NCP
SECURE COMMUNICATIONS

Szenarien
high security remote access

NCP Secure High Availability Services

High Availability Services

Szenarien

NCP Hotline auf Abruf

Sie erreichen unsere NCP Experten unter folgenden Hotlines:

Kunden mit Hotline Service Vertrag
Sie erhalten sofortigen Support unter der vertraglich angegebenen Rufnummer.
Ihnen steht das komplette Serviceportfolio zur Verfügung.

Kunden ohne Hotline Service Vertrag
Sie können wählen zwischen:
Kostenpflichtige Service-Rufnummer 09001996800 (-,80 Euro / Minute)
E-Mail an support@ncp-e.com

Dienstleistungsauftrag (Berechnung nach Aufwand)
mit festen Reaktionszeiten und Zusatzservices.
Bitte nutzen Sie zur Anfrage das NCP Service-Formular von der Website
http://www.ncp-e.com/de/service-support/support.html

Sie möchten mehr über den NCP Hotline Service Vertrag wissen?
Bitte senden Sie eine E-Mail an:
vertrieb@ncp-e.com

Network
Communications
Products engineering GmbH

Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet http:// www.ncp-e.com
E-mail: info@ncp-e.com

Copyright

Hochverfügbarkeitssysteme

Die NCP Secure Enterprise High Availability Services sind Komponenten der ganzheitlichen NCP Enterprise Solution. Sie sorgen für die Hochverfügbarkeit eines oder mehrerer NCP Secure Enterprise Server und damit des Virtual Private Network eines Unternehmens.

Die High Availability Services können im Failsafe-Modus oder im Load Balancing-Modus eingesetzt werden, wobei zwei Verfahren, je nach Szenario auch gleichzeitig, genutzt werden können.

Das Verfahren, das mit dem NCP Secure Enterprise Client eingesetzt werden kann, beruht auf dem NCP DVE-Protokoll. Über dieses Protokoll, das der Enterprise Client unterstützt, kann der HA Server den jeweiligen Tunnelendpunkt des aktiven VPN Gateways übermitteln. NCP Entry Clients oder NCP SSL VPN Clients, die dieses Protokoll nicht unterstützen, werden nach dem Prinzip des VRRP-Technik (Virtual Router Redundancy Protocol) mit der IP-Adresse des aktiven VPN Gateways versorgt.

Das vorliegende Dokument beschreibt diese Verfahren (siehe Tabelle unten) und deren Einsatz mit unterschiedlichen Client-Systemen und ergänzt die Szenarios mit Konfigurationsbeispielen.

Client-Systeme	**HA-System mit optionaler VRRP-Unterstützung**	
NCP Enterprise Client mit DVEP	FS-Modus	plus LB-Modus
NCP SSL VPN Client ohne DVEP	FS-Modus mit VRRP	plus LB-Modus
NCP Entry Client* ohne DVEP	FS-Modus mit VRRP	

** auch 3rd Party Clients*

Failsafe-Modus

Der Failsafe-Modus wird realisiert mit zwei Gateways, dem FS Primary und dem FS Secondary, und, um auch hier Ausfallsicherheit zu gewährleisten, mit zwei HA Servern, dem ersten und dem zweiten HA Server. (Die Lizenzen hierfür sind im Standardlieferumfang enthalten.)

Um die dauerhafte Verfügbarkeit eines einzelnen Enterprise Servers sicherzustellen, erfolgt die Installation des zweiten VPN Gateways (Enterprise Servers) im gleichen Ausbau wie das Master-System. Die Konfigurationen des beiden Gateways müssen dabei identisch sein. Das zweite Gateway hat ausschließlich Backup-Funktion (Hot Standby) und kommt nur im Fehlerfall oder bei Service-Abschaltung des ersten VPN Gateways zum Einsatz.

Failsafe-Modus mit DVEP

Um den DVE (dynamischen VPN-Endpunkt) für den Failsafe-Modus nutzen zu können, müssen remote-seitig NCP Enterprise Clients (DVE Client) eingesetzt sein und zentral-seitig zwei VPN Gateways installiert sein, sowie die HA Server Software mit HA Server Manager. Pro Rechner mit jeweils einem VPN Gateway und einem HA Server wird eine offizielle IP-Adresse benötigt.

(Zu Installation und Konfiguration der Server-Komponenten beachten Sie bitte die Beschreibung “HA-Installation”.)

Funktionsablauf

(Beachten Sie hierzu unten Fig. 1)

Im Failsafe-Modus ist immer nur ein System aktiv. Gemäß der Installation der Server-Komponenten ist dies der erste HA Server und das FS Primary Gateway. Das Secondary Gateway wird bis zur Aktivierung durch den HA Server nicht genutzt.

(1) Der Enterprise Client verbindet sich zum aktiven HA Server und schickt einen DVE Request.
(2) Zur automatischen Ausfallsicherung wird zwischen den Server-Komponenten, Primary und Secondary Gateway, sowie erstem und zweitem HA Server, in einem zu konfigurierenden Abfrageintervall (Konfigurationsfeld “Allgemein” am HA-Manager) der Status abgefragt.
(3) Die externe IP-Adresse des in diesem Intervall aktiven Gateways wird dem Enterprise Client als DVE Response mitgeteilt.
(4) Nachdem der Enterprise Client die IP-Adresse erhalten hat, baut er eine Tunnel-Verbindung zum aktiven Gateway auf
(5) Über das aktive Gateway wird dem Client eine Adresse aus dem Firmennetz zugewiesen. Dabei kann es sich entweder um eine Pool IP-Adresse handeln, oder um eine feste IP-Adresse. (Konfigurationsfeld “Link-Profile / Routing” am Web-Interface).

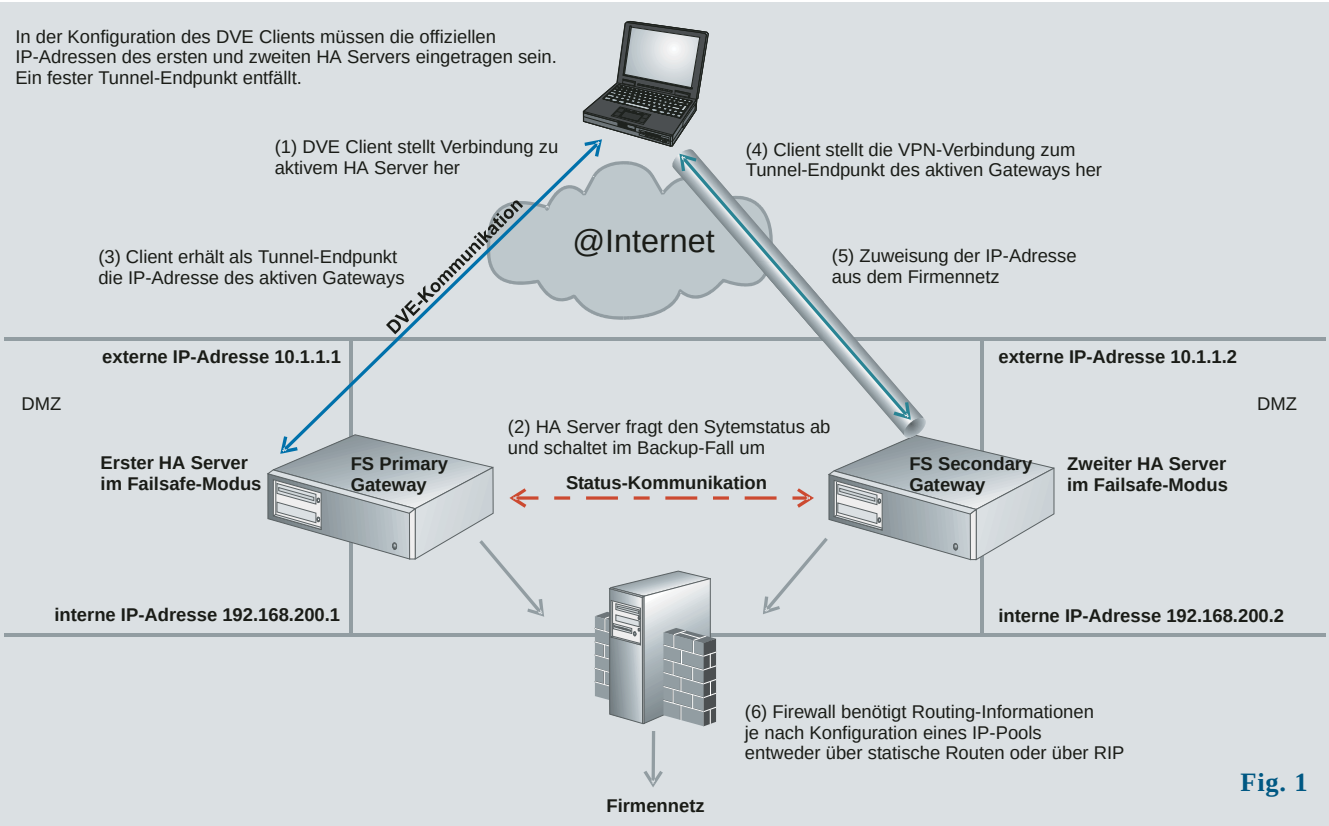


Fig. 1

Pool IP-Adressen

Soll für die Dauer einer Session eine Pool IP-Adresse an die Clients vergeben werden, so wird empfohlen, sich gegenseitig ausschließende Pool-Bereiche an Primary und Secondary Gateway einzurichten. In diesem Fall genügt es, an der Firewall statische Routen entsprechend der Zuordnung von Gateway und Pool-Bereich zu konfigurieren. (Vgl. unten Fig. 1, 6)

Werden gleiche Pool-Bereiche an den Gateways konfiguriert, muss das Routing Information Protocol (RIP) zwischen Firewall und Gateway eingesetzt werden, um die Route der Datenkommunikation zwischen Client und Firmennetz eindeutig festlegen zu können. (Vgl. Fig. 1,6)

Feste IP-Adressen

Soll ein Client immer die gleiche feste IP-Adresse erhalten, unabhängig ob er über Primary oder Secondary Gateway verbunden ist, so müssen die konfigurierten Adressbereiche auf Primary und Secondary Gateway gleich sein, und die Firewall muss die RIP-Meldungen der Gateways verstehen, um die Datenkommunikation zwischen Client und Firmennetz in beide Richtungen über die IP-Adresse des jeweils aktiven Gateways sicherstellen zu können. (Vgl. Fig. 1, 6)

(Zur Zuweisung von IP-Adressen durch wechselnde Gateways siehe Abschnitt **Feste und dynamische IP-Adressen in Remote Access-VPNs**)

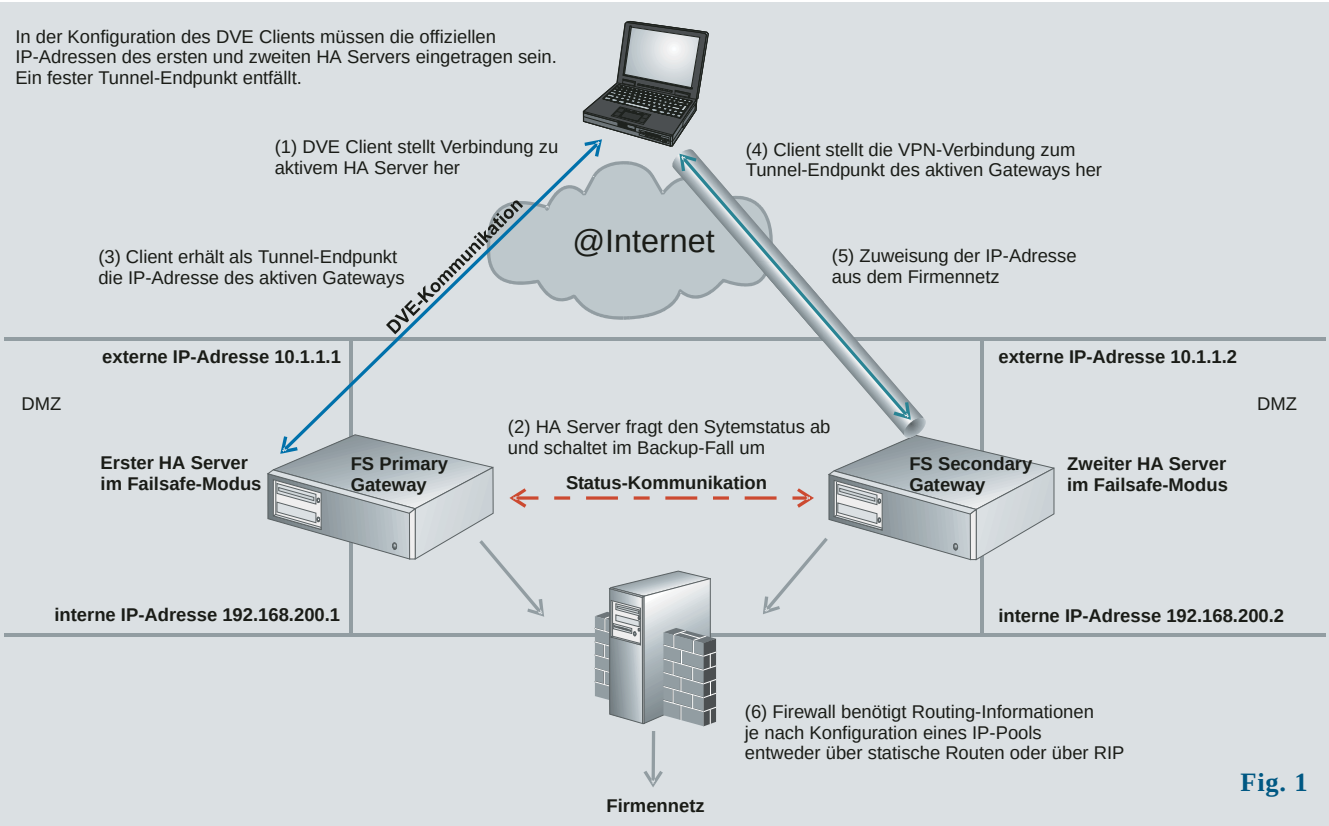


Fig. 1

Failsafe-Modus mit VRRP

Der VRRP-Betriebsmodus wurde entwickelt, um Hochverfügbarkeit über bereits bestehende HA-Systeme nicht nur für DVE Clients, sondern zusätzlich auch für Client-Systeme gewährleisten zu können, die das DVEP nicht unterstützen. NCP HA Server ab Version 1.08 und NCP Secure Server ab Version 6.11 unterstützen zusätzlich zu Failsafe und Load Balancing auch den VRRP-Betriebsmodus. (Zu Installation und Konfiguration der Server-Komponenten beachten Sie bitte die Beschreibung **HA-Installation**.)

