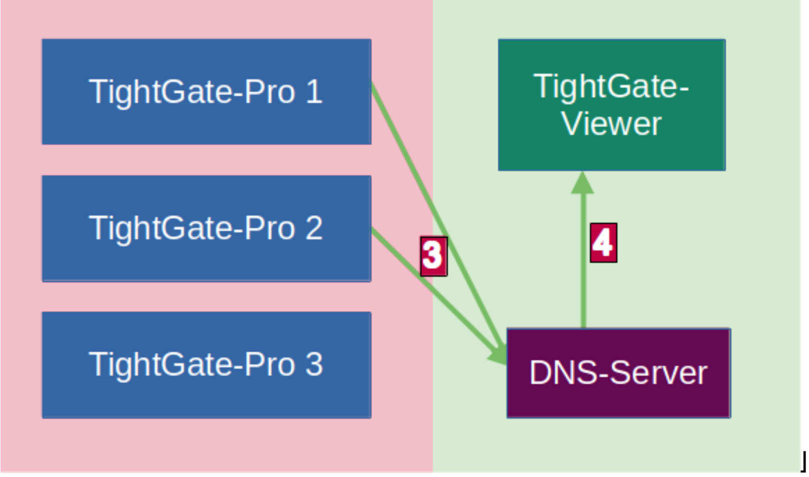
The following example illustrates the schematic structure of the connection request:

- DNS name of TightGate-Pro → internet.intern.netz
- TightGate-Pro cluster with 3 TightGate-Pro servers
- TightGate-Pro 1 (load balancer)
- TightGate-Pro 2 (load balancer)
- TightGate-Pro 3

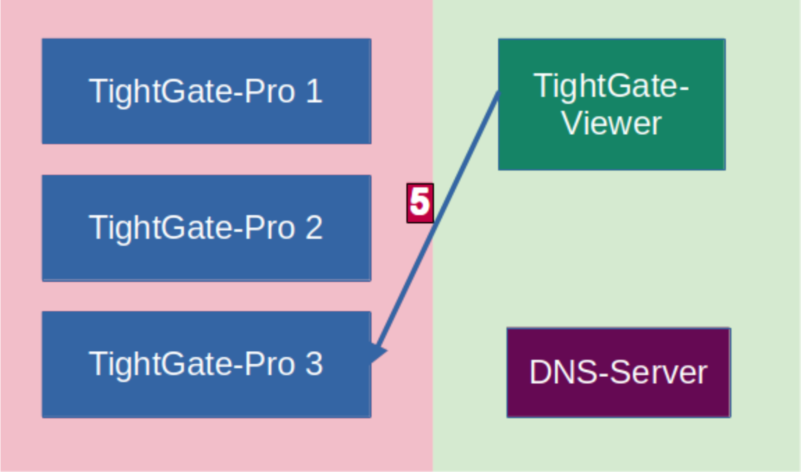
The prerequisite is DNS zone forwarding for the domain **internet.intern.netz** on the local DNS server, in which the first two TightGate-Pro servers (load balancers) are used as the **IP address of the master server** must be entered. The following figure illustrates the communication:



In step **1** the TightGate-Viewer asks the DNS server to which IP it should connect if it wants to connect to the server with the name **internet.intern.netz** server. The DNS server cannot answer this enquiry itself, but asks in step **2** the load balancers of the TightGate-Pro cluster (in the example TightGate-Pro 1 and 2) which servers are available.



In response, the DNS server in step **3** the response from the TightGate-Pro load balancer as to which TightGate-Pro servers are available (in the example TightGate-Pro 1 and 3). From this response, the DNS server selects one (in the example TightGate-Pro 3) and returns it in step **4** to the TightGate-Viewer in step 4.



In step **5** the TightGate-Viewer makes a connection request to the IP address of the returned TightGate-Pro server.

