Hinweise zur Kommunikation mit BRAVIS zwischen mehreren Unternehmensstandorten

Inhaltsverzeichnis

Über BRAVIS

BRAVIS Videokonferenzsysteme

BRAVIS ist ein innovatives Mehrteilnehmer-Videokonferenzsystem für geschlossene Gruppen im Internet. Es benötigt keinen zentralen Konferenzserver. BRAVIS ist ein Desktop-System, dass es erlaubt, Konferenzen vom Arbeitsplatz aus mittels Workstation oder PC spontan zu starten. Es wurde insbesondere für Beratungen, Diskussionen und Konsultationen von Gruppen zwischen 2 bis 16 Personen entworfen.

Die Geschlossenheit der Gruppe wird über die Signalisierung gesichert. Damit können geschlossene Treffen, wie sie im täglichen Leben überwiegend vorkommen, im Internet nachgebildet werden. BRAVIS-Systeme vereinen die Vorzüge verschiedenster Videokonferenzsysteme. Zu seinen Funktionen zählen u. a. Moderation, Whiteboard, Application Sharing und Dateitransfer. Für Installation und Bedienung sind keine Vorkenntnisse erforderlich. Außer Webcam und Headset oder Communicator wird keine zusätzliche Hardware benötigt.

Kontakt

BRAVIS International GmbH
Calauer Str. 70
03048 Cottbus

Tel. +49 (0)355 - 290 243 20
Fax +49 (0)355 - 290 243 24

E-Mail: support@bravis.eu
Internet: www.bravis.eu

Basiseinstellungen

Folgende Basiseinstellungen sollten vorhanden bzw. konfiguriert werden, um einen Einsatz von BRAVIS zu gewährleisten.

- Auf dem Rechner, auf dem BRAVIS läuft, muss der DNS-Dienst mit dem Port 53/TCP+UDP aktiviert sein, um Hostnamen in IP-Adressen umwandeln zu können.

- Für Produktaktivierung und Lizenzprüfung sind Verbindungen über Port 443/TCP (HTTPS) zu *dongle.bravis.de* erforderlich.

- Für den Update-Check der Software ist eine Verbindung über Port 80/TCP (HTTP) zu *support.bravis.de* nötig. Der Update-Check ist jedoch optional und wirkt sich nicht auf die grundlegende Funktionsweise des Programms aus.

- Für die Verweise auf das Handbuch und die Supportseiten auf den BRAVIS-Servern wird ein installierter Standardbrowser mit Webzugriff auf die Domäne *bravis.de* vorausgesetzt.

- Gegebenenfalls müssen Sie in den BRAVIS Optionen, im Menüpunkt „Netzwerk“ → „Erweitert“ die IP-Adresse und den Port Ihres HTTP/HTTPS-Proxies hinterlegen, falls ein solcher in Ihrem Unternehmen eingesetzt wird.

- Die BRAVIS-Software muss zu den Regeln der Windows-internen Firewall für den uneingeschränkten Zugriff hinzugefügt werden und darf nicht von einer Personal-Firewall blockiert werden. Diese muss evtl. vorher mit Administrator-Rechten konfiguriert werden.

Anbindung verschiedener Unternehmensstandorte

Flexible Standardlösung

Einsatzmöglichkeiten

- Wenn **kein** NAT-Router mit einer symmetrischen NAT eingesetzt wird, kann die hier beschriebene Konfiguration eingesetzt werden.
- Sollte eine Kommunikation mit vielen dynamisch wechselnden Partnern stattfinden, wird dieses Szenario empfohlen.

Konfiguration

Um eine flexible Konfiguration zwischen den verschiedenen Unternehmensstandorten und zu externen Konferenzteilnehmern (z.B. Kunden) zu erreichen, die wenig administrativen Aufwand für den zuständigen Administrator bedeutet, sind die folgenden Einstellungen an den Routern/Firewalls der beteiligten Niederlassungen eines Unternehmens zu konfigurieren.