Funktionsablauf

(Beachten Sie hierzu unten Fig. 2)

Die Funktion dieser Betriebsart entspricht einer Routing-Technik mit VRRP (Virtual Router Redundancy Protocol). Dabei werden die Gateways im Failsafe-Modus nicht mehr über zwei unterschiedliche externe IP-Adressen, sondern über nur eine gemeinsame IP-Adresse angesprochen. Die Zuordnung der gemeinsamen IP-Adresse erfolgt über die Netzwerkeinstellungen des Betriebssystems am jeweiligen Gateway.

(1) Beide Failsafe Gateways, die mit **Failsafe-Typ FS Master** und **FS Secondary** konfiguriert werden, fungieren zusammen als ein virtueller Router, der sich auf der externen Schnittstelle gegenüber dem Internet mit nur einer gemeinsamen offiziellen IP-Adresse darstellt. (Auch auf dem internen Netzwerk-Interface beider Gateways kann VRRP mit einer gemeinsamen IP-Adresse betrieben werden.)

(2) Diese gemeinsame IP-Adresse erlaubt den Verzicht auf die Konfiguration der IP-Adressen beider HA Server in den Client-Systemen, da die HA Server nicht mehr nach der Adresse des aktiven Gateways gefragt werden müssen. Statt dessen benötigt der Client nur noch einen VPN-Endpunkt, nämlich die offizielle IP-Adresse des virtuellen Routers, um die Verbindung zu dem darin enthaltenen aktiven Failsafe Gateway aufbauen zu können.

(3) Bei Einsatz der Gateways im VRRP-Modus wird der HA Server nicht mehr dazu benötigt, den jeweiligen VPN-Endpunkt des aktiven Gateways an den Client zu übermitteln, sondern nur zur Status-Überwachung und als Umschalter zwischen den Gateways im virtuellen Router.

(4) Zunächst übernimmt das vom HA Server als VRRP Master gesetzte Gateway (FS Primary) die gemeinsame IP-Adresse. Fällt das VRRP Master Gateway aus, wird die gemeinsame IP-Adresse vom HA Server an das VRRP Backup Gateway (FS Secondary) entsprechend einer gemeinsamen "VRRP ID" übergeben. (Beachten Sie dazu das Konfigurationsbeispiel zu FS-Modus mit VRRP.)

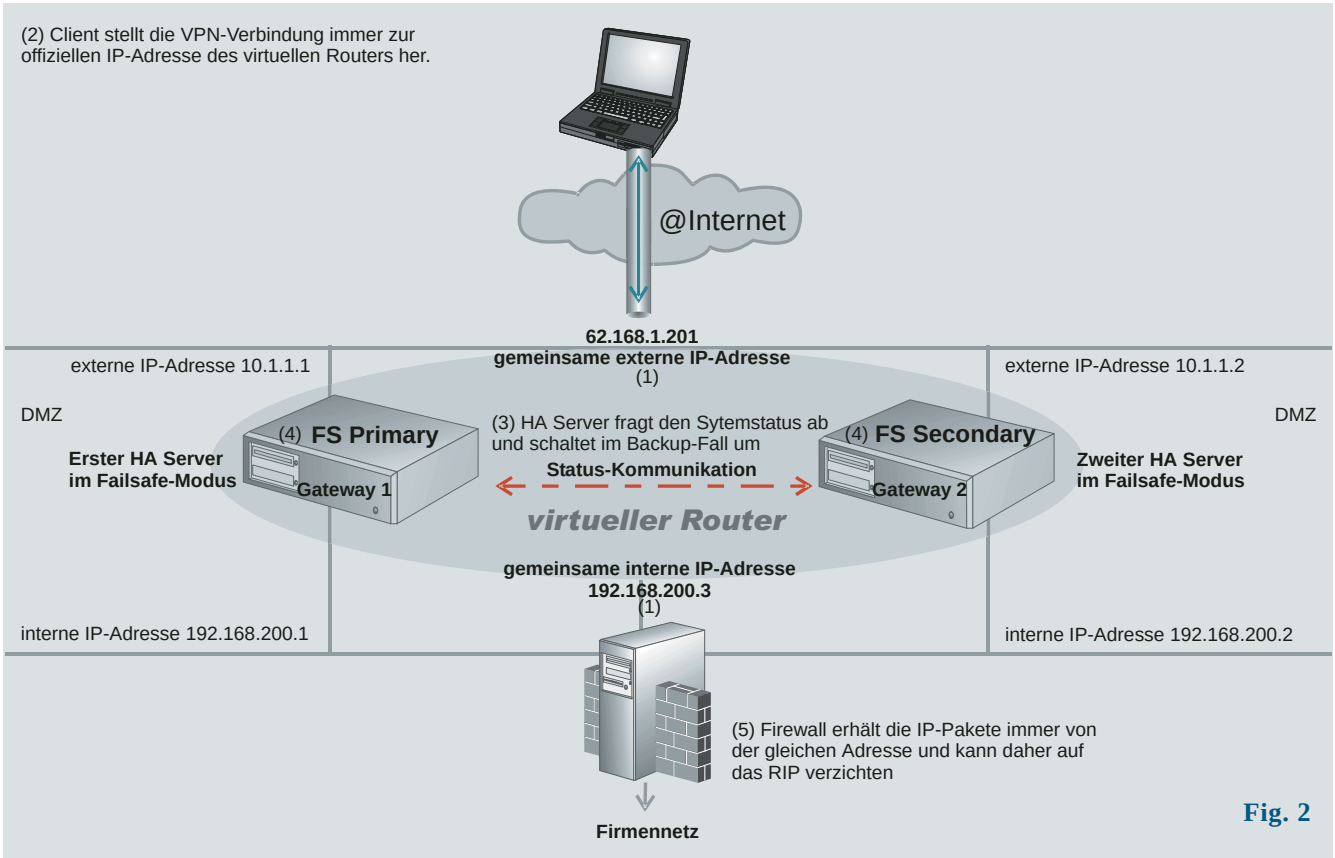


Fig. 2

Pool-Adressen im VRRP-Modus

Sind auf den Gateways verschiedene Pool-Adress-Bereiche definiert, so kann auf eine interne VRRP-Adresse verzichtet werden. Die Firewall benötigt dennoch kein RIP, da die Source-Adressen der Pool-Pakete über statische Routen konfiguriert werden können.

Sind die gleichen Pool-Adress-Bereiche auf beiden Gateways definiert, so wird empfohlen auch für die interne Schnittstelle eine gemeinsame VRRP-Adresse zu definieren, da die Firewall dann die IP-Pakete immer von der gleichen Adresse erhält und auf das Routing Information Protocol verzichten kann (vgl. Fig. 2, 5). Dies gilt sowohl für den Einsatz von Pool-Adressen wie auch für fest zugeordnete IP-Adressen.

Anzahl der offiziellen IP-Adressen

Bei Einsatz einer Failsafe-Architektur mit VRRP wird nur eine offizielle IP-Adresse benötigt, zu der sich das Client-System verbindet, ohne vorher einen HA Server kontaktiert zu haben.

Vereinfachte Konfiguration

Der entscheidende Vorteil bei Einsatz der VRRP-Architektur ist die Vereinfachung der Konfiguration. Dies betrifft sowohl die Konfiguration der Firewall, bei der auf das Routing-Protokoll RIP verzichtet werden kann, wenn mit festen VPN IP-Adressen für Clients oder mit Netzwerkanbindungen gearbeitet wird. Es betrifft aber auch den Konfigurationsaufwand für die Clients-Systeme, für die nur noch ein Tunnel-Endpunkt, nämlich die gemeinsame IP-Adresse der Gateways im VRRP-Madus benötigt wird. Die Angabe für die IP-Adressen der HA Server kann in der Client-Konfiguration komplett entfallen.

VRRP-Varianten mit DVE Clients

Nach Umstellung der Secure Server auf VRRP-Betrieb müssen Enterprise Clients dann nicht umkonfiguriert werden, wenn eine der IP-Adressen für den ersten oder zweiten HA-Server mit der externen IP-Adresse des virtuellen Routers identisch ist.

Bei ausschließlichem Einsatz von DVE Clients kann es sinnvoll sein, eine VRRP-Adresse nur auf der internen Schnittstelle der Gateways zu definieren, da dann die RIP-Konfiguration an der Firewall entfallen kann.

Konfigurationsbeispiel für Failsafe-Modus mit VRRP

Im folgenden Konfigurationsbeispiel wird sowohl auf den externen wie auch auf den internen Schnittstellen der eingesetzten Secure Server jeweils eine gemeinsame virtuelle IP-Adresse eingerichtet.

Die beiden NCP Secure Server stehen innerhalb einer DMZ und besitzen je eine Netzwerkschnittstelle in Richtung Internet und eine in Richtung des internen Unternehmens-Netzes. In diesem Beispiel soll VRRP auf beiden Schnittstellen betrieben werden.

Auf dem externen Interface soll das VPN Gateway 1 die IP-Adresse 10.1.1.1 und das VPN Gateway 2 die P-Adresse 10.1.1.2 haben, die gemeinsame IP-Adresse soll 62.168.1.201 werden.

Auf der internen Netzwerkschnittstelle soll das VPN Gateway 1 die IP-Adresse 192.168.200.1 und das VPN Gateway 2 die P-Adresse 192.168.200.2 haben, die gemeinsame IP-Adresse soll 192.168.200.3 werden.

Bitte beachten Sie zur Vergabe der gemeinsamen IP-Adresse weiter unten den Abschnitt **IP-Adressen aus einem gemeinsamen IP-Netz**.

Konfigurationsablauf

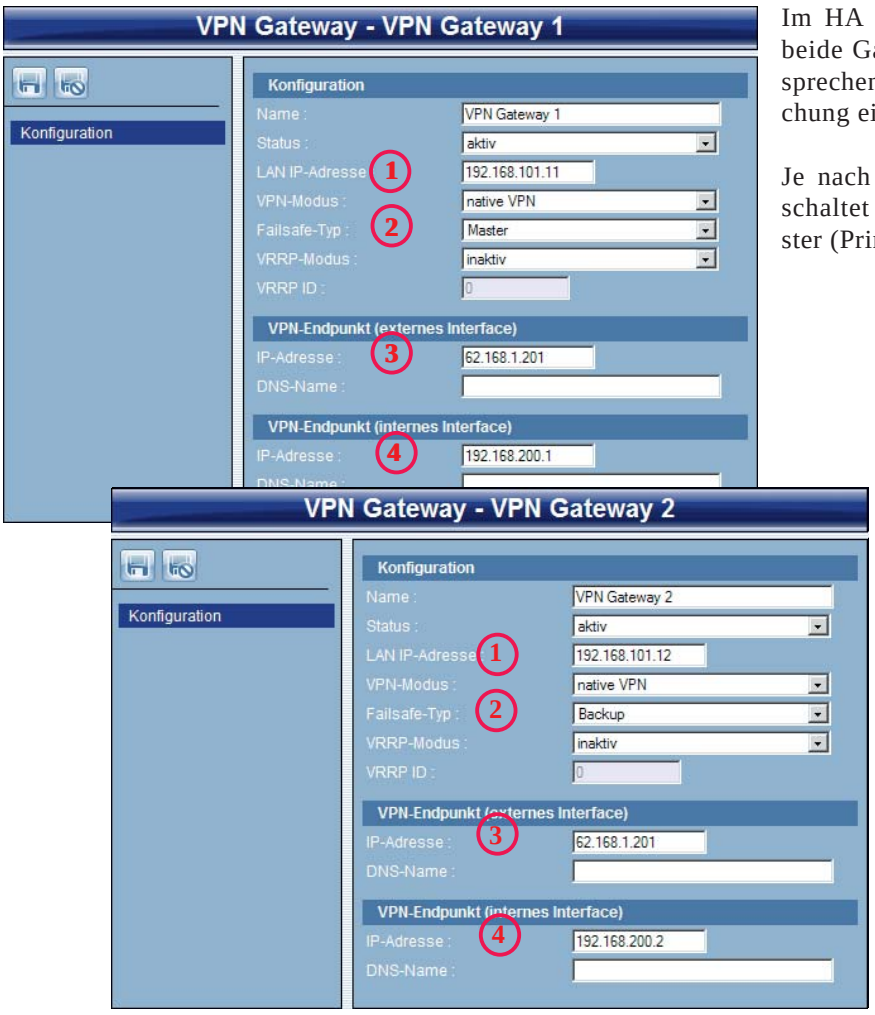
Gehen Sie für Ihre Konfiguration in der gleichen, hier angegebenen Reihenfolge vor. Nur dann vermeiden Sie Störungen in Ihrem Netzwerk:

1. **Konfiguration am HA Server**
2. **Konfiguration am Secure Server**
3. **Konfiguration am Netzwerkadapter**
4. **Konfiguration von Client-System und Firewall**

Konfiguration am HA Server

Zunächst müssen auf beiden Gateways der NCP **Secure Server** und der **HA Server** installiert werden. Die entsprechenden Anleitungen finden Sie in den Handbüchern zu diesen Produkten.

Nach der Installation werden die Systeme, wie in den Handbüchern beschrieben, für den Einsatz im Failsafe Mode konfiguriert. Achten Sie darauf, dass bei der Lizenzierung über das Web-Interface unter **System / Lizenz** Seriennummer und Aktvierungsschlüssel für die Betriebsart Failsafe eingegeben wurden.



Im HA Server werden über das Web-Interface beide Gateways aufgenommen und mit den entsprechenden **LAN IP-Adressen** zur Überwachung eingetragen. (Abb. links 1)

Je nach konfiguriertem **Failsafe-Typ** (Abb. 2) schaltet der HA Server ein Gateway als FS Master (Primary) und das andere als FS Backup.