DNS for clusters with NAT

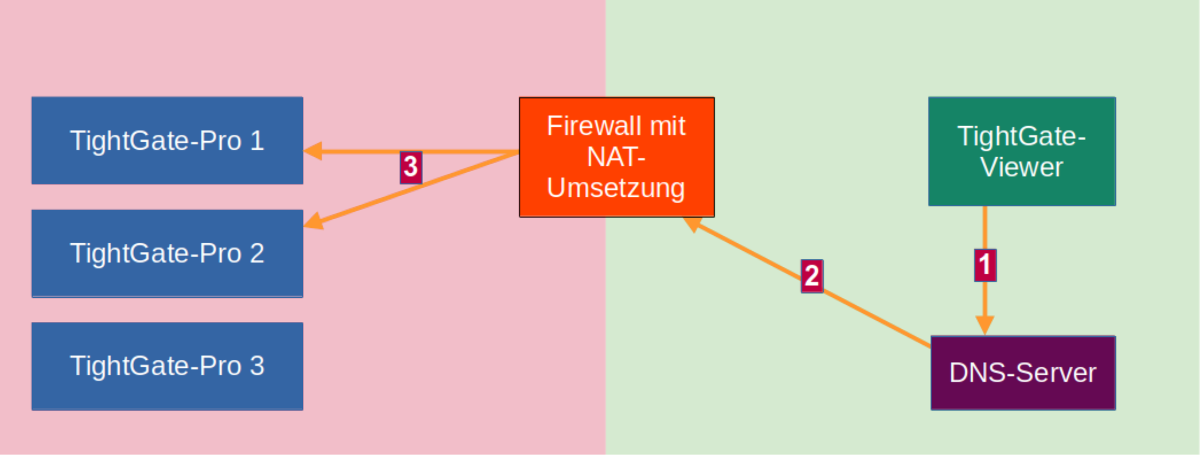
Things get a little more complicated if there is a NAT conversion between the internal network where the TightGate-Viewer is started and the network in which the TightGate-Pro servers are located. In this case, the internal name server cannot simply query the TightGate-Pro cluster for the available TightGate-Pro servers, as the NAT conversion prevents this. However, in order to be able to use the load balancing of TightGate-Pro here, it is necessary for the NAT translator to also perform the DNS query of the available TightGate-Pro servers and make the result available to the internal DNS.

The following example illustrates the schematic structure of the connection request:

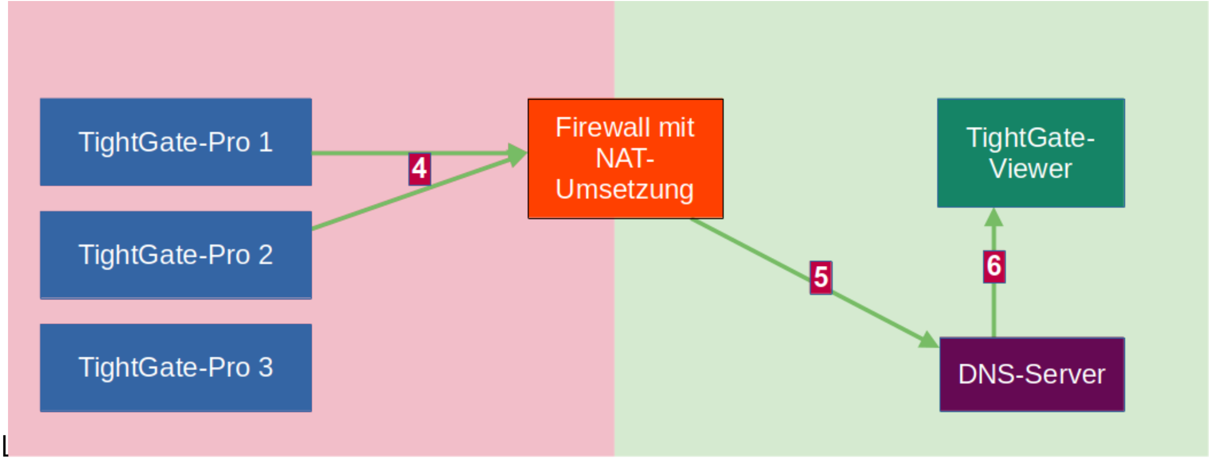
DNS name of TightGate-Pro → internet.intern.netz TightGate-Pro Cluster with 3 TightGate-Pro servers and the following features:

Server	IP address NAT	IP address LAN	Load balancer
TightGate-Pro 1	10.10.10.100	192.168.1.100	yes
TightGate-Pro 1	10.10.10.101	192.168.1.101	yes
TightGate-Pro 1	10.10.10.102	191.168.1.102	no

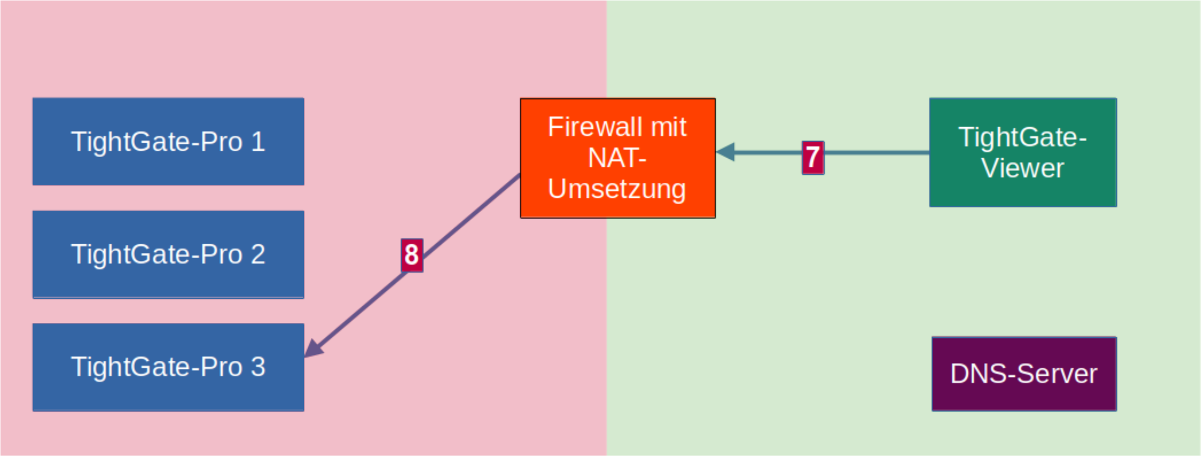
In this case, DNS zone forwarding is required for the domain **internet.intern.netz** must be set up on the local DNS server and the IP address of the NAT translator must be used as the **IP address of the master server** must be entered. The following figure illustrates the communication:



In step **1** the TightGate-Viewer asks the DNS server to which server it should connect if it wants to connect to the server with the name **internet.intern.netz** name. However, the DNS server cannot answer this request itself and also cannot directly query the TightGate-Pro load balancers as it cannot reach them directly. It must therefore send the request in step **2** with the internal IP address of one of the two TightGate-Pro load balancers (192.168.1.100 or 192.168.1.101 in the example) to the DNS translator. For its part, the DNS translator must be configured to act as a DNS forwarder for the domain **internet.intern.netz** domain and, for its part, is configured in step **3** the load balancers of TightGate-Pro with their NAT addresses (in the example 10.10.10.100 or 10.10.10.101) according to the available IP addresses for the domain **internet.intern.netz** domain.



The TightGate-Pro load balancers respond in step **4** to the DNS translator which TightGate-Pro servers are currently available. In doing so, TightGate-Pro immediately returns the correct **LAN IP addresses** (in the example TightGate-Pro 1 and 3, which corresponds to the IP addresses 192.168.1.100 and 192.168.1.103). The DNS converter forwards these addresses in step **5** to the internal DNS server, which forwards them in step **6** to the TightGate-Viewer.



The TightGate-Viewer can now be opened in step **7** make a connection request with the correct LAN address of the available TightGate-Pro server (192.168.1.103 in the example). The NAT converter knows that the address must be NAT converted to the NAT address of TightGate-Pro 3 (10.10.10.103 in the example) and establishes the connection in step **8** establishes the connection.

Hinweis

Special configuration for TightGate-Pro clusters with NAT implementation: As ***config*** under **Cluster > Sub-cluster > Client base NAT/alias IP** enter the first LAN IP of TightGate-Pro, which TightGate-Pro delivers to the requesting DNS server. TightGate-Pro then automatically increments the LAN IPs.