Im NAT-Router/Firewall sollten folgende Regeln für das lokale Netz oder die einzelnen PCs, die BRAVIS nutzen, eingerichtet werden:

```
OUT: <source UDP lan:5530> <destination UDP any:any> <allow>  set <mark>
IN:  <source UDP any:any> <destination UDP lan:any> condition <mark>
```

Erklärung: Vom BRAVIS-Port (voreingestellt ist 5530/UDP) jedes PCs im internen LAN müssen Anfragen an jeden UDP-Port im öffentlichen Netz möglich sein. Auf diese ausgehenden Anfragen folgende hereinkommende Antwortpakete an den Absende-Port müssen akzeptiert werden.

Sollte bloß für einzelne PCs die Kommunikation mit BRAVIS erlaubt werden, kann dies durch die nachstehenden Firewall-Regeln sichergestellt werden:

```
OUT: <source UDP pc1:5530> <destination UDP any:any> <allow> set <mark>
IN:  <source UDP any:any> <destination UDP pc1:any> condition <mark>

OUT: <source UDP pc2:5530> <destination UDP any:any> <allow> set <mark>
IN:  <source UDP any:any> <destination UDP pc2:any> condition <mark>

OUT: <source UDP pc3:5530> <destination UDP any:any> <allow> set <mark>
IN:  <source UDP any:any> <destination UDP pc3:any> condition <mark>

OUT: <source UDP pc4:5530> <destination UDP any:any> <allow> set <mark>
IN:  <source UDP any:any> <destination UDP pc4:any> condition <mark>
```

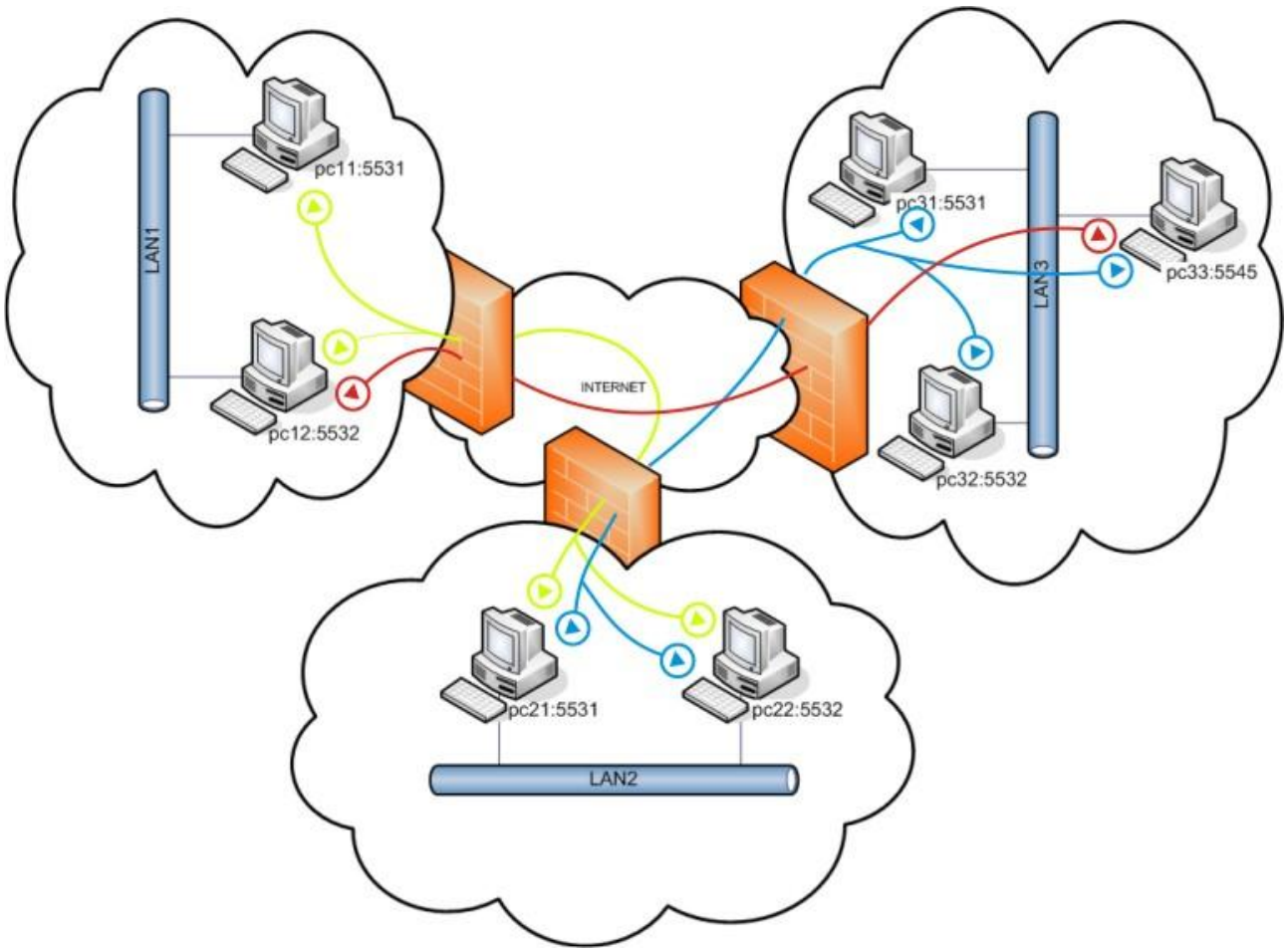
Auf höhere Sicherheit ausgelegte Konfiguration