Für den **VPN-Endpunkt (externes Interface)** (Abb. 4) wird für beide Gateways die gleiche offizielle IP-Adresse eingetragen, über die sich die Client-Systeme verbinden. Über den jeweils unterschiedlichen **VPN-Endpunkt (internes Interface)** (Abb. 4) werden die Gateways vom HA Server angesprochen.

Das Gateway, das in der Betriebsart “FS Backup” steht, nimmt keine Verbindungen von VPN Clients an, ein Verbindungsaufbau ist immer nur zum “FS Master” (Primary) möglich.

Diese Einstellungen können in der Statistik des HA Servers unter “VPN Gateways” abgelesen werden. (Abb. unten, siehe auch **Einstellung des Betriebsmodus**)

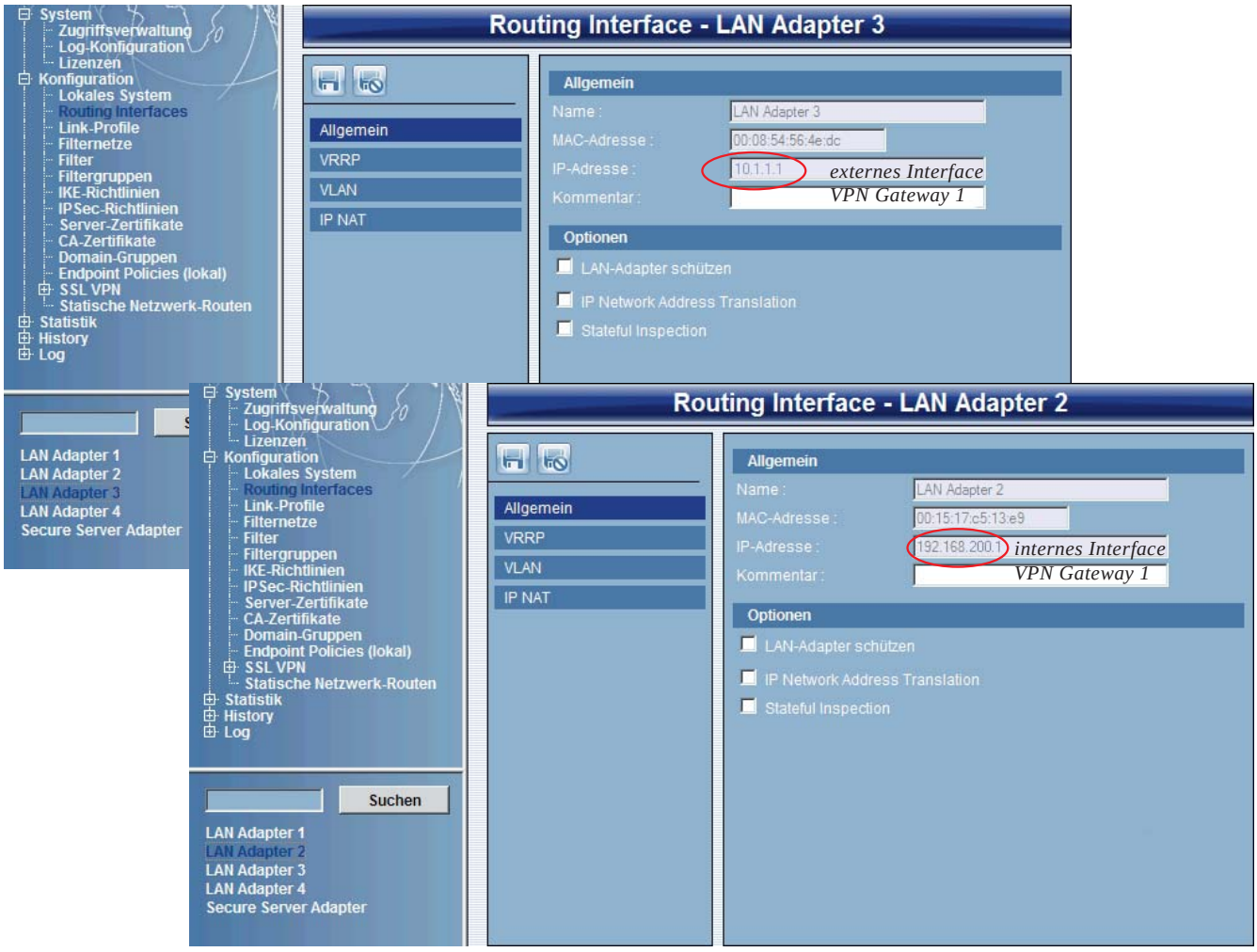
Konfiguration am Secure Server

In der Konfiguration der NCP Secure Server müssen zwei Einstellungen für VRRP vorgenommen werden.

Verbinden Sie sich über das Web-Interface mit Gateway 1 und wechseln Sie in den Bereich “Konfiguration / Routing Interfaces”. Dort suchen Sie sich das entsprechende interne bzw. externe Interface, erkennbar an der **IP-Adresse** im Konfigurationsfeld “Allgemein”.

Der LAN-Adapter für die externe Schnittstelle muss die offizielle IP-Adresse des VPN Tunnel-Endpunkts unter “Lokales System / VPN” besitzen. (Diese Adresse ist an den LAN-Adapter gebunden.) Der LAN-Adapter für die interne Schnittstelle muss die Adresse aus dem Firmennetz besitzen. (Adresse wird bei Installation der Software aus den Netzwerkeinstellungen des Betriebssystems eingelesen.)

Unter “LAN-Adapter / Allgemein” können diese Adressen abgelesen werden.



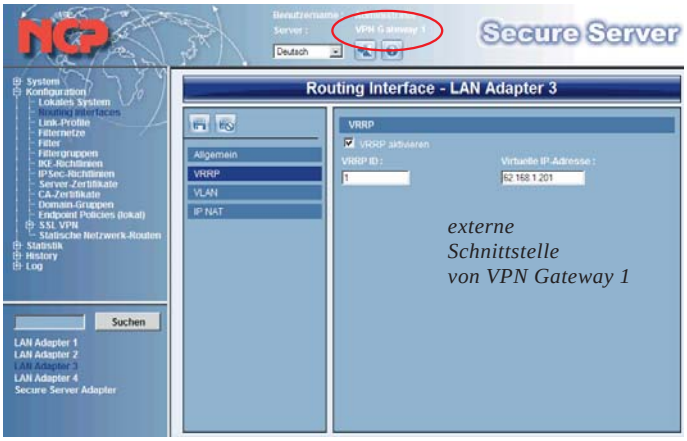
In obigen Abbildungen erkennen Sie die externe und die interne Schnittstelle von VPN Gateway 1.

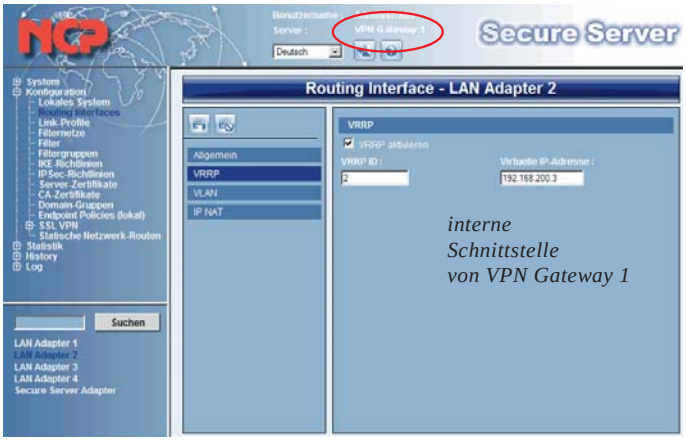
Wechseln Sie nun in das Konfigurationsfeld **VRRP** des jeweiligen Adapters und fahren Sie fort wie folgt.

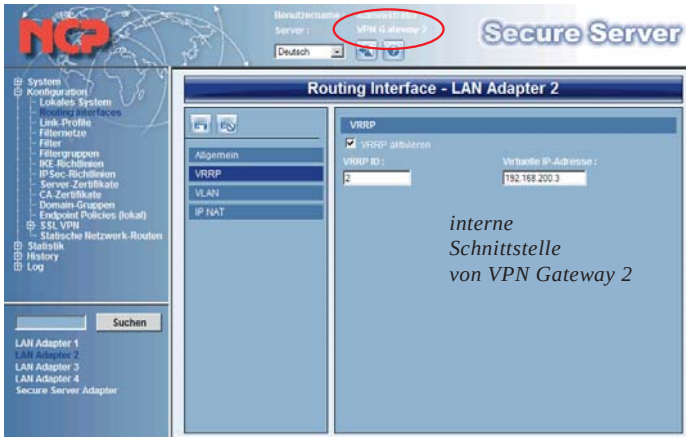
Tragen Sie hier die vorher bestimmte gemeinsame virtuelle VRRP-Adresse ein, die künftig für die jeweilige externe bzw. interne Schnittstelle gelten soll.

Als **VRRP ID** wählen Sie einen Wert von 1 bis 255. Diese ID wird dieser gemeinsamen IP-Adresse zugeordnet und muss daher auch am Gateway 2 der gleichen gemeinsamen IP-Adresse zugeordnet werden, sodass auf beiden Gateways jeweils für die interne wie auch für die externe Schnittstelle die gleiche VRRP ID vergeben sein muss.

Der Anzeigename (unten "VPN Gateway 1 / 2") des Servers wird aus dem Computer-Namen (Host Name) des Systems übernommen. Eine Anpassung dieses Anzeigenamens an den **Namen des Gateways**, *der über das Web-Interface des HA Servers für die Gateway-Konfiguration vergeben wird, kann entweder dort am HA Server oder über die Systemsteuerung des Computers vorgenommen werden.*







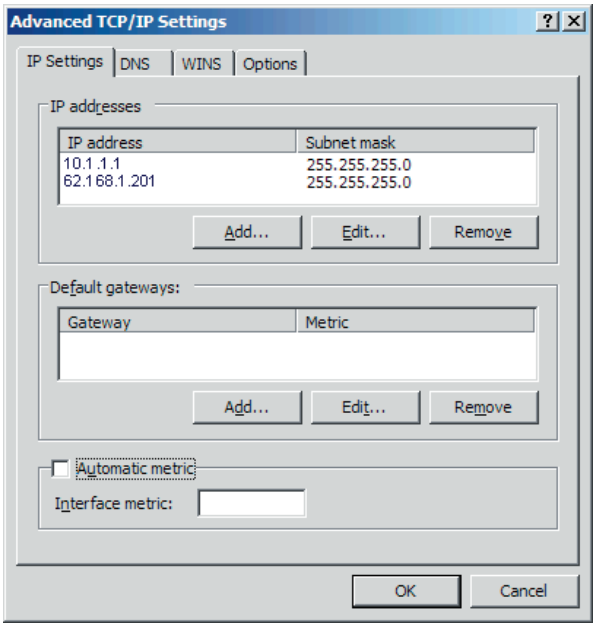
Oben: Konfiguration des VPN Gateway 1 mit:
VRRP-ID = 1 und gemeinsamer IP-Adresse 62.168.1.201 auf dem externen Interface und
VRRP-ID = 2 und gemeinsamer IP-Adresse 192.168.200.3 auf dem internen Interface.

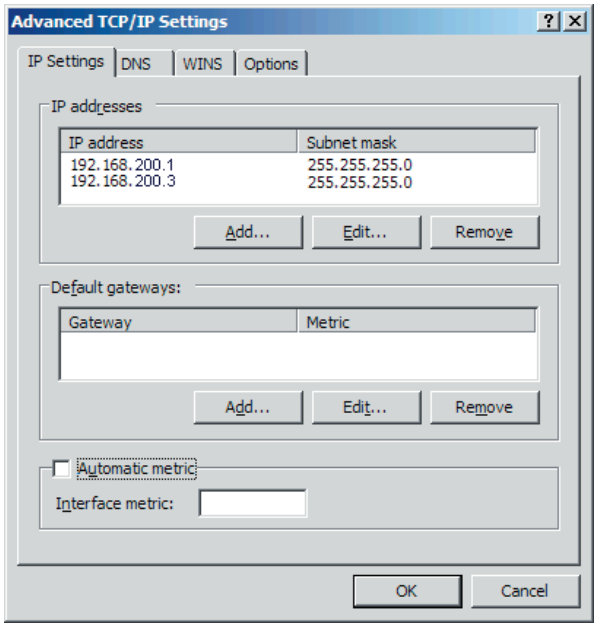
Unten: Konfiguration des VPN Gateway 2 mit:
VRRP-ID = 1 und gemeinsamer IP-Adresse 62.168.1.201 auf dem externen Interface und
VRRP-ID = 2 und gemeinsamer IP-Adresse 192.168.200.3 auf dem internen Interface.

Konfiguration am Netzwerkadapter

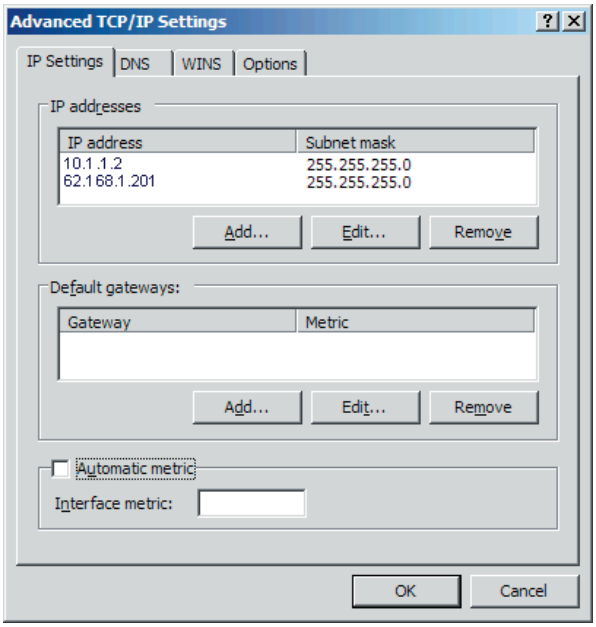
Im Anschluss kann die gemeinsame IP-Adresse jeweils an die entsprechenden physikalischen Adapter gebunden werden.

