DNS-Weiterleitung bei Clustern mit und ohne NAT

Bei der Nutzung von TightGate-Pro baut der TightGate-Viewer eine Verbindung zum TightGate-Server auf. Dies tut er, indem er versucht, eine Verbindung über den Namen des TightGate-Servers aufzubauen. Die Anfrage geht dabei zuerst zum Nameserver im Netzwerk. Dieser löst den angefragten Namen zu der IP-Adresse von TightGate-Pro auf, gibt diese IP dem TightGate-Viewer und dieser kann dann die Verbindung aufbauen. Um das zu ermöglichen, müssen in der Infrastruktur einige Voraussetzungen gegeben sein. Die nachfolgende Anleitung verdeutlicht, wie das Zusammenspiel aus TightGate-Viewer, DNS-Server und TightGate-Pro Server funktioniert.

DNS bei Einzelsystemen

Für TightGate-Pro Einzelsysteme ist diese DNS-Anfrage recht einfach beantwortet, da es eine einfache 1:1 Umsetzung von angefragtem Namen zur IP-Adresse gibt.

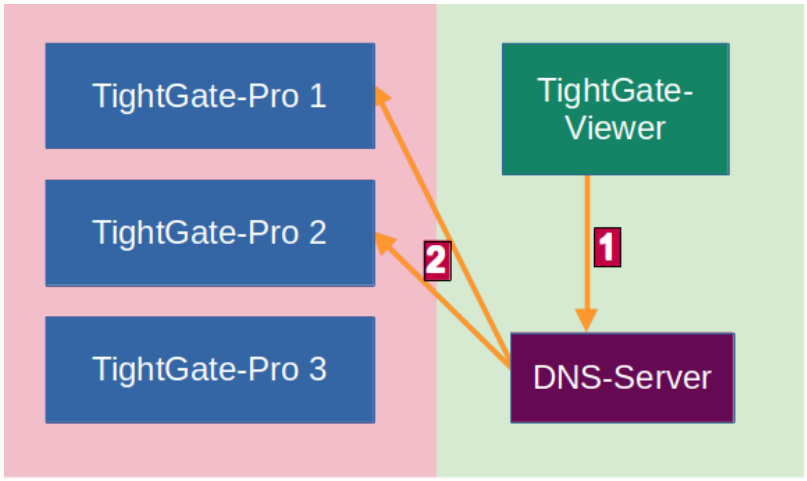
DNS bei Clustern

Für Cluster-Systeme wird es schon etwas komplizierter, da sich hier hinter dem angefragten Namen von TightGate-Pro mehrere Server verbergen. An dieser Stelle muss der angefragte Nameserver sich vorab selber erkundigen, welche TightGate-Pro Server zu dem angefragten Namen zur Verfügung stehen. Zu diesem Zwecke wird bei TightGate-Pro Clustern ein DNS-Zonen-Forwarding verwendet. Das DNS-Zonen-Forwarding dient dazu, dass der DNS-Server jederzeit vom TightGate-Pro Cluster eine Rückmeldung bekommt, welche TightGate-Pro Server gerade für Verbindungsanfragen verfügbar sind.

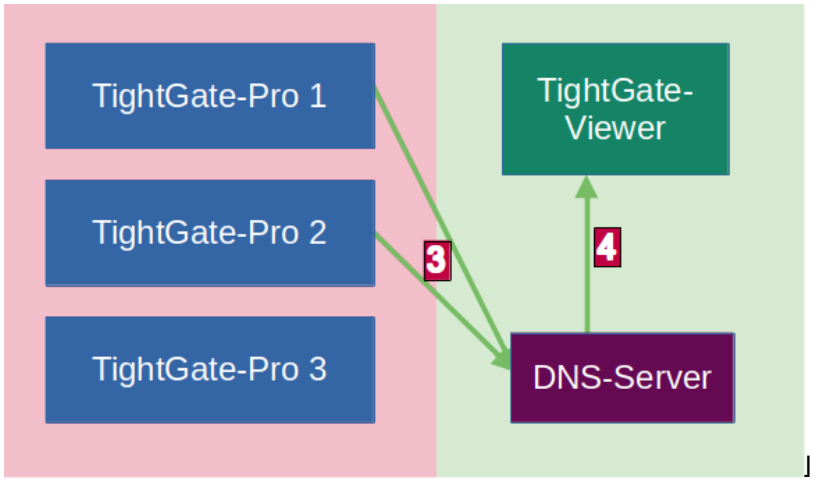
Das nachfolgende Beispiel verdeutlicht den schematischen Aufbau der Verbindungsanfrage:

- DNS-Name von TightGate-Pro → internet.intern.netz
- TightGate-Pro Cluster mit 3 TightGate-Pro Servern
- TightGate-Pro 1 (Loadbalancer)
- TightGate-Pro 2 (Loadbalancer)
- TightGate-Pro 3

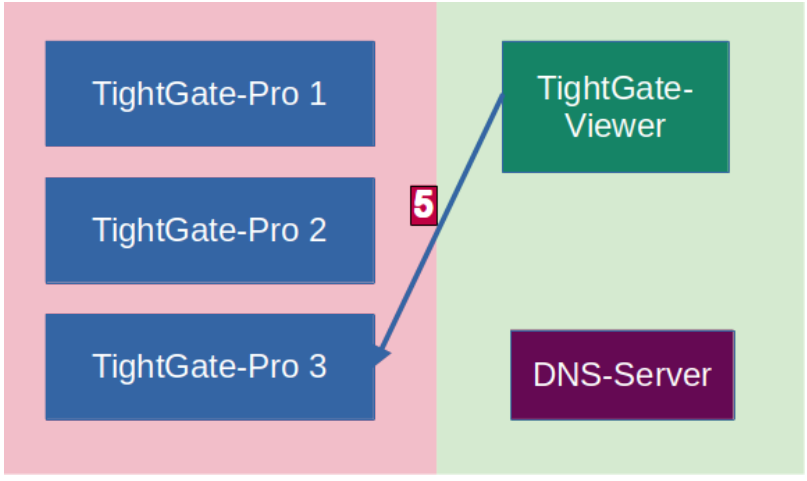
Voraussetzung ist ein DNS-Zonen-Forwarding für die Domäne **internet.intern.netz** am lokalen DNS-Server, bei dem die ersten beiden TightGate-Pro Server (Loadbalancer) als **IP-Adresse der Masterserver** einzutragen sind. Nachfolgende Abbildung verdeutlicht die Kommunikation:



Im Schritt **1** fragt der TightGate-Viewer den DNS-Server an, zu welcher IP er sich verbinden soll, wenn er eine Verbindung zum Server mit dem Namen **internet.intern.netz** aufbauen möchte. Diese Anfrage kann der DNS-Server nicht selber beantworten, sondern befragt im Schritt **2** die Loadbalancer des TightGate-Pro Clusters (im Beispiel TightGate-Pro 1 und 2), welche Server zur Verfügung stehen.



Als Antwort bekommt der DNS-Server in Schritt **3** die Antwort vom TightGate-Pro Loadbalancer, welche TightGate-Pro Server zur Verfügung stehen (im Beispiel TightGate-Pro 1 und 3). Aus dieser Antwort wählt der DNS-Server einen aus (im Beispiel TightGate-Pro 3) und gibt diesen im Schritt **4** an den TightGate-Viewer weiter.



Im Schritt **5** stellt der TightGate-Viewer eine Verbindungsanfrage zur IP-Adresse des zurückgegebenen TightGate-Pro Servers.