Einsatzmöglichkeiten

- Wenn **ein** NAT-Router mit einer symmetrischen NAT eingesetzt wird, muss die hier beschriebene Konfiguration eingesetzt werden.
- Bei dieser Konfiguration ist eine Kommunikation zu vorher definierten Kommunikationspartnern gewährleistet. Für zusätzliche dynamisch wechselnde BRAVIS-Gegenstellen ist jedoch ein erhöhter administrativer Aufwand nötig.
- Diese Konfiguration ist unflexibler, gewährleistet dafür jedoch eine höhere Sicherheit. Sollte eine Kommunikation mit vielen dynamisch wechselnden Partnern stattfinden, wird stattdessen die vorhergehende *Flexible Standardlösung* empfohlen.

Konfiguration

Die hier beschriebene Konfiguration gewährleistet ein sehr hohes Maß an Sicherheit, erfordert aber die vorherige Definition von potentiellen Kommunikationspartnern. Das hier aufgeführte Beispiel symbolisiert die Kommunikation zwischen 3 Unternehmensstandorten, wobei alle PCs, die BRAVIS nutzen, zwischen den Netzwerken LAN1 und LAN2 sowie LAN2 und LAN3 kommunizieren dürfen. Zwischen LAN1 und LAN3 darf nur jeweils ein PC eine vorher festgelegte Gegenstelle des anderen LANs (PC12/LAN1 ← BRAVIS → PC33/LAN3) erreichen. Diese Konfiguration ist in der folgenden Abbildung skizziert:



- Auf jedem Rechner, auf dem BRAVIS eingesetzt wird, sollte ein eigener BRAVIS-Kommunikationsport (Standard 5530) konfiguriert werden.

```
lan1                lan2                lan3
pc11:5531           pc21:5531           pc31:5531
pc12:5532           pc22:5532           pc32:5532
                                        pc33:5545
```

- Im NAT-Router/Firewall sollte ein Port-Forwarding eingerichtet werden.

```
lan1                                lan2
ExterneIP:5531 > pc11:5531          ExterneIP:5531 > pc21:5531
ExterneIP:5532 > pc12:5532          ExterneIP:5532 > pc22:5532

lan3
ExterneIP:5531 > pc31:5531
ExterneIP:5532 > pc32:5532
ExterneIP:5545 > pc33:5545
```

Für jeden internen Port (BRAVIS Kommunikationsport) wird vom externen Port ein Port Forwarding (manchmal auch als Portweiterleitung oder Portfreigabe bezeichnet) eingerichtet. Es sollte darauf geachtet werden, dass jeder Port einzigartig ist und keine Port Redirection (Portumleitung) konfiguriert wird, d.h. interner und externer Port müssen identisch sein.

Welcher Port für BRAVIS konfiguriert wird, ist egal. Es sollte aber nicht der BRAVIS-Standard-Port 5530 sein, da u.U. später hinzukommende PCs diesen nutzen, bevor BRAVIS neu konfiguriert wird. Dadurch kann es passieren, das BRAVIS nicht ordnungsgemäß funktioniert und es zu Komplikationen führt.

Hinweis: Sollte die Vergabe der IP-Adressen über DHCP erfolgen, muss eine Reservierung der jeweiligen IP-Adressen über die MAC-Adresse im DHCP Server konfiguriert werden.