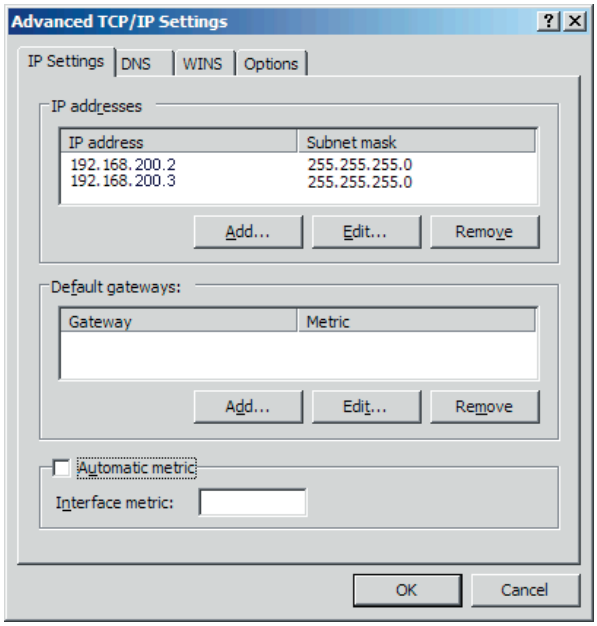
Zum Eintragen der gemeinsamen IP-Adressen öffnen Sie jeweils die Eigenschaften der Netzwerkadapter und fügen in den erweiterten TCP/IP-Einstellungen zusätzlich zur ersten IP-Adresse als zweite IP-Adresse die gemeinsame virtuelle IP-Adresse hinzu.





TCP/IP-Einstellungen der Netzwerkadapter im GW 1





TCP/IP-Einstellungen der Netzwerkadapter im GW 2

Nach dieser Änderung der Netzwerkeinstellungen müssen die Dienste neu gestartet werden. Über das Web-Interface können Sie überprüfen, ob die virtuelle IP-Adresse korrekt konfiguriert wurde. Dazu öffnen Sie in der Konfiguration unter “Routing Interfaces” einen der oben konfigurierten LAN-Adapter. Als IP-Adresse muss nun die ursprüngliche Adresse des physikalischen Adapters und mit Komma dahinter die entsprechende virtuelle IP-Adresse lesbar sein.

Konfiguration von Client-System und Firewall

In den Client-Systemen können Sie nun als Tunnel-Endpunkt die gemeinsame öffentliche Adresse, in diesem Beispiel “62.168.1.201" konfigurieren.

In der Firewall auf der internen Seite der DMZ tragen Sie die gemeinsame interne Adresse als statische Route zum VPN-IP-Netz ein, in diesem Beispiel die Adresse “192.168.200.3".

IP-Adressen aus einem gemeinsamen IP-Netz

Erfolgt die Festlegung der IP-Adressen in der Weise, dass die physikalischen Adressen der Gateways und die gemeinsame virtuelle IP-Adresse, zu der die VPN-Verbindungen hergestellt werden, in einem gemeinsamen IP-Netz liegen, so wird vom Betriebssystem gesteuert mit welcher IP-Adresse die Antwortpakete vom Gateway zum Client zurück gesendet werden.

Unter Windows und Linux werden die Antwortpakete bei ICMP- (Ping) oder TCP-Kommunikation (https) in der Regel mit der Adresse versendet, die vom Client angesprochen wurde, d. h. mit der virtuellen IP-Adresse, die am Client als VPN Tunnel-Endpunkt konfiguriert ist.

Bei UDP werden die Antwortpakete mit der IP-Adresse versendet, die sich mit dem Standard-Gateway bzw. einer passenden Route im gleichen IP-Netz befindet. Trifft das auf zwei IP-Adressen zu, so wird die zuerst am Gateway gebundene also nicht die virtuelle IP-Adresse verwendet.

Dies führt dazu, dass ein VPN Client der über den UDP-Port 1701 (L2TP), den UDP-Port 500 (IPsec) oder den UDP-Port 4500 (NAT-T) die VRRP-Adresse anspricht, die Antwort mit der physikalischen Adresse als Absender erhält. Diese Kommunikation ist mit “stateful” arbeitenden Firewalls nicht möglich.

Beispiel (beachten Sie unten Fig. 3):

Wurde für die dem Internet zugewandte externe Schnittstelle an Gateway 1 die Adresse 62.168.1.202, an Gateway 2 die Adresse 62.168.1.203, als VRRP-Adresse 62.168.1.201 konfiguriert und lautet die Adresse des Standard-Gateways 62.168.1.1, so erreichen zwar alle UDP-Anfragen aus dem Internet die VRRP-Adresse 62.168.1.201. Alle UDP-Antwortpakete werden jedoch mit der Adresse 62.168.1.202 oder 62.168.1.203 verschickt.

Dasselbe Adressierungs-Problem tritt auch bezüglich der internen Schnittstelle auf, wenn zur internen VRRP-Adresse eine UDP-Kommunikation stattfinden soll, beispielsweise SNMP.

Ab der Version 7.0 des NCP Secure Server ist dies für IPsec-Kommunikation korrigiert. Die Kommunikation über die UDP-Ports 500 (IKE) und 4500 (NAT-T) sowie einen evtl. verwendeten alternativen Port für UDP-Encapsulation wird vom Secure Server so gesteuert, dass die Antwortpakete korrekt mit der VRRP-Adresse als Source-Adresse versendet werden. Für L2TP ist eine solche Steuerung nicht vorgesehen!

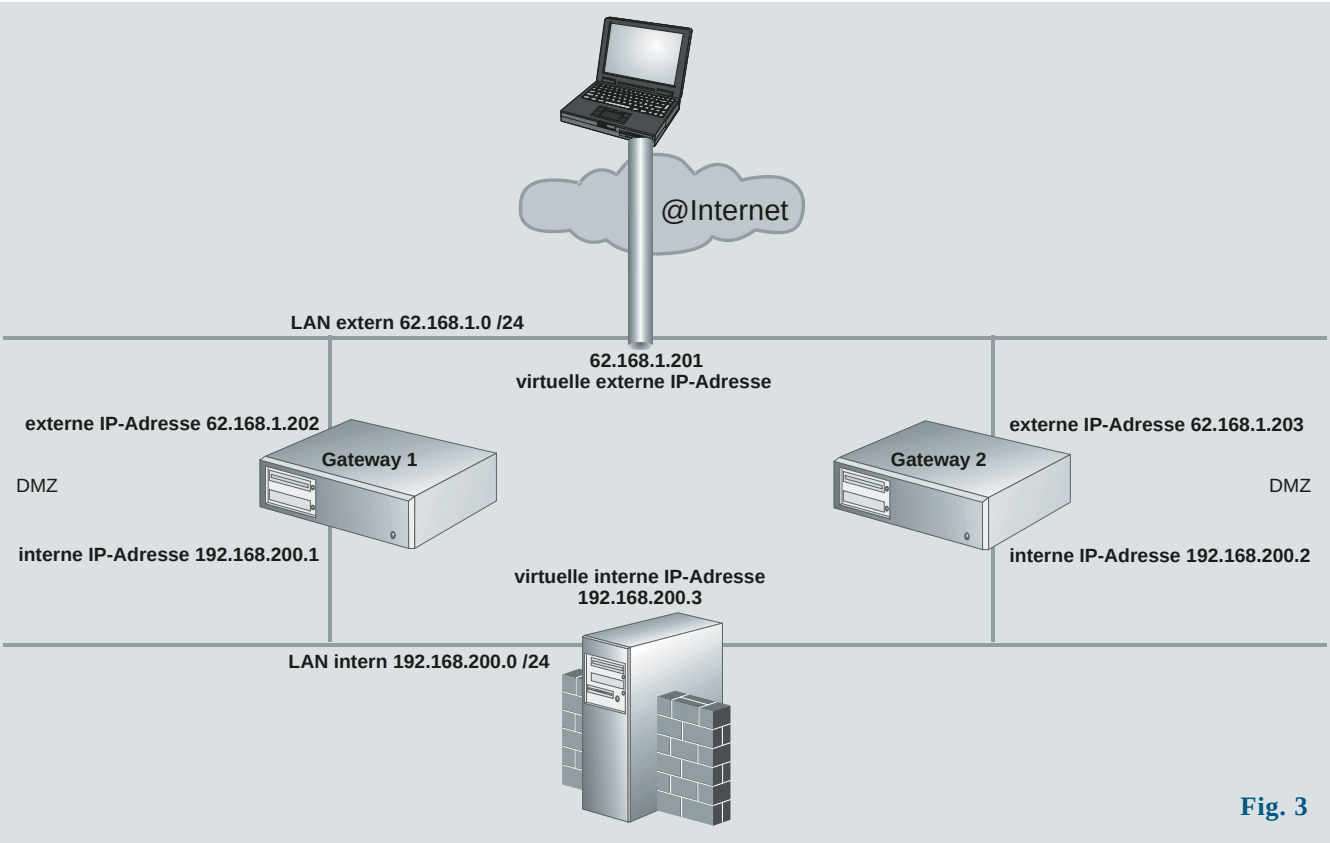


Fig. 3

VRRP-Adressierung mit Gateways unter Linux

Wird der NCP Secure Server unter Linux installiert, so muss ebenfalls die VRRP-Adresse an den LAN-Adapter gebunden werden. Wird dies über die Einstellungen des Betriebssystems vorgenommen, so ist die VRRP-Adresse aktiv, unabhängig davon, ob der NCP Secure Server gestartet ist.

Am NCP Secure Server für Linux sind die beiden Scripte “dve_up” und “dve_down” hinterlegt. Sie befinden sich im Verzeichnis:
`/usr/local/ncp/ses/`

Diese Scripte werden vom NCP Secure Server dann aufgerufen, wenn er durch den HA-Server in den Betriebs-Modus FS_Master (dve_up) bzw. zum FS_Secondary (dve_down) geschaltet wird.

In diesen Beispielscripten (dve_up.sam und dve_down.sam) wird die Verwendung von arptables empfohlen. Arptables blockiert eingehende arp-Anfragen auf dem Backup Gateway (Secondary), während auf dem Master Gateway (Primary) diese Anfragen durchgelassen werden.

Arptables ist als zusätzliches Paket für viele Linux Distributionen erhältlich. Sollte die Verwendung von arptables nicht möglich sein, muss der Netzadapter gemäß der Beispiele aktiviert bzw. deaktiviert werden.

Beispiel dve_up.sam

```
#!/bin/bash
# It is recommended to use arptables to switch between VRRP Gateways
# If possible please install arptables and uncomment the following line:
# arptables -F
# If the installation of arptables is not possible use the following example
# and change the ip to the VRRP ip address
# ifconfig eth0:1 192.168.x.y netmask 255.255.255.0
```

Beispiel dve_down.sam

```
#!/bin/bash
# It is recommended to use arptables to switch between VRRP Gateways
# If possible please install arptables, uncomment the following line and adjust
# the ip address to your VRRP ip address
# arptables -A INPUT -d 192.168.x.y -j DROP
# If the installation of arptables is not possible use the following example
# ifconfig eth0:1 down
```

Load Balancing-Modus

Load Balancing kommt dann zum Einsatz, wenn es gilt den VPN-Verkehr ins zentrale Datennetz möglichst gleichmäßig zu verteilen und wenn diese Verteilung automatisiert und dynamisch erfolgen soll. Das Tunnelaufkommen wird über zwei oder mehr Gateways (Server Farm) von einem HA Server im LB-Modus verteilt. Das HA-System sorgt dabei einerseits für die gleichmäßige Auslastung aller verfügbaren VPN Gateways (Enterprise Server) und andererseits für die automatische Ausgliederung eines VPN Gateways, wenn dies im Service- oder Störungsfall ausfällt. In diesem Fall wird es aus der Zuteilungsroutine von VPN-Tunnels herausgenommen und die Tunnelverbindungen auf die verbliebenen Gateways gleichmäßig verteilt.

Im Load Balancing- werden anders als im Failsafe-Betrieb alle VPN Gateways gleichzeitig genutzt. Nur der zweite HA Server befindet sich im passiven Betriebszustand des Hot Standby.

Der aktive HA Server ist in der Lage, die tatsächliche Auslastung der Gateways zu berücksichtigen. Dazu können, je nach Bedarf, mehrere Auslastungskriterien verschieden gewichtet werden. Nach diesen Kriterien, die im HA-Manager konfiguriert werden, werden die Stati der einzelnen Gateways vom HA Server abgefragt und intern miteinander verglichen.

Folgende Kriterien für die Auslastung eines Gateways können gewichtet werden:

– die Übertragungsrate
– die Anzahl der genutzten Tunnels
– die Anzahl der reservierten IP-Pool-Adressen gegenüber Verbindungsanforderungen anderer Benutzer
– die CPU-Auslastung

Je nach Konfiguration werden diese Faktoren in einem festzulegenden Abfrageintervall zur Ermittlung des am wenigsten ausgelasteten VPN Gateways herangezogen.

Der Load Balancing-Modus (LB-Modus) eines NCP HA-Systems kann nur für Verbindungen von NCP Clients genutzt werden, für Enterprise Clients aufgrund des DVE-Protokolls, für NCP SSL VPN Clients nur dann, wenn gleichzeitig der VRRP-Betriebsmodus eingesetzt wird.

Gleichwohl können mit Hilfe des VRRP-Betriebsmodus innerhalb eines Load Balancing-Systems auch gleichzeitig Verbindungen von VPN Clients anderer Hersteller gemanagt werden. Zwar ist ein dynamisches Ausbalancieren der Tunnels (zur Zeit) nicht möglich, doch kann für Verbindungen dieser Clients Hochverfügbarkeit sichergestellt werden, indem zwei Gateways aus dem Load Balancing-Verbund gleichzeitig für den **Failsafe-Modus mit VRRP** konfiguriert werden, dessen Prinzip oben beschrieben wurde.