DNS bei Clustern mit NAT

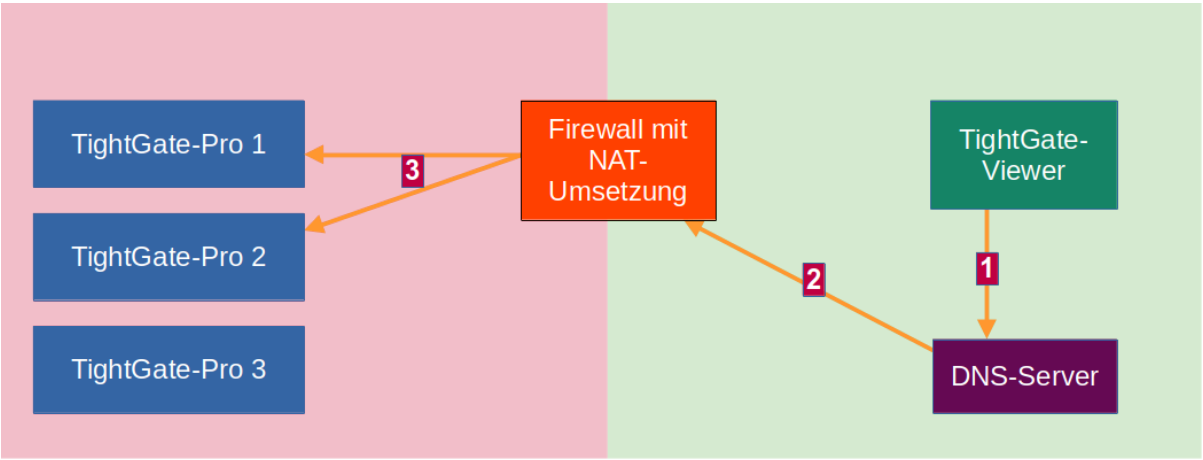
Etwas komplizierter wird es, wenn zwischen dem internen Netzwerk, wo der TightGate-Viewer gestartet wird, und dem Netz, in dem sich die TightGate-Pro Server befinden, noch eine NAT-Umsetzung stattfindet. Hier kann der interne Nameserver nicht einfach den TightGate-Pro Cluster nach den verfügbaren TightGate-Pro Servern befragen, da die NAT-Umsetzung dies verhindert. Um hier aber das Loadbalancing von TightGate-Pro verwenden zu können, ist es notwendig, dass der NAT-Umsetzer auch die DNS-Abfrage der verfügbaren TightGate-Pro Server durchführt und das Ergebnis dem internen DNS zur Verfügung stellt.

Das nachfolgende Beispiel verdeutlicht den schematischen Aufbau der Verbindungsanfrage:

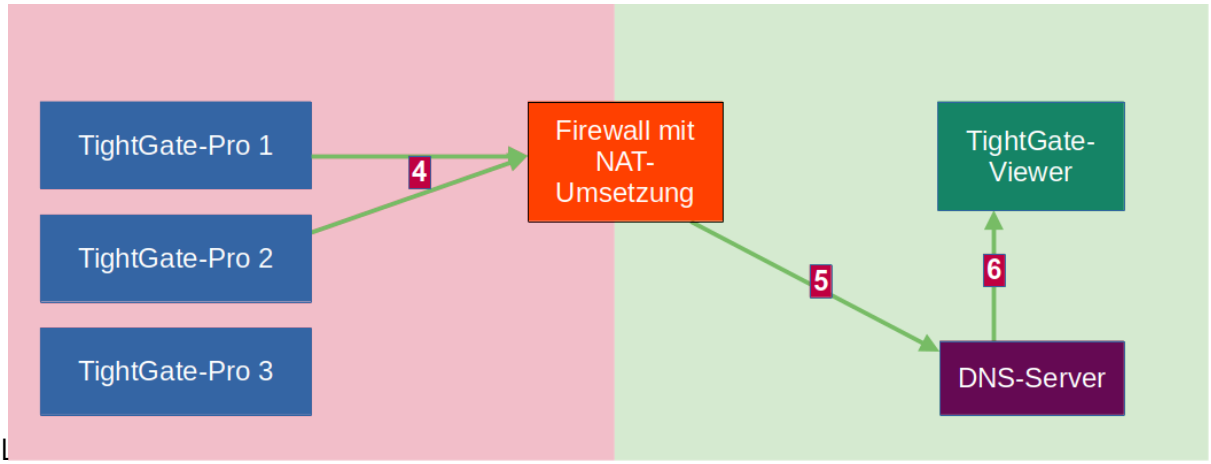
DNS-Name von TightGate-Pro → internet.intern.netz TightGate-Pro Cluster mit 3 TightGate-Pro Servern und folgenden Merkmalen:

Server	IP-Adresse NAT	IP-Adresse LAN	Loadbalancer
TightGate-Pro 1	10.10.10.100	192.168.1.100	ja
TightGate-Pro 1	10.10.10.101	192.168.1.101	ja
TightGate-Pro 1	10.10.10.102	191.168.1.102	nein