- Im NAT-Router/Firewall sollte Regel erstellt.

Regeln für Lan1:

```
OUT: <source UDP pc11:5531> <destination UDP sipserver:5060> <allow> set <mark>
IN:  <source UDP sipserver:any> <destination UDP pc11:5531> condition <mark>

OUT: <source UDP pc11:5531> <destination UDP stunserver:3478> <allow> set <mark>
IN:  <source UDP stunserver:any> <destination UDP pc11:5531> condition <mark>

OUT: <source UDP pc12:5532> <destination UDP sipserver:5060> <allow> set <mark>
IN:  <source UDP sipserver:any> <destination UDP pc12:5532> condition <mark>

OUT: <source UDP pc12:5532> <destination UDP stunserver:3478> <allow> set <mark>
IN:  <source UDP stunserver:any> <destination UDP pc12:5532> condition <mark>

OUT: <source UDP pc11:5531> <destination UDP lan2:5531-5532> <allow> set <mark>
IN:  <source UDP lan2:5531-5532> <destination UDP pc11:5531> condition <mark>

OUT: <source UDP pc12:5532> <destination UDP lan2:5531-5532> <allow> set <mark>
IN:  <source UDP lan2:5531-5532> <destination UDP pc12:5532> condition <mark>

OUT: <source UDP pc12:5532> <destination UDP lan3:5545> <allow> set <mark>
IN:  <source UDP lan3:5545> <destination UDP pc12:5532> condition <mark>
```

Regeln für Lan2:

```
OUT: <source UDP pc21:5531> <destination UDP sipserver:5060> <allow> set <mark>
IN:  <source UDP sipserver:any> <destination UDP pc21:5531> condition <mark>

OUT: <source UDP pc21:5531> <destination UDP stunserver:3478> <allow> set <mark>
IN:  <source UDP stunserver:any> <destination UDP pc21:5531> condition <mark>
```

```
OUT: <source UDP pc22:5532> <destination UDP sipserver:5060> <allow> set <mark>
IN:  <source UDP sipserver:any> <destination UDP pc22:5532> condition <mark>

OUT: <source UDP pc22:5532> <destination UDP stunserver:3478> <allow> set <mark>
IN:  <source UDP stunserver:any> <destination UDP pc22:5532> condition <mark>

OUT: <source UDP pc21:5531> <destination UDP lan1:5531-5532> <allow> set <mark>
IN:  <source UDP lan1:5531-5532> <destination UDP pc21:5531> condition <mark>

OUT: <source UDP pc22:5532> <destination UDP lan1:5531-5532> <allow> set <mark>
IN:  <source UDP lan2:5531-5532> <destination UDP pc12:5532> condition <mark>

OUT: <source UDP pc21:5531> <destination UDP lan3:5531-5545> <allow> set <mark>
IN:  <source UDP lan3:5531-5545> <destination UDP pc21:5531> condition <mark>

OUT: <source UDP pc22:5532> <destination UDP lan3:5531-5545> <allow> set <mark>
IN:  <source UDP lan3:5531-5545> <destination UDP pc22:5532> condition <mark>
```

Regeln für Lan3:

```
OUT: <source UDP pc31:5531> <destination UDP sipserver:5060> <allow> set <mark>
IN:  <source UDP sipserver:any> <destination UDP pc31:5531> condition <mark>

OUT: <source UDP pc31:5531> <destination UDP stunserver:3478> <allow> set <mark>
IN:  <source UDP stunserver:any> <destination UDP pc31:5531> condition <mark>

OUT: <source UDP pc32:5532> <destination UDP sipserver:5060> <allow> set <mark>
IN:  <source UDP sipserver:any> <destination UDP pc22:5532> condition <mark>

OUT: <source UDP pc32:5532> <destination UDP stunserver:3478> <allow> set <mark>
IN:  <source UDP stunserver:any> <destination UDP pc22:5532> condition <mark>

OUT: <source UDP pc33:5545> <destination UDP sipserver:5060> <allow> set <mark>
IN:  <source UDP sipserver:any> <destination UDP pc33:5545> condition <mark>

OUT: <source UDP pc33:5545> <destination UDP stunserver:3478> <allow> set <mark>
IN:  <source UDP stunserver:any> <destination UDP pc33:5545> condition <mark>

OUT: <source UDP pc33:5545> <destination UDP lan1:5532> <allow> set <mark>
IN:  <source UDP lan1:5532> <destination UDP pc33:5545> condition <mark>

OUT: <source UDP pc31:5531> <destination UDP lan2:5531-5532> <allow> set <mark>
IN:  <source UDP lan2:5531-5532> <destination UDP pc31:5531> condition <mark>

OUT: <source UDP pc32:5532> <destination UDP lan2:5531-5532> <allow> set <mark>
IN:  <source UDP lan2:5531-5532> <destination UDP pc32:5532> condition <mark>

OUT: <source UDP pc33:5545> <destination UDP lan2:5531-5532> <allow> set <mark>
IN:  <source UDP lan2:5531-5532> <destination UDP pc33:5545> condition <mark>
```