Load Balancing-Modus mit DVE-Protokoll

Wie im Failsafe-Modus mit DVE-Protokoll, muss auch hier remote-seitig der NCP Enterprise Client (DVE Client) eingesetzt sein. Zentral-seitig können mehr als zwei VPN Gateways installiert sein. Der HA Server wird redundant installiert.

(Zu Installation und Konfiguration der Server-Komponenten beachten Sie bitte **die weiteren Beschreibungen**, die auf der letzten Seite dieses Dokuments angegeben sind.)

Pro VPN Gateway wird eine offizielle IP-Adresse benötigt. Erster und zweiter HA Server werden auf zwei der Gateway-Rechner installiert und erhalten für gewöhnlich die gleichen offiziellen IP-Adressen wie die Gateways.

Funktionsablauf

(Beachten Sie hierzu unten Fig. 4)

Im Prinzip erfolgt der Ablauf bis zum Verbindungsaufbau mit einem VPN Gateway genauso wie im oben beschriebenen “Failsafe-Modus mit DVE-Protokoll”.
(1) Der Enterprise Client verbindet sich zunächst zum aktiven HA Server und schickt einen DVE Request.
(2) Der aktive HA Server ermittelt den Status der zur Verfügung stehenden Gateways nach den vorgegebenen Kriterien und wählt das am wenigsten ausgelastete Gateway aus.
(3) Die externe IP-Adresse des in diesem Intervall aktiven Gateways wird dem Enterprise Client als DVE Response mitgeteilt.
(4) Nachdem der Enterprise Client die IP-Adresse erhalten hat, baut er eine Tunnel-Verbindung zum aktiven Gateway auf.
(5) Über das aktive Gateway wird dem Client eine Adresse aus dem Firmennetz zugewiesen. Dabei kann es sich entweder um eine Pool IP-Adresse handeln, oder um eine feste IP-Adresse. (Konfigurationsfeld **Link-Profile / Routing** am Server).

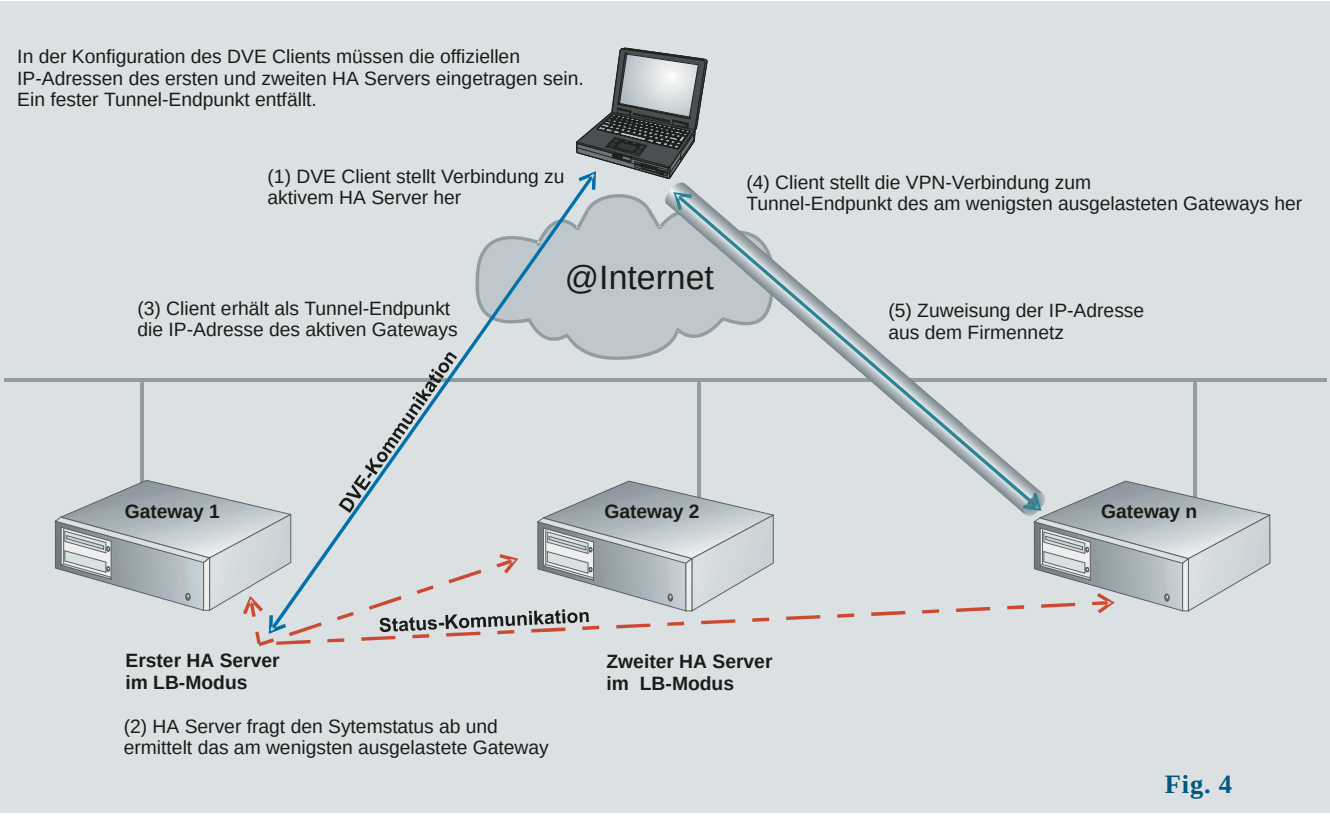
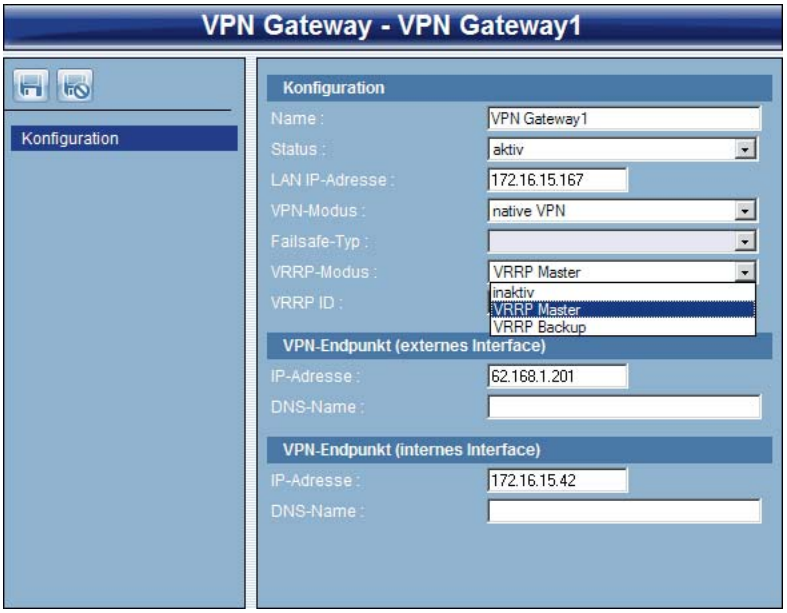


Fig. 4

Load Balancing mit VRRP für NCP Entry Clients

Um die Gateways im Load Balancing-System auch für VPN-Verbindungen für Clients ohne DVEP-Unterstützung nutzen zu können, muss der VRRP-Modus an mindestens zwei dieser Gateways eingesetzt werden. Dies erfolgt über die Gateway-Konfiguration, wo der **VRRP-Modus** für eines der Gateways auf “VRRP Master” für ein anderes auf “VRRP Backup” gesetzt wird (siehe Abb. rechts).

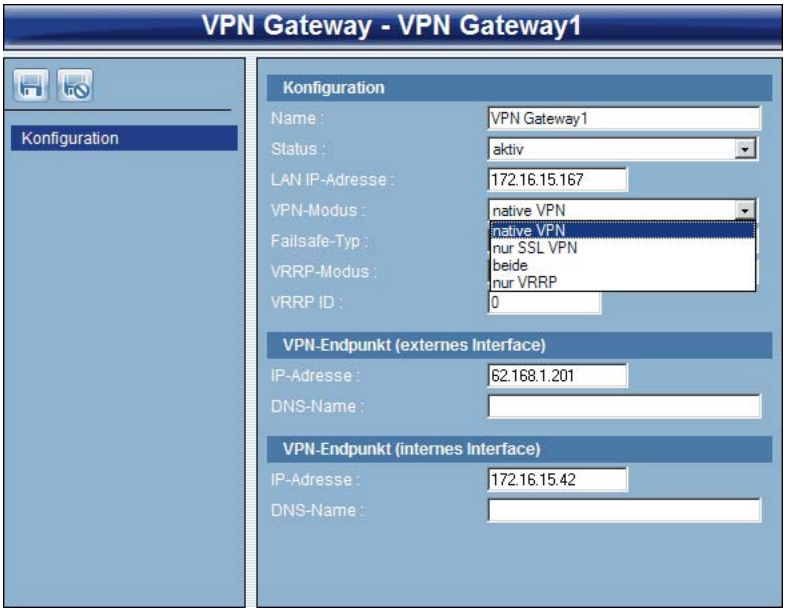
Die **Schnittstellen-Konfiguration** der für den VRRP-Modus ausgewählten Gateways erfolgt genauso wie oben für den Failsafe-Modus mit VRRP beschrieben. Zusätzlich wird die gleiche VRRP-ID, die auch in der Konfiguration der virtuellen IP-Adresse an den Gateways eingetragen wurde, der entsprechenden Schnittstelle des jeweiligen Gateways zugeordnet. Dadurch erkennt der HA Server welche Gateway-Schnittstellen im VRRP-Modus zur Verfügung stehen sollen.



Oben: Einstellung des VRRP-Modus

Mit dieser Konfiguration wird mittels zweier Gateways innerhalb der Load Balancing Server Farm eine Ausfallsicherung nach dem Failsafe-Prinzip mit VRRP für NCP Entry Clients (oder andere nicht-DVE-fähige VPN Clients) bereitgestellt. Diese Clients nutzen nur den VRRP-Modus des sogenannten virtuellen Routers (bestehend aus Gateway 1 und Gateway 2) zum Verbindungsaufbau.

Der Load Balancing-Betriebsmodus der beiden Gateways kann weiterhin parallel von NCP Enterprise Clients oder NCP SSL VPN Clients genutzt werden, solange der **VPN-Modus** nicht auf “nur VRRP” gestellt wird (siehe Abb. rechts).



Oben: Einstellung des VPN-Modus

In bestimmten Konstellationen, z. B. viele nicht-DVE-fähige Clients, kann es sinnvoll sein den “VPN-Modus” auf “nur VRRP” zu stellen. Damit werden die VRRP Gateways aus dem Load Balancing-Verbund herausgenommen und es wird sichergestellt, dass DVE Clients vom HA Server nicht über die VRRP Gateways geleitet werden. (Der **VPN-Modus** ist weiter unten beschrieben.)

Funktionsablauf

(Beachten Sie hierzu Fig. 5)

(1) Beide Gateways, deren **VRRP-Modus** als “VRRP Master” und “VRRP Backup” eingerichtet wurde, fungieren zusammen als ein virtueller Router, der sich gegenüber dem Internet mit nur einer gemeinsamen offiziellen IP-Adresse darstellt. (Auch auf dem internen Netzwerk-Interface beider Gateways kann VRRP mit einer gemeinsamen IP-Adresse betrieben werden.)

(2) Diese gemeinsame IP-Adresse erlaubt den Verzicht auf die Konfiguration der IP-Adressen beider HA Server in den Client-Systemen, da die HA Server nicht mehr nach der Adresse des aktiven Gateways gefragt werden müssen. Statt dessen benötigt der Client nur noch einen VPN-Endpunkt, nämlich die offizielle IP-Adresse des virtuellen Routers, um die Verbindung zu dem darin enthaltenen aktiven Failsafe Gateway (VRRP Master) aufbauen zu können.

(3) Der HA Server dient der Status-Überwachung und im Backup-Fall als Umschalter zwischen den Gateways im virtuellen Router.

(4) Zunächst übernimmt das vom HA Server als VRRP Master gesetzte Gateway die gemeinsame IP-Adresse. Fällt das VRRP Master Gateway aus, wird die gemeinsame IP-Adresse vom HA Server an das VRRP Backup Gateway entsprechend einer gemeinsamen “VRRP ID” übergeben.

(5) Sowohl VRRP Master als auch VRRP Backup, stehen parallel im LB-Modus mit weiteren Gateways zur Verfügung, sofern der VPN-Modus der beiden Gateways auch native VPN- oder SSL VPN-Verbindungen zulässt.

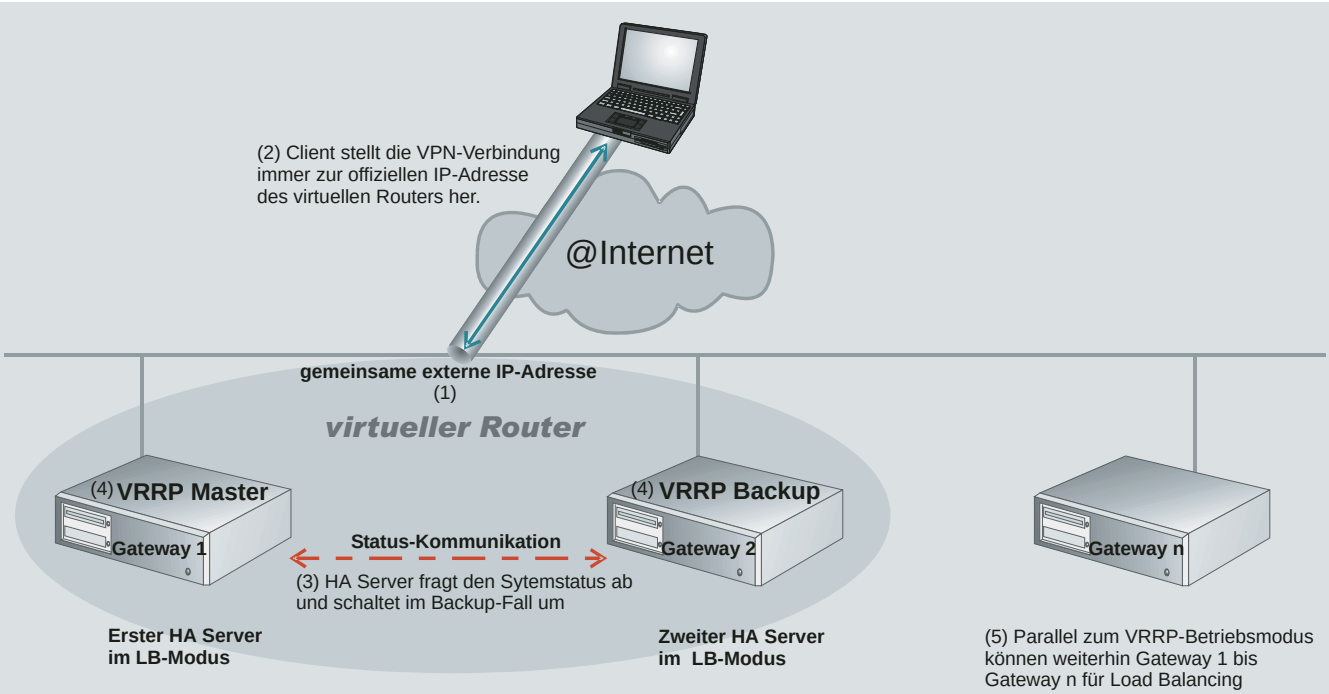


Fig. 5

Load Balancing mit VRRP für NCP SSL VPN Clients

Wird der VRRP-Modus (wie oben beschrieben) an zwei Gateways der Server Farm konfiguriert, so kann der virtuelle Router als Ausfallsicherung für NCP Entry Clients aber auch für NCP SSL VPN Clients oder für beide genutzt werden.