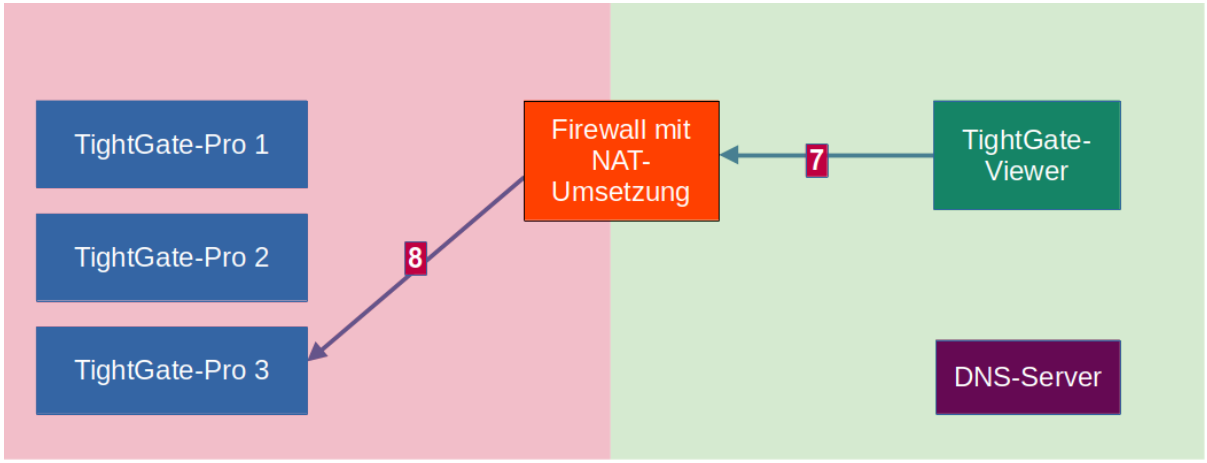
In diesem Fall ist ein DNS-Zonen-Forwarding für die Domäne **internet.intern.netz** am lokalen DNS-Server einzurichten und die IP-Adresse des NAT-Umsetzers als **IP-Adresse der Masterserver** einzutragen. Nachfolgende Abbildung verdeutlicht die Kommunikation:



Im Schritt **1** fragt der TightGate-Viewer den DNS-Server an, zu welchem Server er sich verbinden soll, wenn er eine Verbindung zum Server mit dem Namen **internet.intern.netz** aufbauen möchte. Diese Anfrage kann der DNS-Server aber nicht selber beantworten und auch nicht direkt die TightGate-Pro Loadbalancer befragen, da er diese nicht direkt erreicht. Er muss also die Anfrage im Schritt **2** mit der internen IP-Adresse einer der beiden TightGate-Pro Loadbalancer (im Beispiel 192.168.1.100 oder 192.168.1.101) an den DNS-Umsetzer weiter leiten. Der DNS-Umsetzer seinerseits muss so konfiguriert sein, dass er als DNS-Forwarder für die Domäne **internet.intern.netz** eingerichtet ist und seinerseits im Schritt **3** die Loadbalancer von TightGate-Pro mit deren NAT-Adressen (im Beispiel 10.10.10.100 oder 10.10.10.101) nach den verfügbaren IP-Adressen für die Domäne **internet.intern.netz** befragt.



Die TightGate-Pro Loadbalancer antworten im Schritt **4** dem DNS-Umsetzer, welche TightGate-Pro Server aktuell zur Verfügung stehen. Dabei gibt TightGate-Pro als Rückgabe auf die Anfrage gleich die richtigen **LAN-IP-Adressen** zurück (im Beispiel TightGate-Pro 1 und 3, was den IP-Adressen 192.168.1.100 und 192.168.1.103 entspricht). Diese Adressen leitet der DNS-Umsetzer im Schritt **5** an den internen DNS-Server und dieser weiter im Schritt **6** an den TightGate-Viewer.



Der TightGate-Viewer kann nun im Schritt **7** eine Verbindungsanfrage mit der richtigen LAN-Adresse des verfügbaren TightGate-Pro Servers stellen (im Beispiel 192.168.1.103). Der NAT-Umsetzer weiß, dass für die Adresse eine NAT-Umsetzung auf die NAT-Adresse von vom TightGate-Pro 3 (im Beispiel 10.10.10.103) zu erfolgen hat und stellt die Verbindung im Schritt **8** her.

Hinweis

Besondere Konfiguration bei TightGate-Pro Clustern mit NAT-Umsetzung: Als ***config*** unter **Cluster > Teil-Cluster > Klienten-Basis-NAT-/Alias-IP** ist die erste LAN-IP von TightGate-Pro anzugeben, welche TightGate-Pro dem anfragenden DNS-Server ausliefert. TightGate-Pro zählt die LAN-IPs dann automatisch hoch.