VPN Verbindung zwischen Unternehmensstandorten

Ist eine VPN-Verbindung zwischen den einzelnen Unternehmensstandorten vorhanden, kann diese für die Kommunikation zwischen den PCs, die BRAVIS einsetzen, genutzt werden.

Site-to-Site VPN

Sind zwei lokale Netze durch VPN-Gateways verbunden, bauen diese untereinander eine VPN-Verbindung auf, die meist permanent bestehen bleibt. Alle PCs aus dem lokalen Unternehmensnetzen können nun das VPN-Gateway verwenden, um Daten in das andere Netz zu senden.

Der Kommunikationsaufbau erfolgt über die Hostadressen (Hostname oder IP-Adresse). Um dies über den Hostnamen zu gewährleisten, müssen die Hostnamen der PCs, die mit BRAVIS kommunizieren, im lokalen DNS (standortübergreifend) verfügbar sein.

End-to-Site / Client-to-Site VPN

Sind einzelne PCs eines Unternehmensstandortes oder einzelnen Mitarbeiter aus Ihrem Home-Office über einen VPN-Client mit einem weiteren Unternehmensstandort verbunden, kann eine Kommunikation über BRAVIS nur durch einen dieser PCs zum Unternehmensstandort, der ein VPN Gateway nutzt, aufgebaut werden. Soll auch vom Unternehmensstandort (mit VPN Gateway) eine Verbindung über BRAVIS zu den PCs mit VPN Client erfolgen, muss dieser VPN Client vorher gestartet werden.

Der Kommunikationsaufbau erfolgt über die Hostadressen (Hostname oder IP-Adresse). Um dies über den Hostnamen zu gewährleisten müssen die Hostnamen der PCs die mit BRAVIS Kommunizieren im lokalen DNS (standortübergreifend) verfügbar sein.

VPN Kommunikationssteuerung

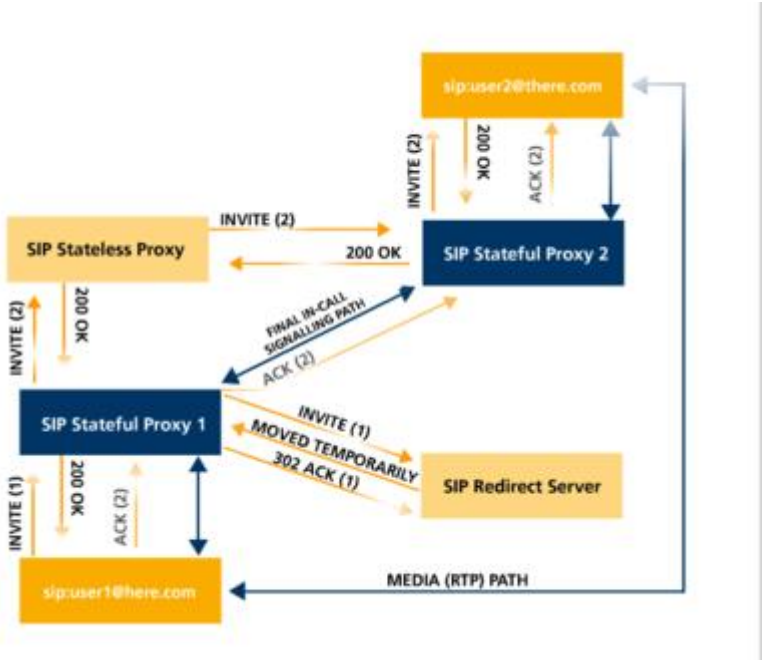
Eine Kommunikation über BRAVIS durch die VPN Verbindungen, kann bei Bedarf durch das Konfigurieren von Regeln, wie sie im Abschnitt *Anbindung verschiedener Unternehmensstandort*“ beschrieben worden sind, gesteuert bzw. eingeschränkt werden.