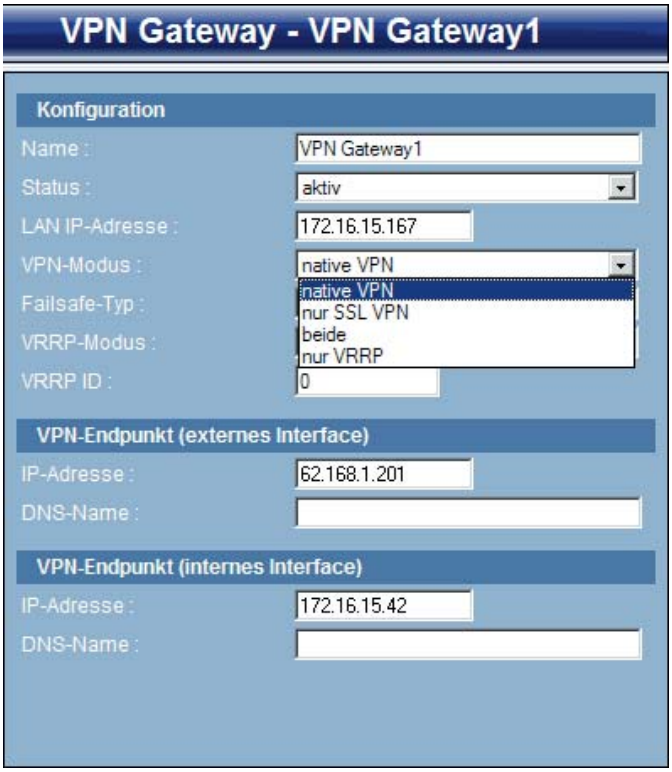
Welche Tunnelverbindungen vom HA-System angenommen werden, kann mit dem **VPN-Modus** konfiguriert werden: native VPN, SSL VPN oder beide. Wird der VPN-Modus “beide” eingestellt, können sowohl NCP Entry Clients als auch NCP SSL VPN Clients eine Verbindung zur VRRP-Adresse des virtuellen Routers herstellen (siehe Abb. rechts).

Sowohl native VPN- als auch SSL VPN-Clients stellen in einer ersten Phase des Verbindungsaufbaus den Kontakt zum aktiven VRRP Master Gateway her.

SSL VPN-Verbindungen werden vom Master Gateway in den Load Balancing-Verbund weitergeleitet. Dies erfolgt durch einen HTTP Redirect an den Browser, womit dieser die IP-Adresse des Tunnelendpunkts des am wenigsten ausgelasteten Gateways im LB-Verbund erhält. In einer zweiten Phase des Verbindungsaufbaus verbindet er sich zu diesem Gateway.

Für native VPN-Verbindungen ist die VRRP-Adresse des Master Gateways der Tunnelendpunkt, sodass für sie nur der Failsafe-Modus des virtuellen Routers genutzt werden kann.

Die DVE-Kommunikation zwischen Enterprise Client und HA Server bleibt durch den VRRP-Modus der Gateways unbeeinflusst, sodass Verbindungen des Enterprise Clients weiterhin von allen Gateways im LB-Verbund entgegen genommen werden können, deren VPN-Modus nicht ausdrücklich auf “nur VRRP” gestellt wurde.



Oben: Einstellung des VPN-Modus

Funktionsablauf

(Beachten Sie hierzu unten Fig. 6)

(1) In das Adressfeld des Browsers wird die vom Administrator vorgegebene virtuelle IP-Adresse eingetragen (VRRP-Adresse).

(2) Durch die am HA Server erzeugte VRRP-Konfiguration wird die Verbindung immer zuerst zu dem als “Master” definierten Gateway aufgebaut. (Das Backup Gateway nimmt eine Verbindung vom Browser mit virtueller VRRP IP-Adresse nur dann an, wenn es in einem Backup-Fall vom HA Server dazu veranlasst wird.)

(3) Am Master Gateway wird der Listener angesprochen, der in der Listener-Konfiguration als IP-Adresse die gemeinsame virtuelle IP-Adresse erhalten hat. Dieser Listener hat in den HA Load Balancing-Optionen keinen SSL VPN-Endpunkt eingetragen, nur eine VRRP-ID.

(4) Der HA Server ist über die aktuelle Auslastung der LB Gateways informiert, die diese VRRP-ID besitzen und sucht unter diesen Gateways das mit der geringsten Auslastung aus.

(5) Er veranlasst das Master Gateway zu einem HTTPS Redirect, mit welchem dem Browser die Adresse des SSL VPN-Endpunkts übergeben wird, das zu dem Gateway mit genau dieser VRRP-ID und der geringsten Auslastung passt.

(6) Daraufhin wird im Browser die SSL VPN-Verbindung zu diesem Endpunkt aufgebaut.

Master- und Backup Gateway werden in der ersten Phase des Verbindungsaufbaus (1) als virtueller Router genutzt. Parallel erfüllen sie in der zweiten Phase des Verbindungsaufbaus ihre Funktion als Gateways im LB-Verbund (6).

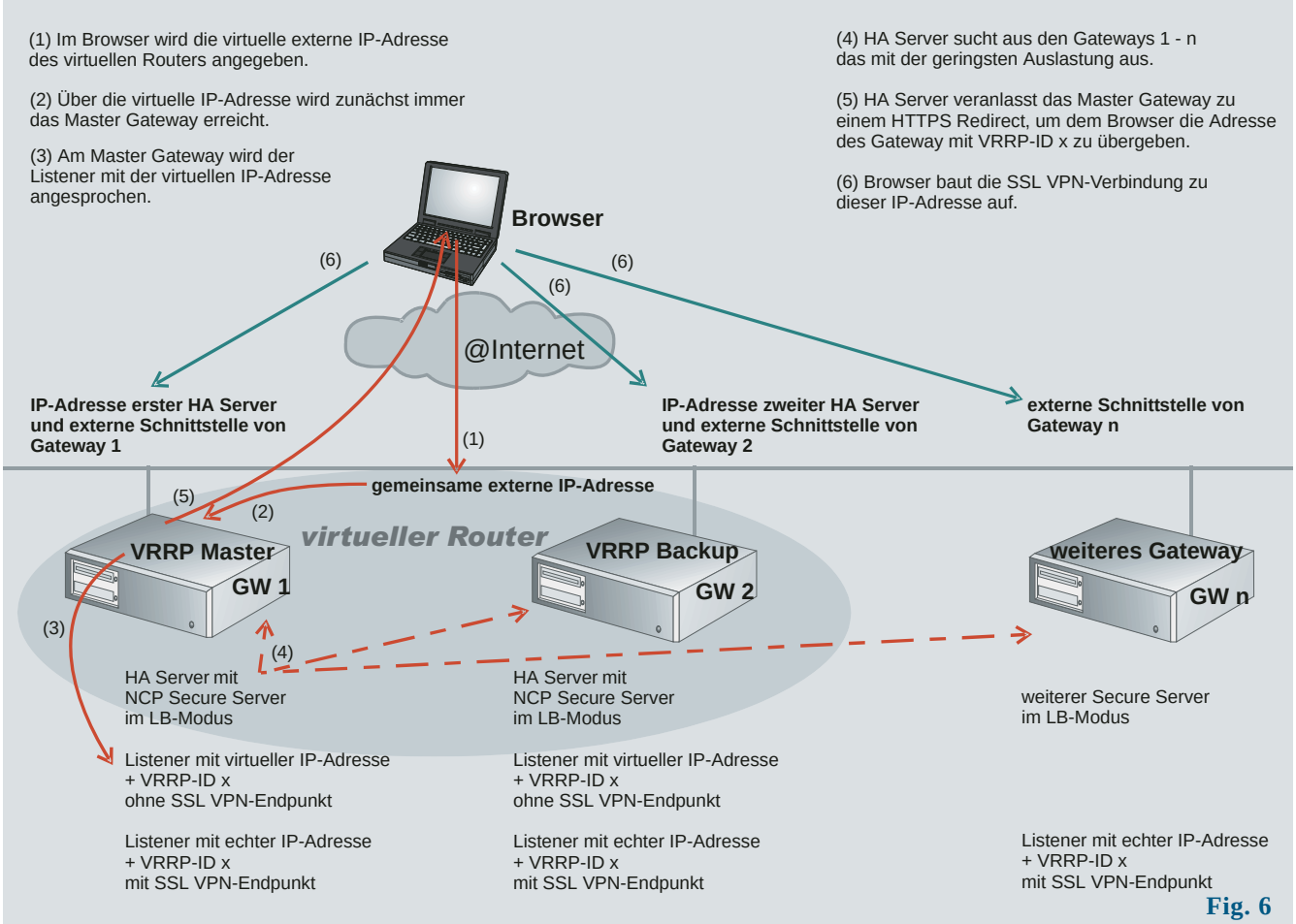


Fig. 6

Hochverfügbarkeit in heterogenen Umgebungen

Mittels VRRP-Technik der NCP High Availability Services kann eine Server Farm im Load Balancing-Modus nicht nur für die Verbindungen von NCP Enterprise Clients, sondern zusätzlich für NCP SSL VPN Clients genutzt werden.

Gleichzeitig können die Verbindungen von NCP Entry Clients oder einfachen IPsec Clients anderer Hersteller über den immanenten virtuellen Router des Load Balancing-Verbunds gemanagt werden. Dazu können bei Einsatz mehrerer Gateways paarweise immer zwei mit einer gemeinsamen VRRP-Adresse konfiguriert werden.

Konfigurationsbeispiel für Load Balancing-Modus mit VRRP

In diesem Beispiel verfügen je ein HA Server und ein Gateway über die gleiche offizielle IP-Adresse in Richtung des Internets.

Die beiden Rechner mit je einem installierten Secure Server und einem HA Server stehen innerhalb einer DMZ und besitzen je eine externe Netzwerkschnittstelle und eine in Richtung des internen Unternehmens-Netzes. VRRP wird hier nur auf der externen Schnittstelle der Gateways betrieben.

Auf dem externen Interface soll das VPN Gateway 1 die physikalische LAN IP-Adresse 62.168.1.201 und das VPN Gateway 2 die physikalische LAN IP-Adresse 62.168.1.202 haben, die gemeinsame virtuelle VRRP IP-Adresse soll 62.168.1.203 werden.

Konfigurationsablauf

Gehen Sie für Ihre Konfiguration in der gleichen, hier angegebenen Reihenfolge vor. Nur dann vermeiden Sie Störungen in Ihrem Netzwerk.

1. Konfiguration am HA Server
2. Konfiguration am Secure Server
3. Konfiguration der Netzwerkeinstellungen
4. Konfiguration der Listener am Secure Server (SSL VPN-Einstellungen)

IP-Adressen

Gateway 1
physikalische IP-Adresse des LAN-Adapters:
62.168.1.201
VRRP-Adresse: 62.168.1.203

1. Listener
Listener IP-Adresse: 62.168.1.201
Port: 443
VRRP ID: 31
Endpunkt: 62.168.1.201

2. Listener
Listener IP-Adresse: 62.168.1.201
Port: 443
VRRP ID: 31

Gateway 2
physikalische IP-Adresse des LAN-Adapters:
62.168.1.202
VRRP-Adresse: 62.168.1.203

1. Listener
Listener IP-Adresse: 62.168.1.202
Port: 443
VRRP ID: 31
Endpunkt: 62.168.1.202

2. Listener
Listener IP-Adresse: 62.168.1.203
Port: 443
VRRP ID: 31

Konfiguration am HA Server

Zunächst müssen auf beiden Gateways der NCP **Secure Server** und der **HA Server** installiert werden. Die entsprechenden Anleitungen finden Sie in den Handbüchern zu diesen Produkten.

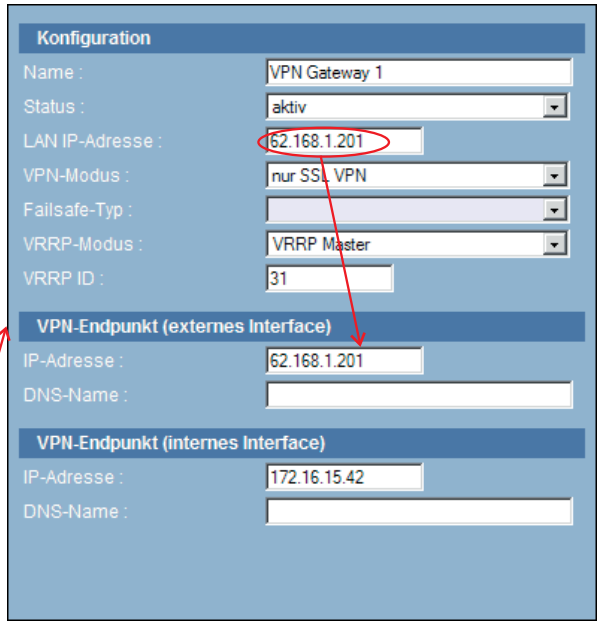
Nach der Installation werden die Systeme, wie in den Handbüchern beschrieben, für den Einsatz im Load Balancing-Modus konfiguriert.