Session Initiation Protocol (SIP)

Definition

Das Session Initiation Protocol (SIP) ist ein Netzprotokoll zum Aufbau einer Kommunikationssitzung zwischen zwei und mehr Teilnehmern. Das Protokoll wird im RFC 3261 (früher RFC 2543) spezifiziert. In der IP-Telefonie ist SIP ein häufig angewandtes Protokoll. SIP ähnelt stark dem HTTP-Protokoll – es verwendet eine ähnliche Header-Struktur und ist ebenfalls ein textbasiertes Protokoll. Zur Schreibweise der Teilnehmeradressen wird das von E-Mail bekannte URI-Format benutzt: "sip:user@domain".

SIP dient lediglich dazu, die Kommunikationsmodalitäten zu vereinbaren bzw. auszuhandeln – die eigentlichen Daten für die Kommunikation werden über andere, dafür geeignete Protokolle ausgetauscht. Zu den Vorteilen von SIP gehört, dass es sich hierbei um einen offenen Standard handelt, der mittlerweile sehr weite Verbreitung gefunden hat.



SIP Server

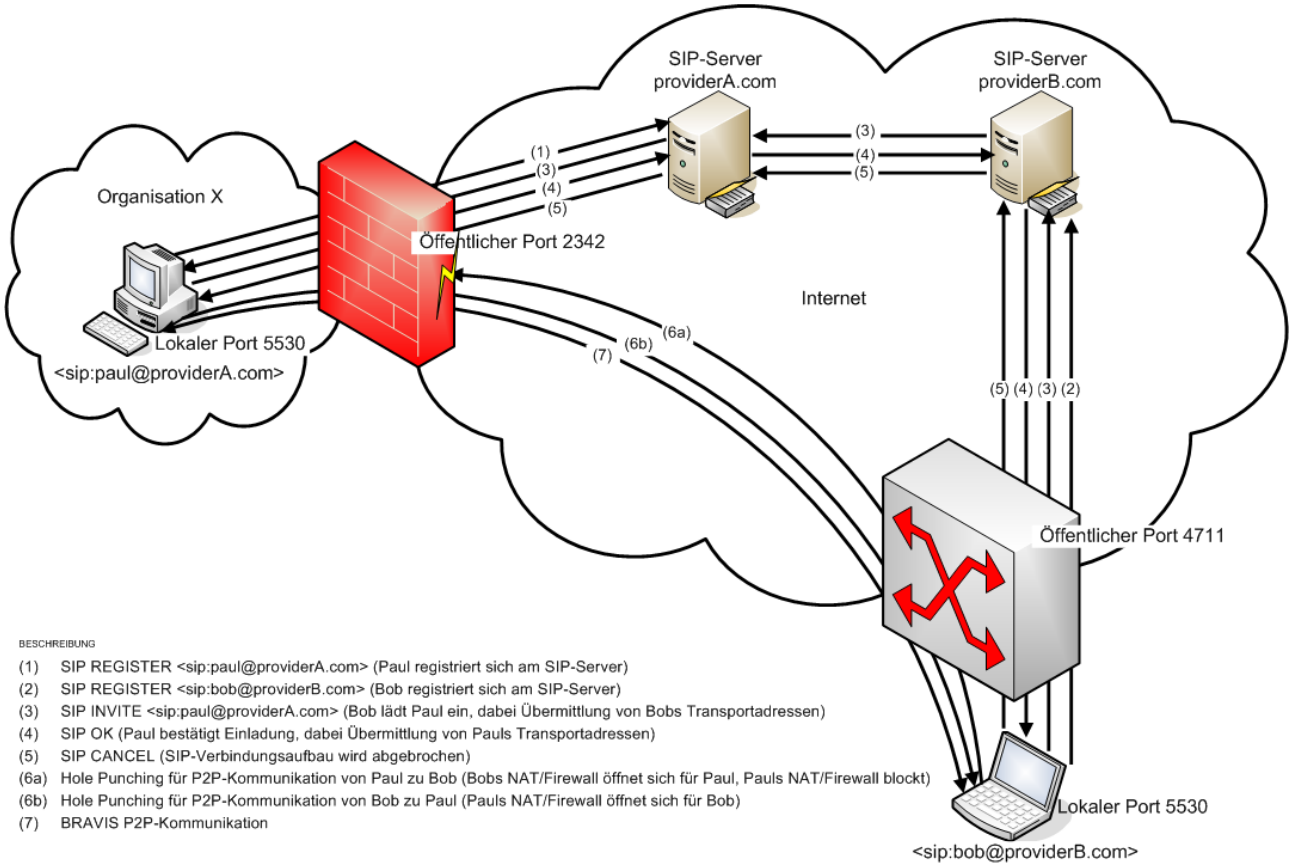
In BRAVIS wird die SIP-Adresse für den Verbindungsaufbau zwischen Clients benötigt, **die über keine dauerhaft feste IP-Adresse verfügen**, d.h. zwischen Nutzern, welche über eine NAT (Network Address Translation) eine Verbindung zum Internet herstellen oder trotz wechselnder Standorte nur mit einer Adresse erreichbar sein wollen.