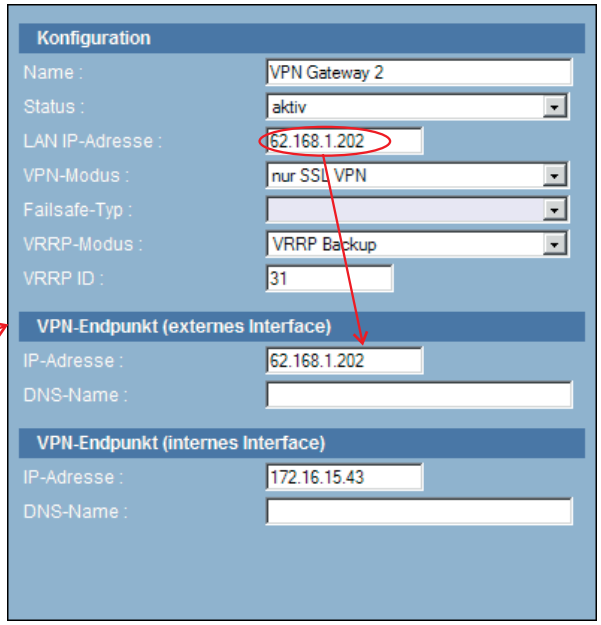
Achten Sie darauf, dass bei der Lizenzierung über das Web-Interface unter **System / Lizenz** Seriennummer und Aktvierungsschlüssel für die Betriebsart Load Balancing eingegeben wurden, sowie anschließend der Aktivierungsschlüssel für die SSL VPN-Lizenz.

Abbildungen rechts: Zwei Gateways für den Einsatz im Load Balancing-Modus müssen konfiguriert werden. Hierfür werden die entsprechenden IP-Adressen zur Überwachung (LAN IP-Adresse) durch den HA Server und für den VPN-Endpunkt am externen Interface eingetragen.

Da sich der Browser, der HA Server und das VPN Gateway im Internet befinden, handelt es sich bei der LAN IP-Adresse, über die das Gateway vom HA Server angesprochen wird, wie auch bei der IP-Adresse für den VPN-Endpunkt an der externen Schnittstelle (die IP-Adresse die der Client als Tunnel-Endpunkt erhält) um die jeweils gleichen offiziellen IP-Adressen. (Abb. rechts: Gateway 1 und Gateway 2)

Diese Einstellungen erfolgen unter **Konfiguration / VPN Gateways**.





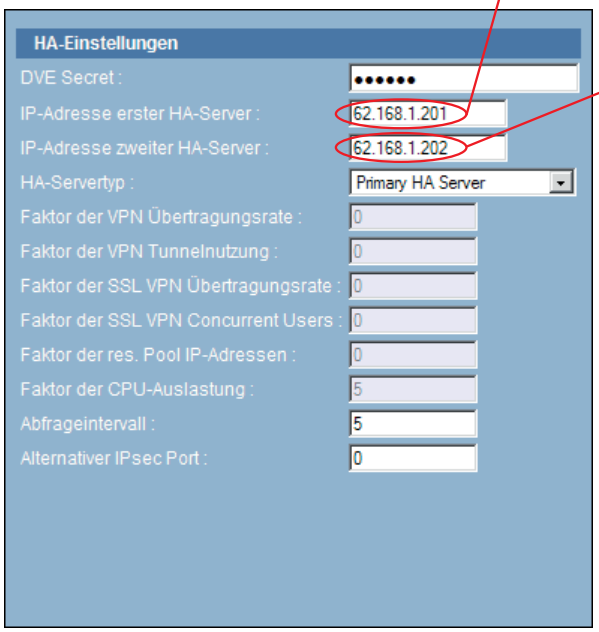
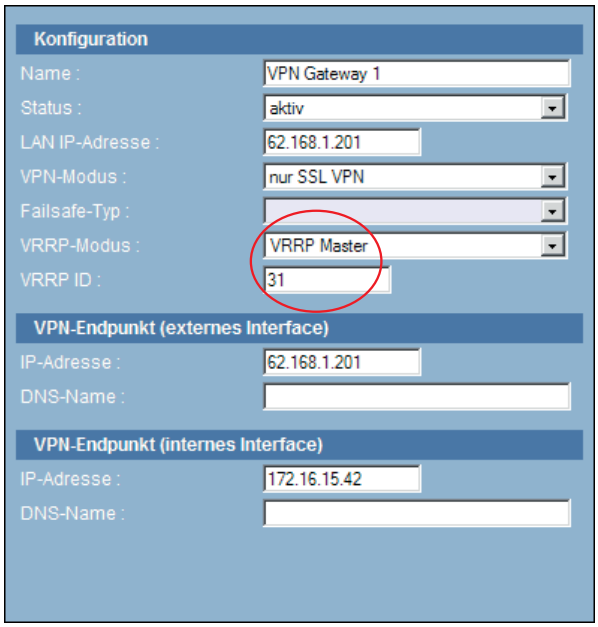


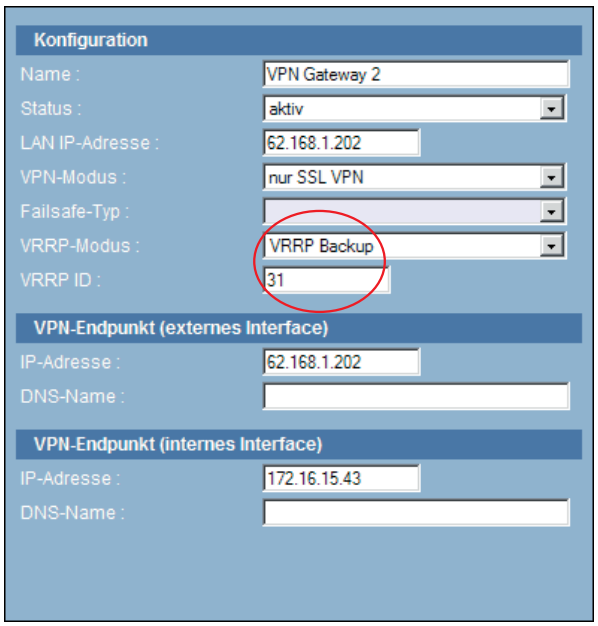
Abbildung links: Der erste HA Server erhält die gleiche IP-Adresse wie die externe Schnittstelle von Gateway 1, der zweite HA Server die gleiche wie Gateway 2.

Diese Einstellung erfolgt unter Konfiguration / Allgemein / **HA-Einstellungen**.

Einstellung des Betriebsmodus

Für die Gateways 1 und 2 wird der VRRP-Modus eingestellt, Gateway 1 wird das “VRRP Master” Gateway und Gateway 2 das “VRRP Backup” Gateway.



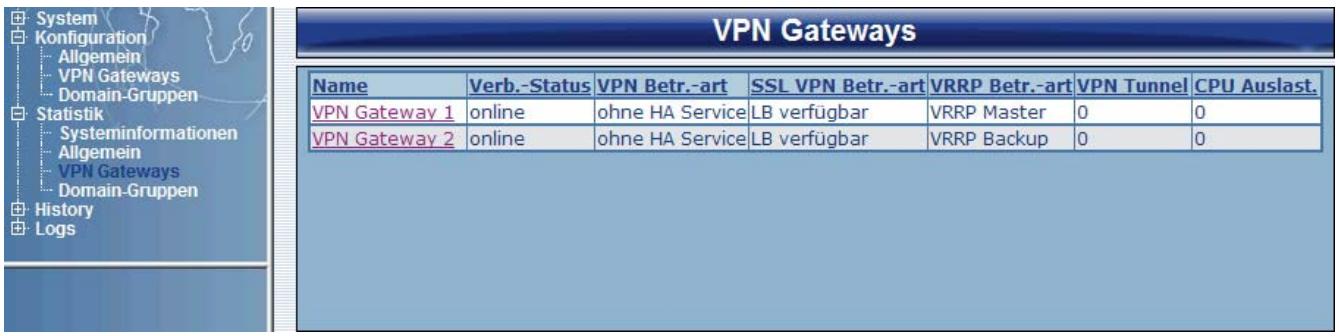


Die VRRP-ID von beiden Gateways muss gleich sein. Diese müssen später auch in der VRRP-Konfiguration der Secure Server unter “Routing Interfaces” eingetragen werden.

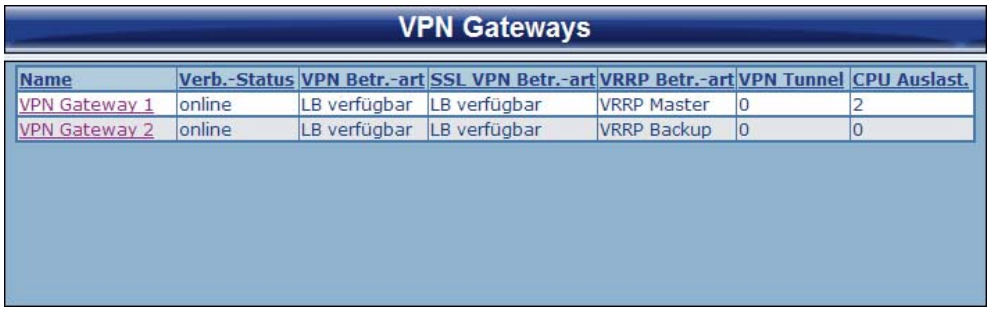
Der VPN-Modus muss auf “nur SSL VPN” oder “beide” geschaltet sein. (Mit “nur SSL VPN nimmt dieses Gateway nur SSL VPN-Verbindungen entgegen. Mit “beide” werden auf dem gleichen Gateway auch native VPN-Verbindungen entgegen genommen. (Beachten Sie dazu weiter unten die Beschreibung zum VPN-Modus.)

Nach dieser Konfiguration schaltet der HA Server ein Gateway als Master und das andere als Backup. Das Gateway, das in der Betriebsart “VRRP Backup” steht, nimmt in der ersten Phase des Verbindungsaufbaus keine Verbindungen an, nur das “VRRP Master”.

In der Statistik des HA Servers kann Status und Verfügbarkeit der Gateways für die jeweilige Betriebsart überprüft werden. (Abb. unten)



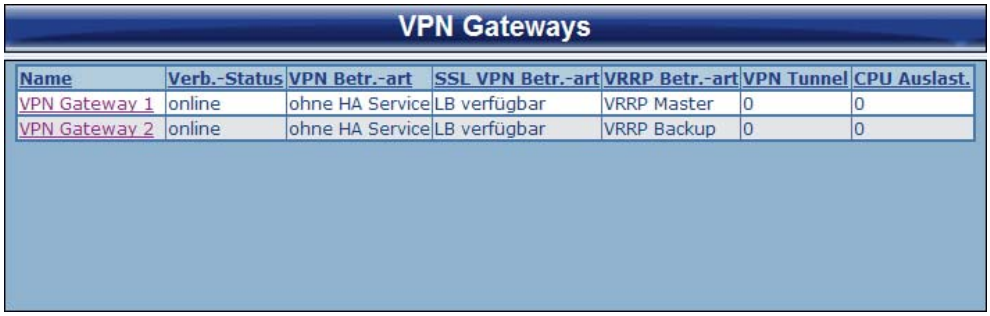
Name	Verb.-Status	VPN Betr.-art	SSL VPN Betr.-art	VRRP Betr.-art	VPN Tunnel	CPU Auslast.
VPN Gateway 1	online	ohne HA Service	LB verfügbar	VRRP Master	0	0
VPN Gateway 2	online	ohne HA Service	LB verfügbar	VRRP Backup	0	0



VPN Gateways

Name	Verb.-Status	VPN Betr.-art	SSL VPN Betr.-art	VRRP Betr.-art	VPN Tunnel	CPU Auslast.
VPN Gateway 1	online	LB verfügbar	LB verfügbar	VRRP Master	0	2
VPN Gateway 2	online	LB verfügbar	LB verfügbar	VRRP Backup	0	0

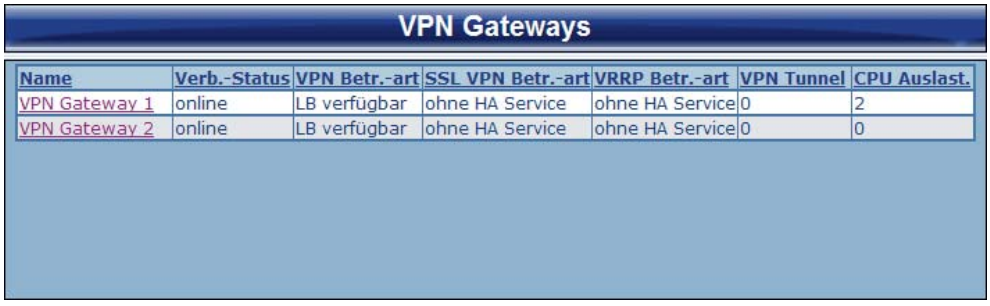
Wurde an den Gateways für den VPN-Modus jeweils “beide”, also ein Load Balancing sowohl für native VPN (IPsec/L2Sec Clients) plus SSL VPN Clients eingestellt, so müssen beide Gateways sowohl für die VPN HA-Betriebsart als auch für die SSL VPN HA-Betriebsart im LB-Modus verfügbar sein.



VPN Gateways

Name	Verb.-Status	VPN Betr.-art	SSL VPN Betr.-art	VRRP Betr.-art	VPN Tunnel	CPU Auslast.
VPN Gateway 1	online	ohne HA Service	LB verfügbar	VRRP Master	0	0
VPN Gateway 2	online	ohne HA Service	LB verfügbar	VRRP Backup	0	0

Wurde an den Gateways für den VPN-Modus jeweils “nur SSL VPN”, also kein Load Balancing für native VPN eingestellt, so dürfen beide Gateways nur für die SSL VPN HA-Betriebsart im LB-Modus verfügbar sein.



VPN Gateways

Name	Verb.-Status	VPN Betr.-art	SSL VPN Betr.-art	VRRP Betr.-art	VPN Tunnel	CPU Auslast.
VPN Gateway 1	online	LB verfügbar	ohne HA Service	ohne HA Service	0	2
VPN Gateway 2	online	LB verfügbar	ohne HA Service	ohne HA Service	0	0

Werden die Gateways ohne VRRP-Modus für Load Balancing konfiguriert, so können nur NCP DVE Clients über das HA-System verwaltet werden. Die VRRP-Betriebsart ist in diesem Fall nicht aktiviert und somit ein Load Balancing für die SSL VPN-Verbindungen nicht möglich.

Je nach Lizenzierung der High Availability Services können Gateways im LB-Modus für verschiedene Betriebsarten bzw. Clients gleichzeitig genutzt werden. Die als Master und Backup definierten Gateways können z. B. gleichzeitig für Load Balancing von “beiden”, native VPN- und SSL VPN-Verbindungen genutzt werden plus zusätzlich als Failsafe-System für IPsec Clients, die das DVEP nicht unterstützen.

VPN-Modus

Mit dem VPN-Modus wird entschieden für welche Verbindungen die lizenzierten VPN-Tunnels im Load Balancing-Modus genutzt werden sollen. Prinzipiell ist Load Balancing nur für NCP DVE Clients möglich.

Sollen die Tunnels darüber hinaus für SSL VPN-Verbindungen (im LB-Modus) oder für VPN-Verbindungen von Clients anderer Hersteller genutzt werden, so muss zusätzlich zum VPN-Modus der VRRP-Modus für Failsafe eingesetzt werden.

native VPN: Die Tunnels können für IPsec- oder L2Sec-Verbindungen von NCP Clients im Load Balancing-Modus genutzt werden. Wird zusätzlich der VRRP-Modus aktiviert, können gleichzeitig auch VPN-Verbindungen von Clients anderer Hersteller im Failsafe-Modus verwaltet werden.

nur SSL VPN: Sollen ausschließlich SSL VPN-Verbindungen über Load Balancing verteilt werden, so wird dieser Modus in Verbindung mit dem VRRP-Modus (siehe unten) gewählt. Ist der VRRP-Modus aktiviert, so ist für die SSL VPN-Verbindungen auch Ausfallsicherheit hergestellt, da dann über SSL VPN die gemeinsame VRRP IP-Adresse des Master- wie auch des Backup Gateways angesprochen werden kann.

beide: Sollen sowohl native VPN- wie auch SSL VPN-Verbindungen mit den gleichen Gateways über Load Balancing verteilt werden, so wird dieser Modus in Verbindung mit der VRRP-Betriebsart (siehe unten) eingestellt. (Dies gestattet darüber hinaus das Verbindungs-Management für VPN Clients anderer Hersteller im Failsafe-Modus.)

nur VRRP: Mit diesem VPN-Modus wird dieses Gateway für den Load Balancing-Modus ignoriert. Sollte das VRRP Master Gateway ausfallen, übernimmt das VRRP Backup Gateway dessen Funktion. Bei hoher Tunnelnutzung auf dem Master Gateway kann es daher sinnvoll sein auch das Backup Gateway “nur für VRRP” zu betreiben. Wird der VPN-Modus für beide Gateways auf “nur VRRP” gestellt, so können sie für SSL VPN Clients wie auch für VPN Clients anderer Hersteller im Failsafe-Modus genutzt werden.

VRRP-Modus

Mit dem VRRP-Modus wird festgelegt, ob ein Gateway (Master) mit einem zweiten Gateway (Backup) mit einer gemeinsamen VRRP IP-Adresse für Clients eingesetzt wird, die das NCP DVE-Protokoll nicht unterstützen oder nutzen.

inaktiv: Dieses Gateway wird nur für NCP Secure Enterprise Clients (DVE Clients) genutzt.

VRRP Master / Backup: Dieses Gateway besitzt mit einem zweiten Gateway eine gemeinsame virtuelle IP-Adresse, die für nicht-DVE-fähige Clients genutzt werden kann.

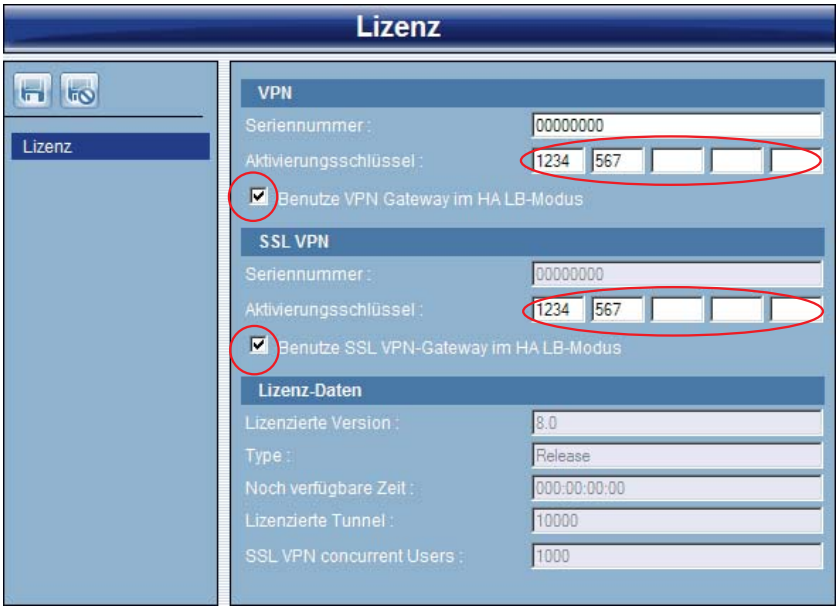
Das VRRP Master und das VRRP Backup Gateway stellen innerhalb des Load Balancing-Verbunds die VRRP Failsafe-Funktionalität für VPN Clients ohne DVE-Unterstützung bereit.

Ein SSL VPN-Verbindungaufbau über Browser erfolgt in zwei Phasen. Zunächst wird nach der VRRP Failsafe-Funktionalität immer das VRRP Master Gateway kontaktiert. In der zweiten Phase wird die Verbindung zu einem weniger ausgelasteten Gateway des Load Balancing-Verbunds (sofern konfiguriert) aufgebaut. Die IP-Adresse dazu wird dem Browser über HTTP Redirect mitgeteilt.

Bitte beachten Sie beim Einsatz von VRRP unter Linux den Abschnitt **VRRP-Adressierung mit Gateways unter Linux** in dieser Dokumentation.

Konfiguration am Secure Server

Um den Secure Server im Load Balancing-Modus nutzen zu können, muss die Lizenz dafür freigeschaltet werden.



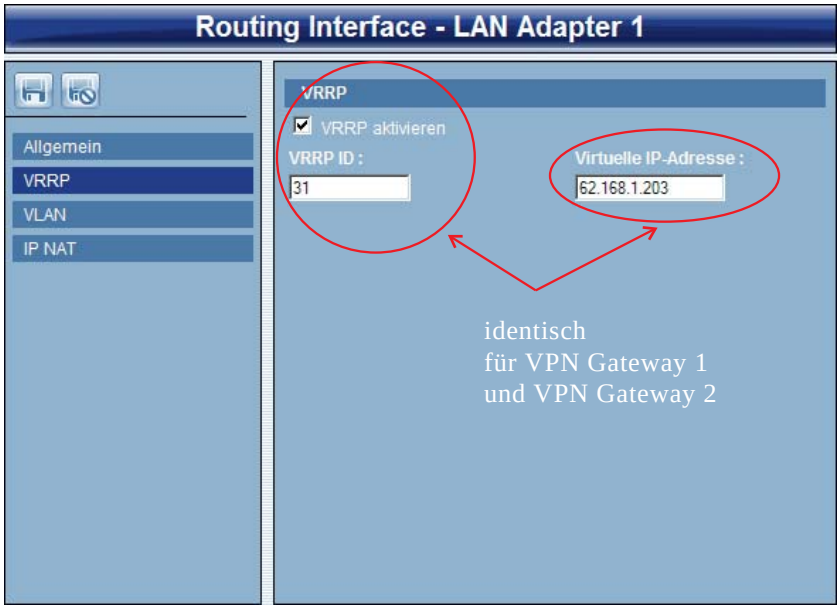
Im Konfigurationsmenü des Secure Server wird unter “System / Lizenz / VPN” der LB-Modus für Verbindungen von Enterprise Clients oder native VPN-Verbindungen ohne DVEP freigeschaltet.

Unter “SSL VPN” wird der LB-Modus für Verbindungen freigeschaltet, die per Browser über SSL VPN hergestellt werden.

Bitte beachten Sie, dass die LB-Lizenzierung für alle Gateways erfolgen muss, die über einen HA Server in einem Load Balancing-Verbund verwaltet werden.

Erst mit der LB-Lizenz für SSL VPN werden in der Listener-Konfiguration des Gateways die “HA Load Balancing-Optionen” wirksam (siehe unten **Listener-Konfiguration**).

Die Gateways werden wie folgt konfiguriert.



An der externen Schnittstelle von Gateway 1 wird unter “Routing Interfaces / LAN Adapter 1" VRRP aktiviert und die VRRP ID eingetragen, die auch mit dem HA-Konfiguration für Gateway 1 eingetragen wurde (hier 31). Schließlich wird die virtuelle IP-Adresse vergeben, die vorher festgelegt wurde (hier 62.168.1.203).

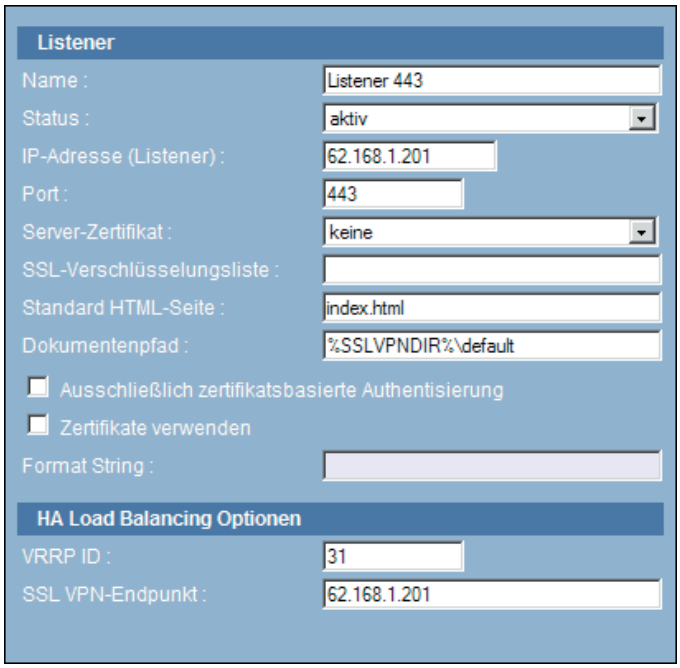
Ebenso wird an der externen Schnittstelle von Gateway 2 unter “Routing Interfaces / LAN Adapter 1" VRRP aktiviert und die gleiche VRRP ID eingetragen wie für Gateway 1, die gleiche die auch in der HA-Konfiguration für Gateway 2 eingetragen wurde (hier 31). Schließlich wird die virtuelle IP-Adresse vergeben, die vorher festgelegt wurde (hier 62.168.1.203).

Konfiguration am Netzwerkadapter

Im Anschluss kann die gemeinsame virtuelle IP-Adresse jeweils an die entsprechenden physikalischen Adapter gebunden werden.

Zum Eintragen der gemeinsamen IP-Adressen öffnen Sie jeweils die Eigenschaften der Netzwerkadapter und fügen in den erweiterten TCP/IP-Einstellungen zusätzlich zur ersten IP-Adresse als zweite IP-Adresse die gemeinsame virtuelle IP-Adresse hinzu. Beachten Sie dazu die Beschreibung oben zur **Konfiguration der Netzwerkadapter** im Failsafe-Modus mit VRRP.

Nach dieser Änderung der Netzwerkeinstellungen müssen die Dienste neu gestartet werden.



Konfiguration der Listener (SSL VPN-Konfiguration)

Sowohl für Gateway 1 wie auch für Gateway 2 müssen jeweils 2 Listener angelegt werden. Dies erfolgt in der Server-Konfiguration unter SSL VPN / Listener.

Der 1. Listener erhält (siehe Abb. links unten):
– als IP-Adresse (Listener) die physikalische IP-Adresse des Gateways (hier 62.168.1.201).
– als VRRP ID diejenige, die auch unter den “Routing Interfaces” und am HA Server vergeben wurde (hier 31).
– als SSL VPN-Endpunkt den Hostnamen oder die IP-Adresse (ggf. einschließlich Port), die der Browser per HTTPS Redirect erhalten soll. In diesem Beispiel ist es die offizielle IP-Adresse des eigenen Listeners, d. h. die offizielle IP-Adresse von Gateway 1.

(Der SSL VPN Tunnel-Endpunkt ist in der Regel immer die offizielle physikalische IP-Adresse des Gateways, es sei denn die Verbindung wird über eine Firewall hergestellt; dann wird hier die Adresse eingetragen, die im Browser eingegeben werden muss, um das Gateway über die Firewall zu erreichen.)

Wird nicht der Standard-Port für http (443) verwendet, kann optional zusätzlich ein Port angegeben werden. Syntax:
`hostname:port`

Der 2. Listener erhält:
– als IP-Adresse (Listener) die virtuelle VRRP IP-Adresse (hier 62.168.1.203).
– als VRRP ID die gleiche wie der 1. Listener, nämlich ebenso diejenige, die auch unter den “Routing Interfaces” und am HA Manager vergeben wurde (hier 31).
– als SSL VPN-Endpunkt wird **keine** Adresse eingetragen.

Weitere Dokumentationen

HA-Funktionsbeschreibung

HA-Installation und Web-Interface

HA-Parameterbeschreibung

SES-Parameter (Secure Enterprise Server)