Bei der Installation der BRAVIS Software können Sie sich eine BRAVIS-SIP Adresse anlegen.

Es besteht auch die Möglichkeit einen eigenen SIP-Server oder eine bestehende SIP-Adresse eines anderen SIP-Anbieters zu benutzen.

BRAVIS SIP Kommunikation

Der BRAVIS-Verbindungsaufbau erfolgt über SIP, wie es im folgenden Schema dargestellt wird:



HINWEIS:
Es ist zu beachten, dass der eingesetzte DNS-Dienst auch externe Hostnamen auflösen muss. Sollte dies nicht der Fall sein, sollte der DNS-Dienst in die Unternehmens-DMZ ausgegliedert werden und so konfiguriert werden, dass er auch externe Domänennamen auflöst. Sollte auch dies nicht möglich sein, sollte der eigene externe SIP-Provider in den lokalen DNS mit aufgenommen werden oder ein eigener interner SIP Service installiert werden.

Alternativ zu SIP kann auch ein Verbindungsaufbau über die Hostadressen (Hostname oder IP-Adresse) erfolgen. Um dies über den Hostnamen zu gewährleisten müssen die Hostnamen der PCs, die mit BRAVIS kommunizieren, im lokalen DNS (standortübergreifend) verfügbar sein.

Simple Traversal of UDP over NATs (STUN)

Definition

STUN (Simple Traversal of UDP over NATs = einfaches Überqueren von UDP über NAT) ist ein einfaches Netzwerkprotokoll um das Vorhandensein und die Art von Firewalls und NAT-Routern zu erkennen und letztere zu durchdringen. Es soll den unkomplizierten Einsatz von Geräten (z. B. SIP-Telefone) und Computer-Programmen in Heimnetzwerken ermöglichen, welche Daten aus dem Internet empfangen möchten. Derzeit wird STUN hauptsächlich im VoIP-Bereich im Zusammenhang mit SIP eingesetzt.

Mit Hilfe von STUN kann BRAVIS die derzeit öffentliche IP-Adresse des Anschlusses ermitteln. So kann ein BRAVIS-Endsystem seine derzeit gültige IP-Adresse ermitteln und mittels SIP seinem Kommunikationspartner beim Verbindungsaufbau mitteilen. Dies ist nötig, damit die Gegenstelle ihre Konferenzdaten korrekt adressieren kann. Bei den derzeit vorhandenen NAT-Routern kann grob zwischen vier NAT-Typen unterschieden werden: Full Cone NAT, Restricted Cone NAT, Port Restricted NAT und Symmetric NAT. Mit Ausnahme von symmetrischen NATs kann BRAVIS automatisch die notwendigen Kommunikationsbeziehungen herstellen. Wird eine symmetrische NAT eingesetzt, so ist in der Regel eine manuelle Konfiguration der NAT erforderlich (siehe nachfolgende Konfigurationsbeispiele).

Im nachstehenden Bild ist erläutert, wie mit Hilfe von STUN der Typ der Firewall oder des NAT-Router ermittelt wird: