„MATRIX“

„Eine Einführung in Matrix“

„Thema: Eine Einführung in Matrix“

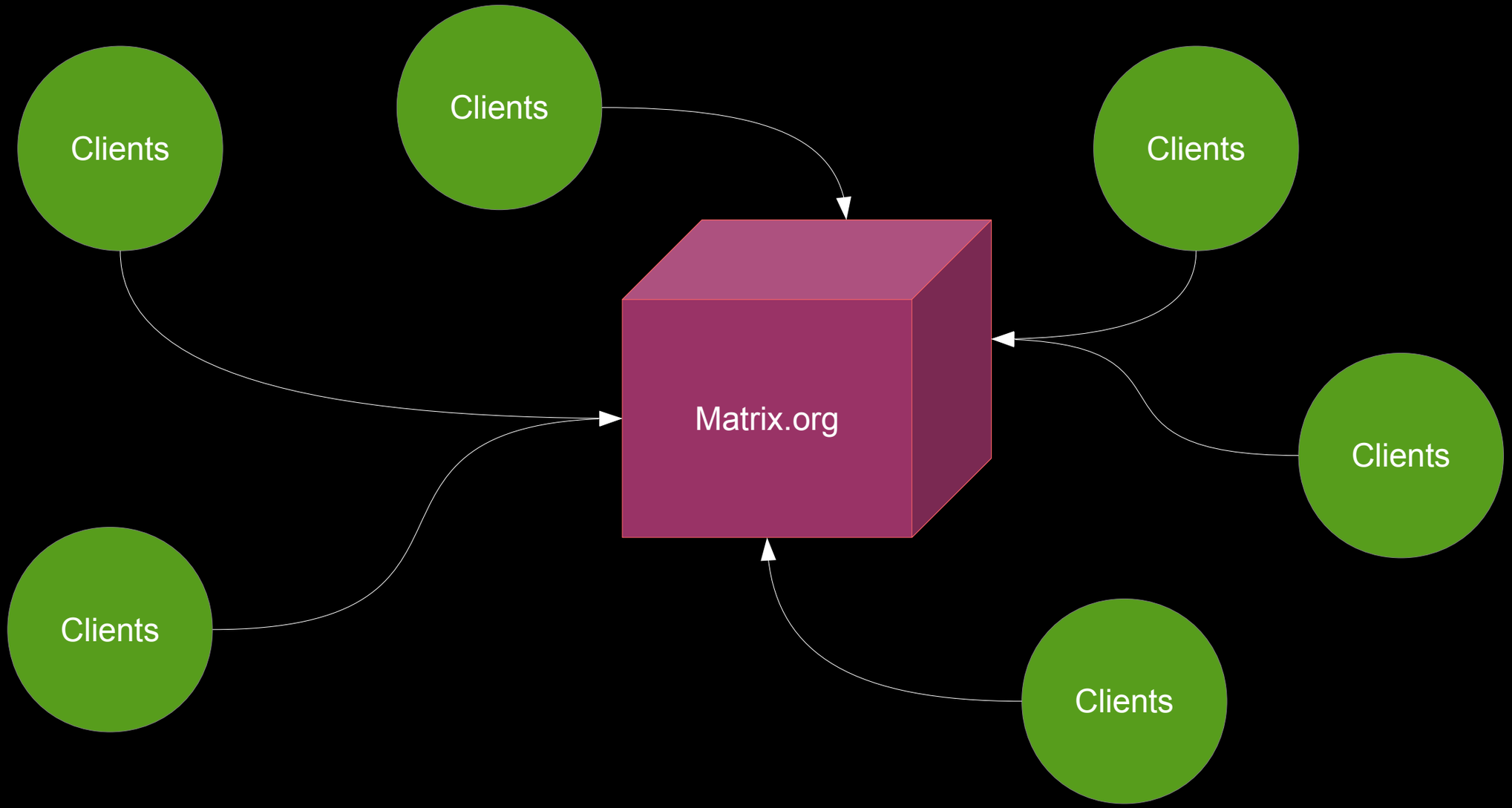
Matrix ist ein dezentrales und föderiertes Nachrichtenverteilsystem.

„Thema: Eine Einführung in Matrix“

Matrix ist ein dezentrales und föderiertes Nachrichtenverteilsystem.

Und was meint das?

„Thema: Eine Einführung in Matrix“

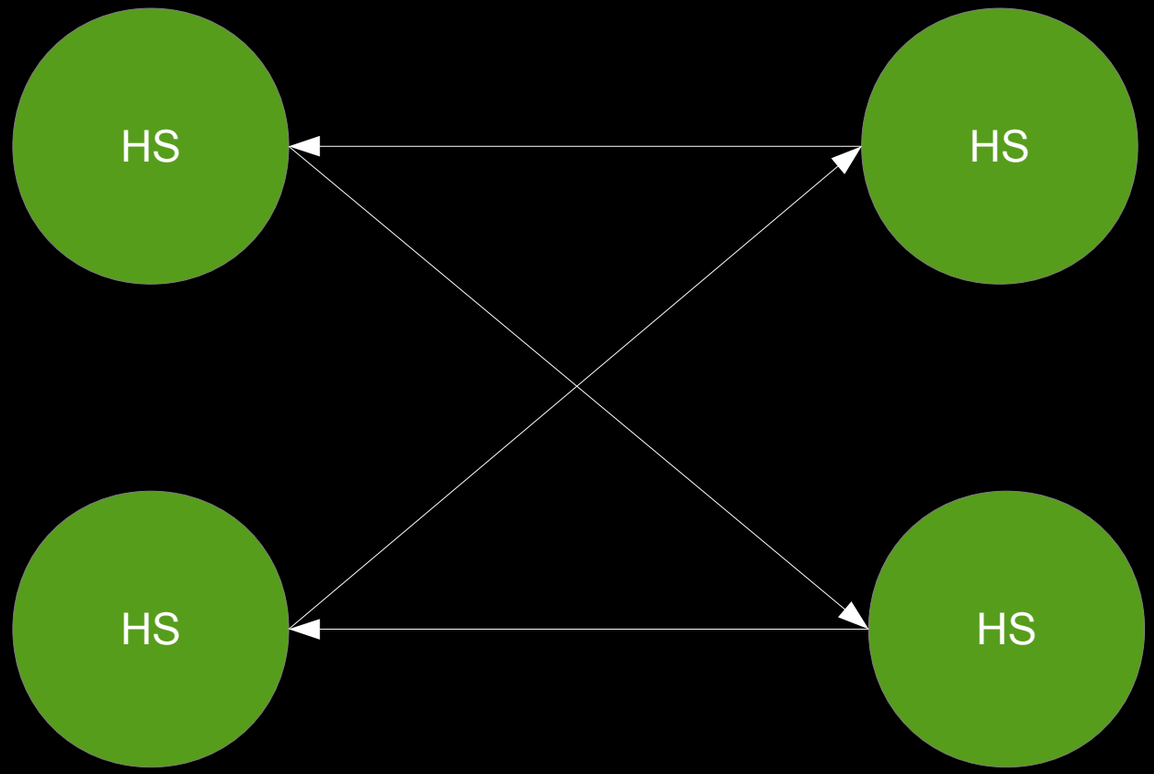


„Thema: Eine Einführung in Matrix“

„Thema: Eine Einführung in Matrix“

In **Matrix** reden **H**ome**s**erver miteinander.

„Thema: Eine Einführung in Matrix“



„Thema: Eine Einführung in Matrix“

Müssen die sich kennen?

„Thema: Eine Einführung in Matrix“

überraschende Antwort: **Nein** :)

„Thema: Eine Einführung in Matrix“

Jeder **Homeserver** hat einen eigenen **Domainnamen**.

„Thema: Eine Einführung in Matrix“

Jeder **Homeserver** hat einen eigenen **Domainnamen**.

Eine **Matrixkennung** basiert auf dem **Domainnamen**.

„Thema: Eine Einführung in Matrix“

Beispiel:

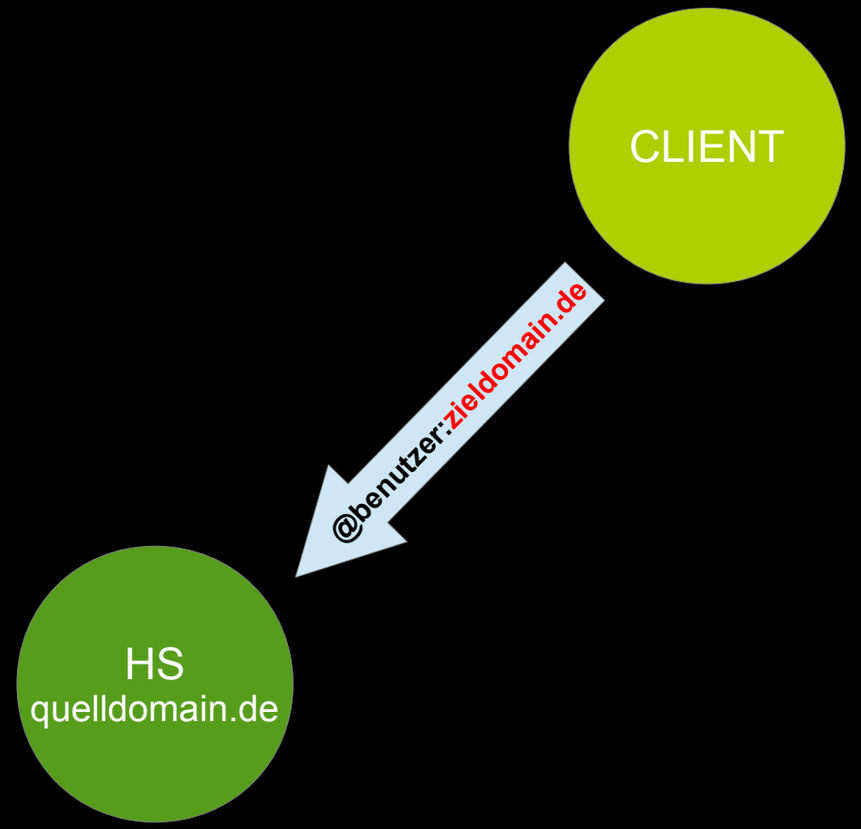
@marius:linuxphones.de

„Thema: Eine Einführung in Matrix“

Anhand des Domainnamens findet ein **Matrixserver**

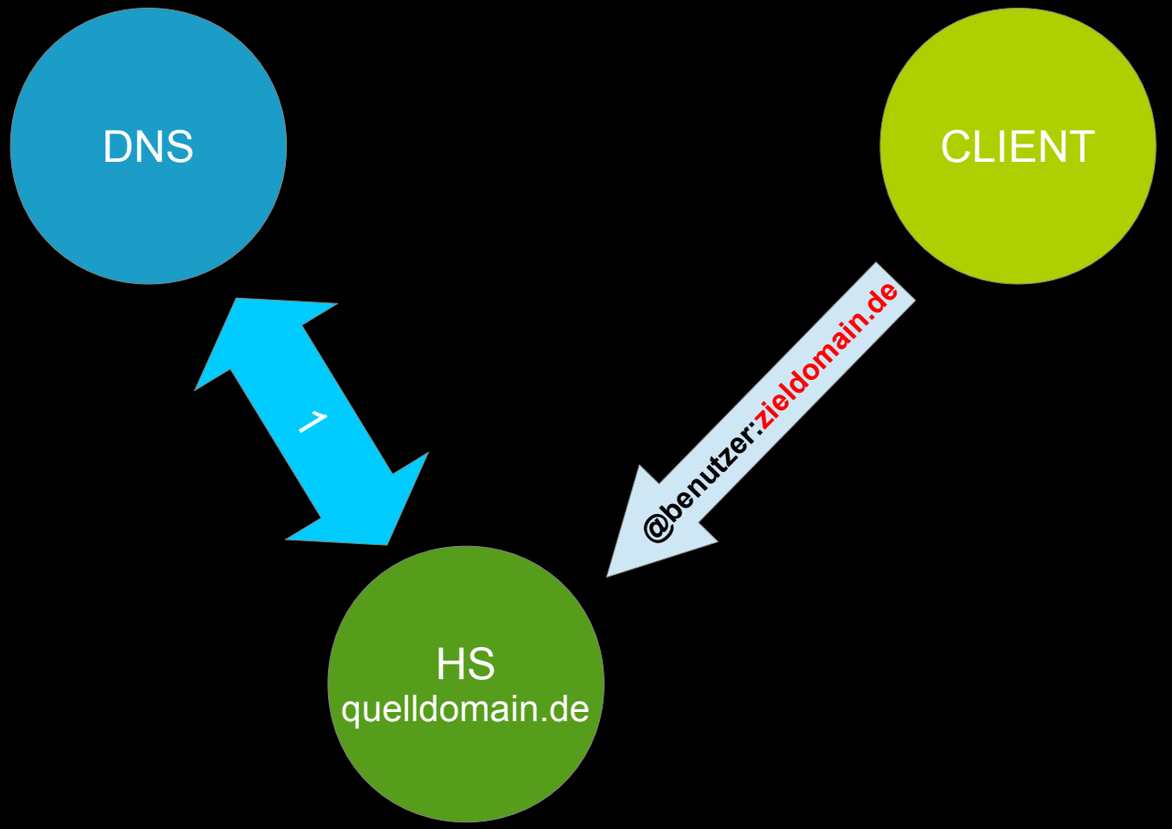
den Homeserver des Empfängers.

„Thema: Eine Einführung in Matrix“
Nachrichtenaustausch



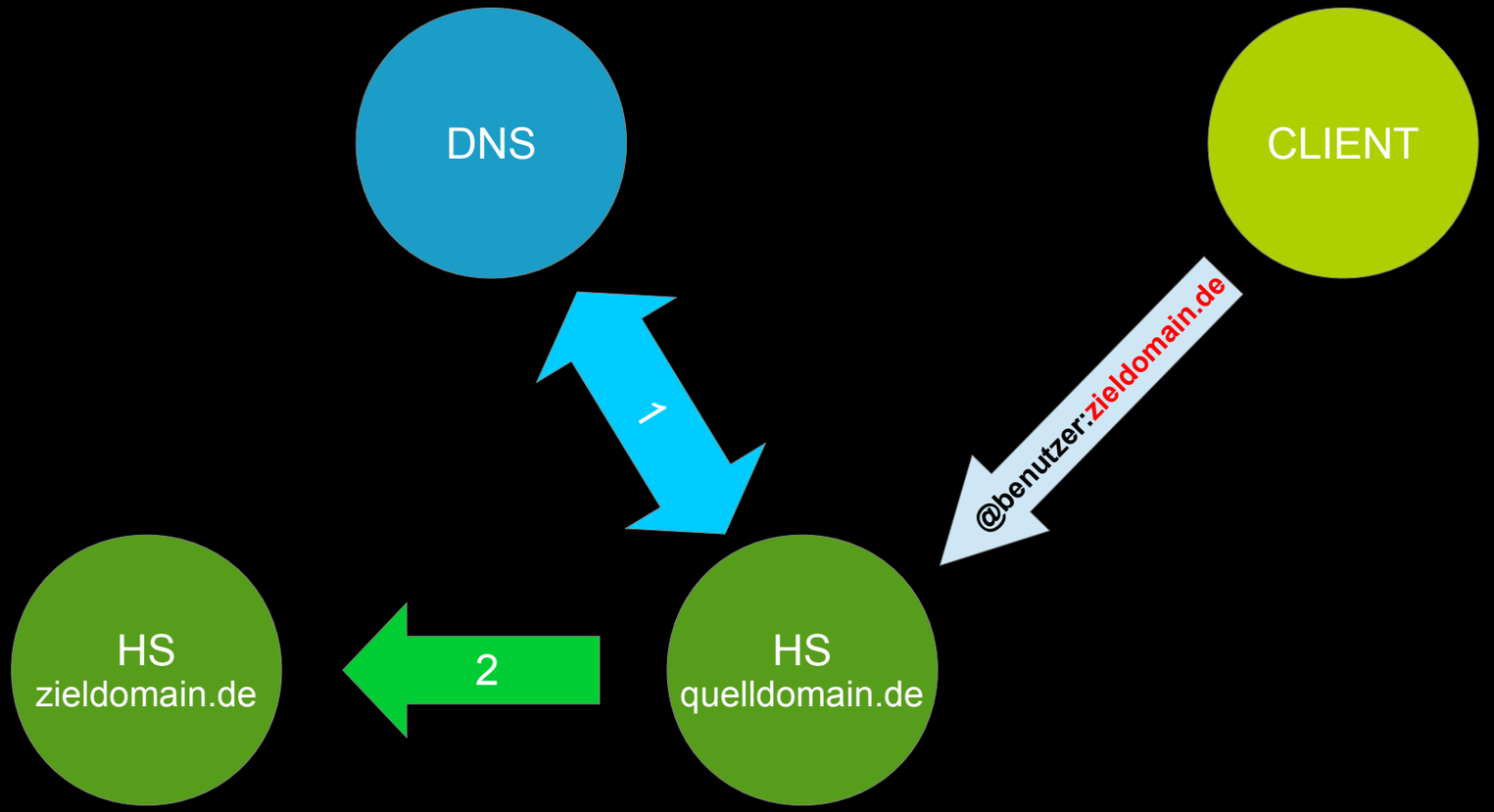
Aus der Kennung wird die Domain extrahiert, der DNS befragt und der Ziel-HS kontaktiert.

„Thema: Eine Einführung in Matrix“
Nachrichtenaustausch



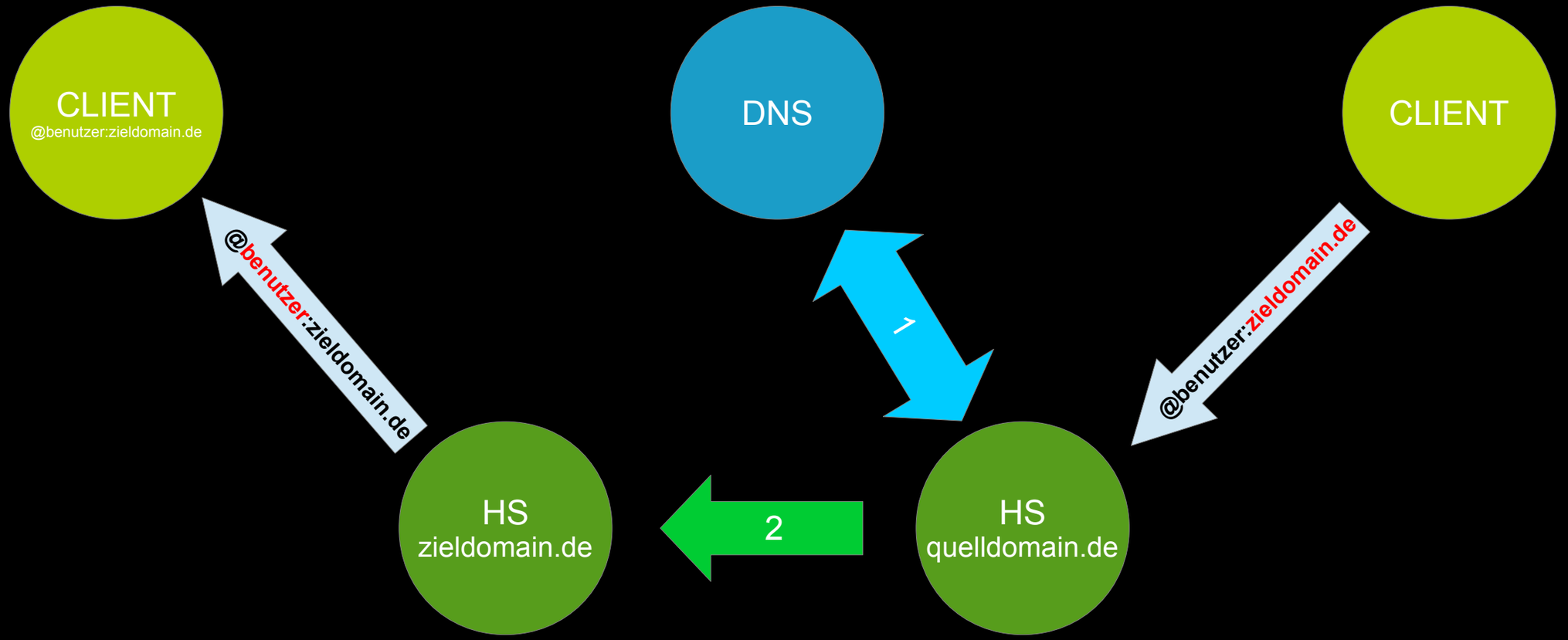
Aus der Kennung wird die Domain extrahiert, der DNS befragt und der Ziel-HS kontaktiert.

„Thema: Eine Einführung in Matrix“
Nachrichtenaustausch



Aus der Kennung wird die Domain extrahiert, der DNS befragt und der Ziel-HS kontaktiert.

„Thema: Eine Einführung in Matrix“
Nachrichtenaustausch



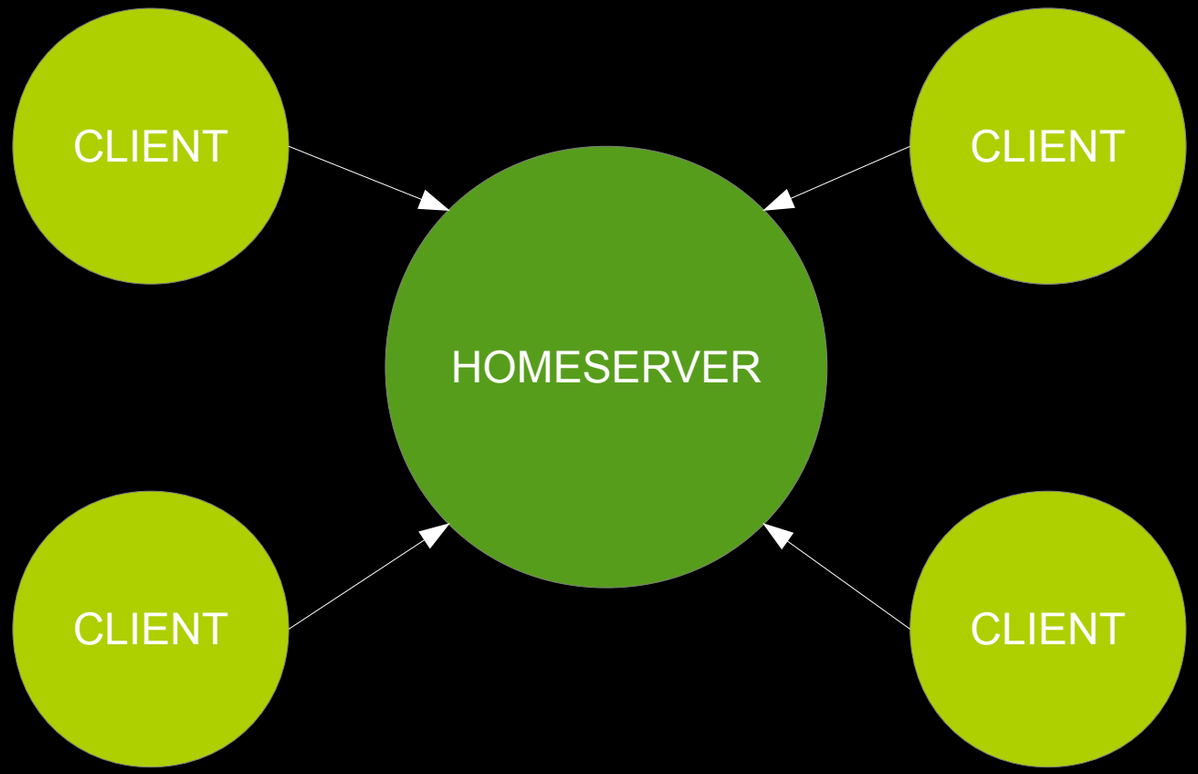
Aus der Kennung wird die Domain extrahiert, der DNS befragt und der Ziel-HS kontaktiert.

„Thema: Eine Einführung in Matrix“

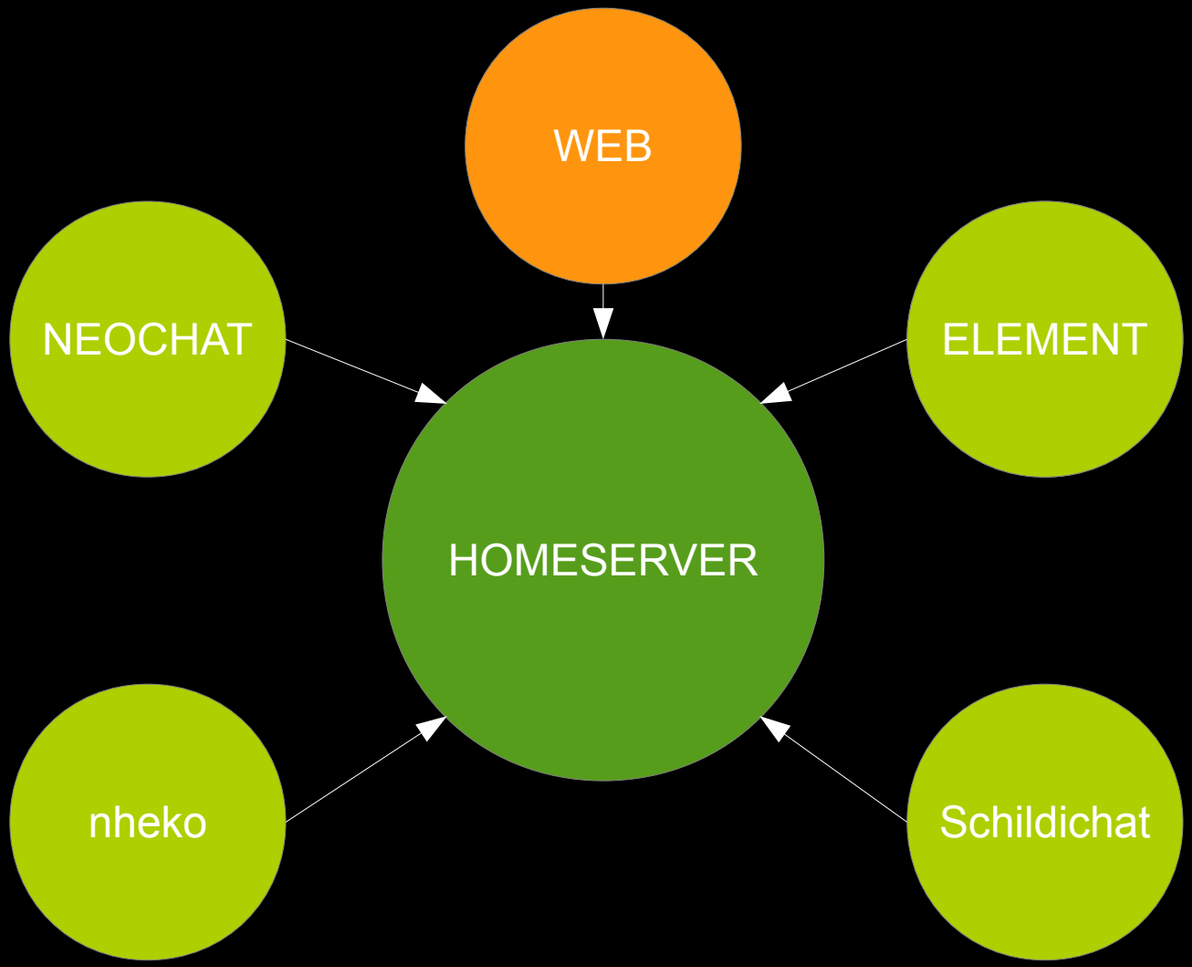
An den Homeservern sind die verschiedenen Benutzer

mit Ihren Clienten angehängt.

„Thema: Eine Einführung in Matrix“



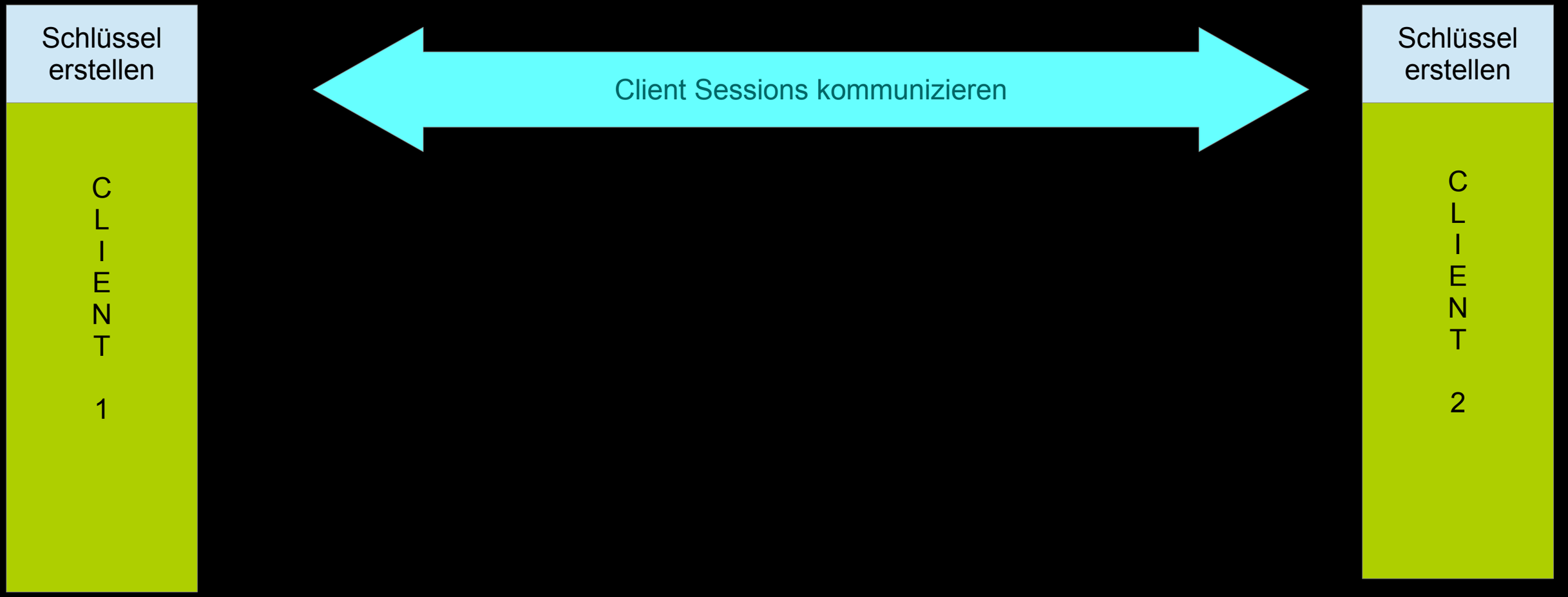
„Thema: Eine Einführung in Matrix“



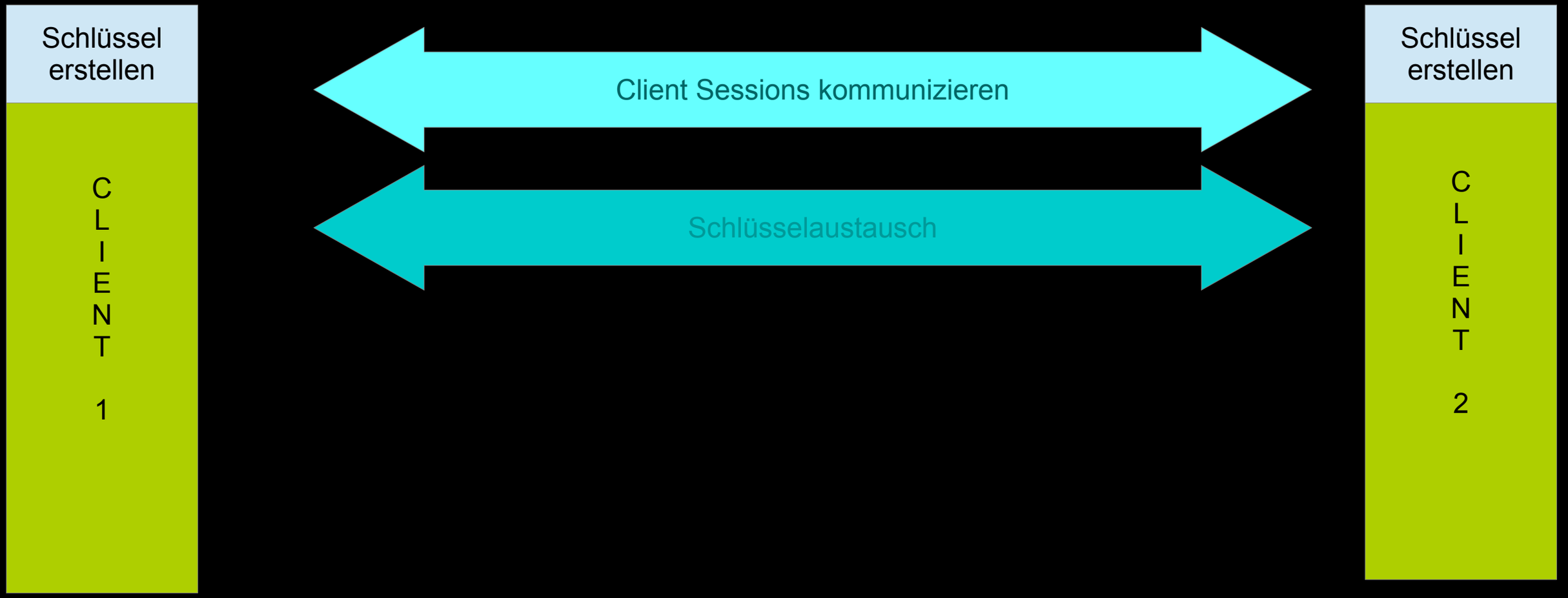
„Thema: Eine Einführung in Matrix“

Ende-Zu-Ende-VERSCHLÜSSELUNG

„Thema: Eine Einführung in Matrix“



„Thema: Eine Einführung in Matrix“



„Thema: Eine Einführung in Matrix“

„Thema: Eine Einführung in Matrix“

„Thema: Eine Einführung in Matrix“

Auf den beteiligten Homeservern werden

die Nachrichteninhalte verschlüsselt gespeichert.

„Thema: Eine Einführung in Matrix“

Dateien werden verschlüsselt auf dem sendenden Homeservern abgelegt

und an Andere als Link verteilt.

„Thema: Eine Einführung in Matrix“

Dateien werden verschlüsselt auf dem sendenden Homeservern abgelegt

und an Andere als Link verteilt.

Dies führt leider auf Dauer zu einem Hohen Platzverbrauch auf dem Homeserver.

„Thema: Eine Einführung in Matrix“

ABER:

Die META-Daten sind weiterhin verfügbar,

also wann, wer, wem etwas geschickt hat.

„Thema: Eine Einführung in Matrix“

Es kann also nicht abgestritten werden,

das jemand kommuniziert hat.

„Thema: Eine Einführung in Matrix“

Diese Daten können beim Homeserverbetreiber

illegal von Kriminellen

oder

legal von der Polizei

erbeutet bzw. beschlagnahmt werden.

„Thema: Eine Einführung in Matrix“

Abschottung

„Thema: Eine Einführung in Matrix“

Obwohl Matrix an sich ein föderiertes System ist,

kann es auch abgeschlossen eingesetzt werden.

z.B. Firmenintern ohne Außenkontakte

„Thema: Eine Einführung in Matrix“

In einem geschlossenen System

wird natürlich die Einbindung

zu per Mobilfunk betriebenen Endgeräten schwieriger.

„Thema: Eine Einführung in Matrix“

Datenschutz

„Thema: Eine Einführung in Matrix“

Die Einstellungen in den besseren Klienten

lassen unabsichtliche Datenlöcher gar nicht erst entstehen,

da z.B. **Verschlüsselung** und **Authentizität** **eingefordert** werden können.

„Thema: Eine Einführung in Matrix“

Verschlüsselung erlaubt:

WebRTC Audio- und Video-Chats

„Thema: Eine Einführung in Matrix“

E2E-Verschlüsselung meint auch E2E-Verbindung.

„Thema: Eine Einführung in Matrix“

E2E-Verschlüsselung meint auch E2E-Verbindung.

Audio/Videochats laufen direkt von PC1 zu PC2,

ohne einen Server dazwischen.

„Thema: Eine Einführung in Matrix“

TURN-Server

Traversal **U**sing **R**elays around **N**AT (**TURN**):

hierbei handelt es sich um einen Tunnel/Relay-Server,

der den beteiligten Klienten einen Kanal zum Aushandeln

der Verbindung bereitstellt oder notfalls als Tunnel/Relay-Dienst fungiert.

„Thema: Eine Einführung in Matrix“

Einsatz von TURN-Server

[1]TURN [RFC5766] ist ein Protokoll, das häufig verwendet wird, um die Konnektivität von P2P-Anwendungen zu verbessern. Durch die Bereitstellung eines cloudbasierten Relay-Dienstes stellt TURN sicher, dass eine Verbindung auch dann hergestellt werden kann, wenn eine oder beide Seiten nicht in der Lage sind, eine direkte P2P-Verbindung herzustellen. Als Relay-Dienst ist er jedoch mit nicht-trivialen Kosten für den Datentransfer beim Hoster verbunden.[a]

„Thema: Eine Einführung in Matrix“

NAT/Firewall umgehen durch Einsatz von UDP

„Thema: Eine Einführung in Matrix“

Bei einer UDP basierten Datenübertragung,

wie sie bei WebRTC zum Einsatz kommt,

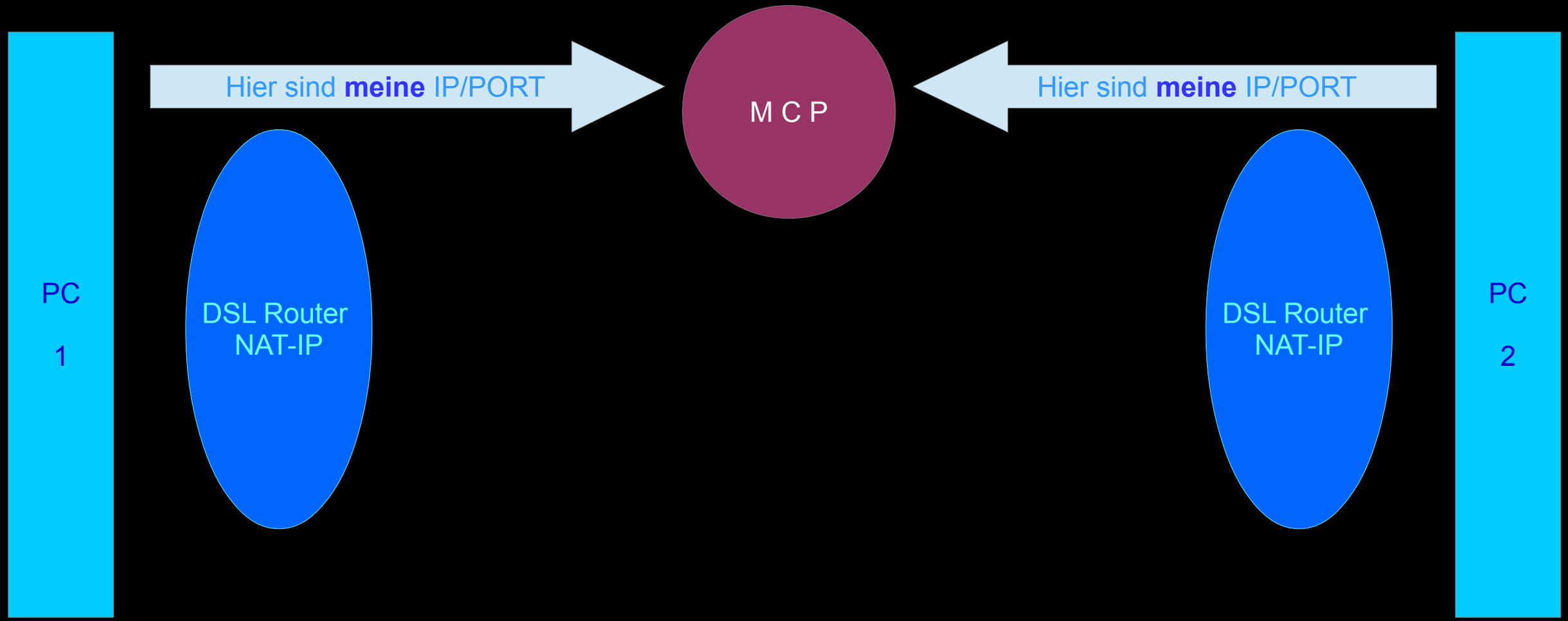
können die beteiligten Klienten die Firewall austricksen,

in dem Ihnen über einen Dritten (hier die HS)

die IP und der Port des jeweils anderen Klienten mitgeteilt wird.

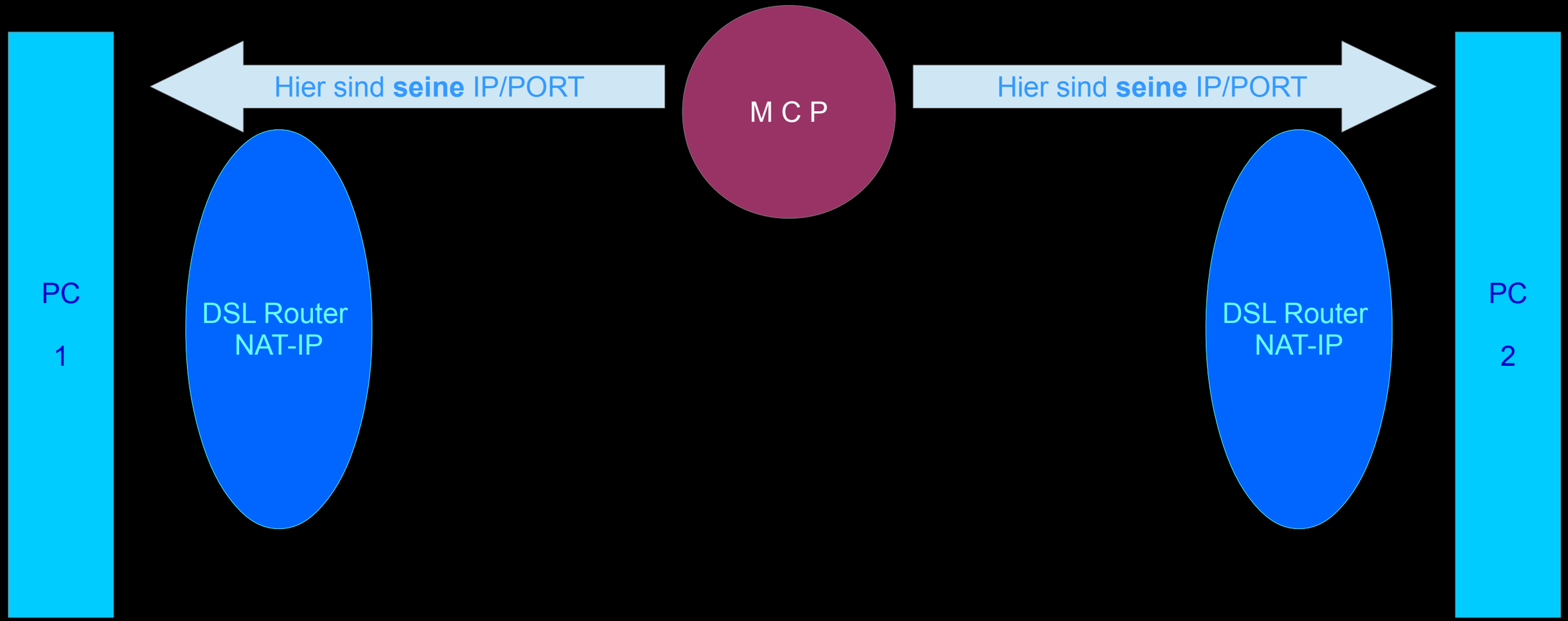
„Thema: Eine Einführung in Matrix“

PEER-2-PEER



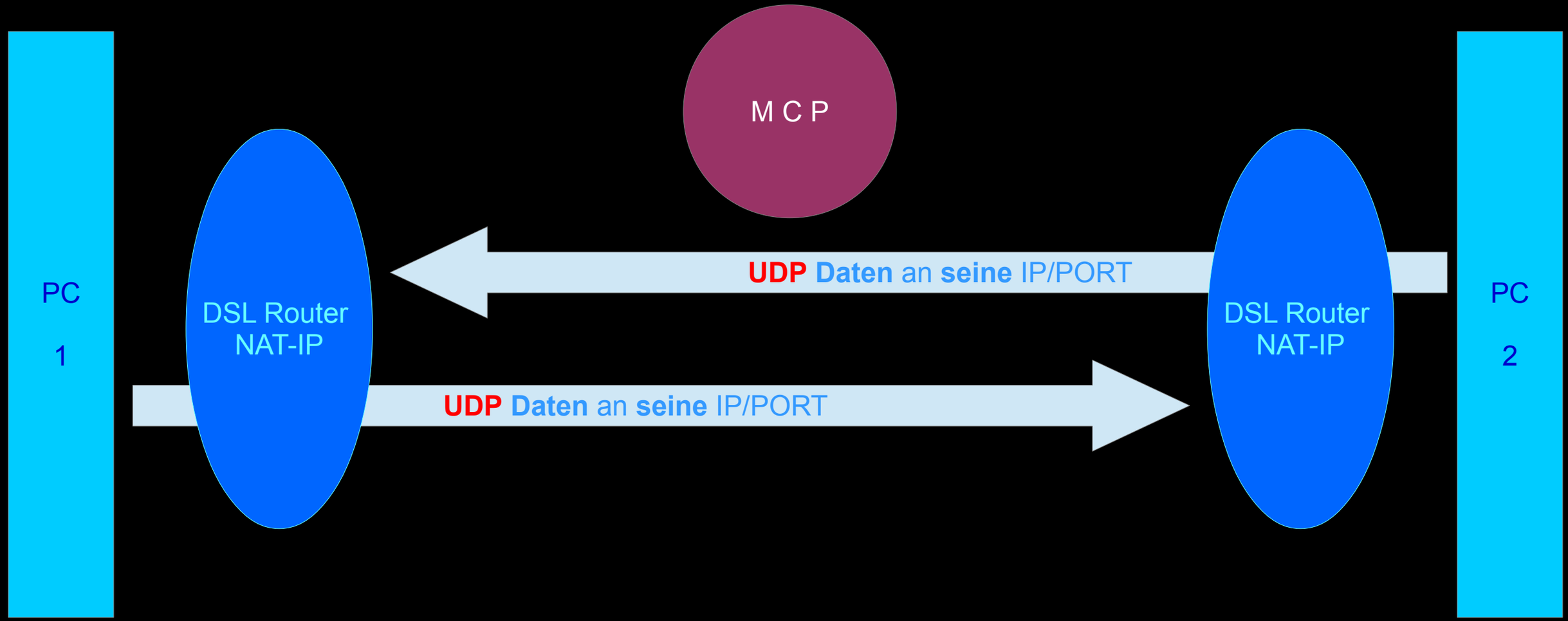
„Thema: Eine Einführung in Matrix“

PEER-2-PEER



„Thema: Eine Einführung in Matrix“

PEER-2-PEER



„Thema: Eine Einführung in Matrix“
Verbindung finden mit Hilfe des TURN-Servers

UDP & Firewalls

Da ein UPD Datenpaket keine Sequenznummern und SYN/FIN Pakete wie TCP hat,

muß eine Firewall eine Zeitlang einen offenen Rückkanal für die Antwortpakete

eines UDP Services schaffen.

„Thema: Eine Einführung in Matrix“
Verbindung finden mit Hilfe des TURN-Servers

Meint:

„Schicke ICH ein UDP Paket an IP:PORT durch die Firewall durch,

muß eine Antwort zu MIR von IP:PORT für eine gewisse Zeit erlaubt werden.“

„Thema: Eine Einführung in Matrix“

PEER-2-PEER

Dieser Kanal durch die Firewall wird von den beteiligten Programmen genutzt.

Solange Daten fließen, bleibt der Kanal auf.

„Thema: Eine Einführung in Matrix“
Verbindung finden mit Hilfe des TURN-Servers

Wenn das **nicht** geht,

kommt der TURN Server als TUNNEL/RELAY zum Einsatz.

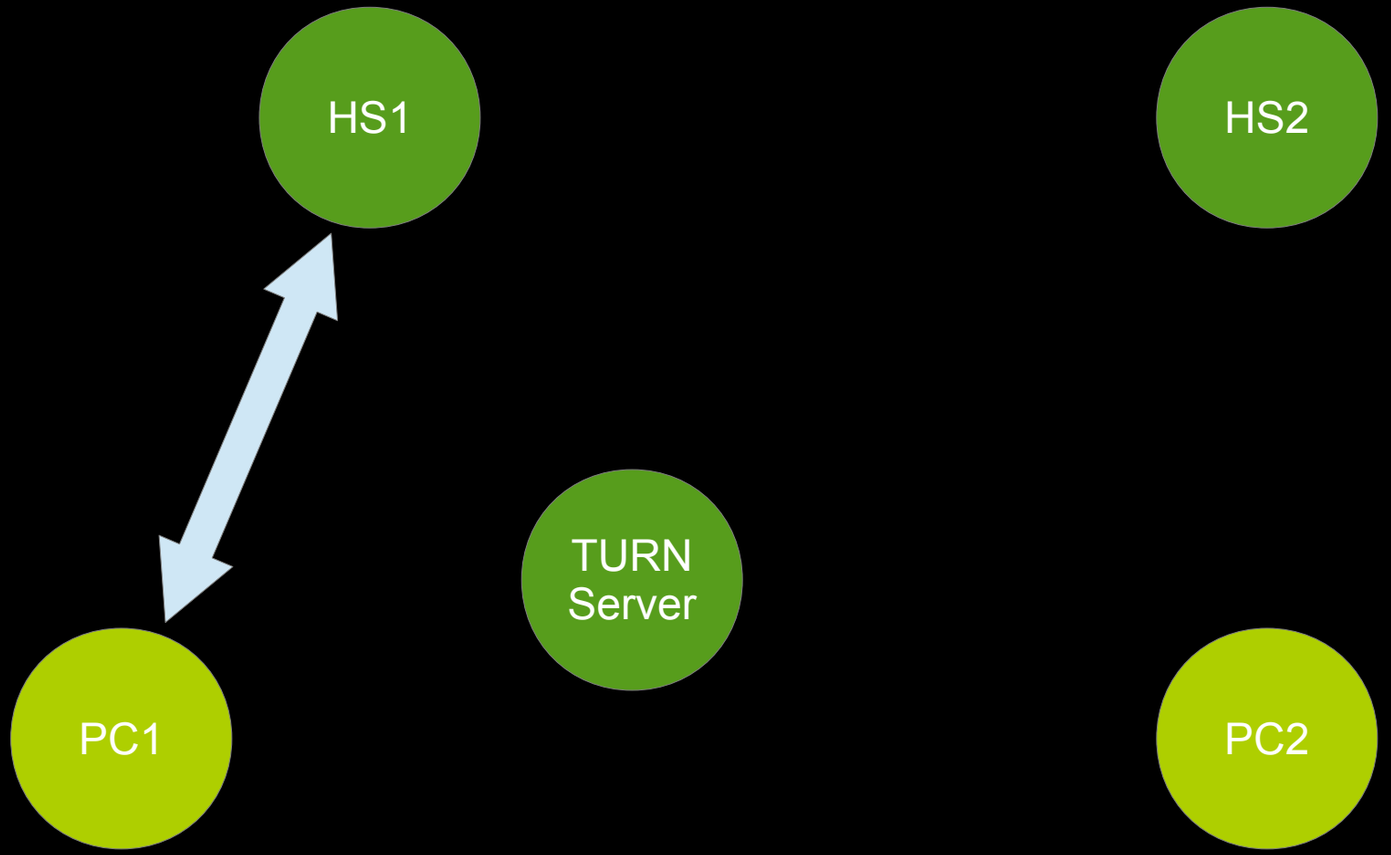
„Thema: Eine Einführung in Matrix“
Verbindung finden mit Hilfe des TURN-Servers

Hinweis:

Die folgende Darstellung kann in der Reihenfolge in der Realität abweichen.

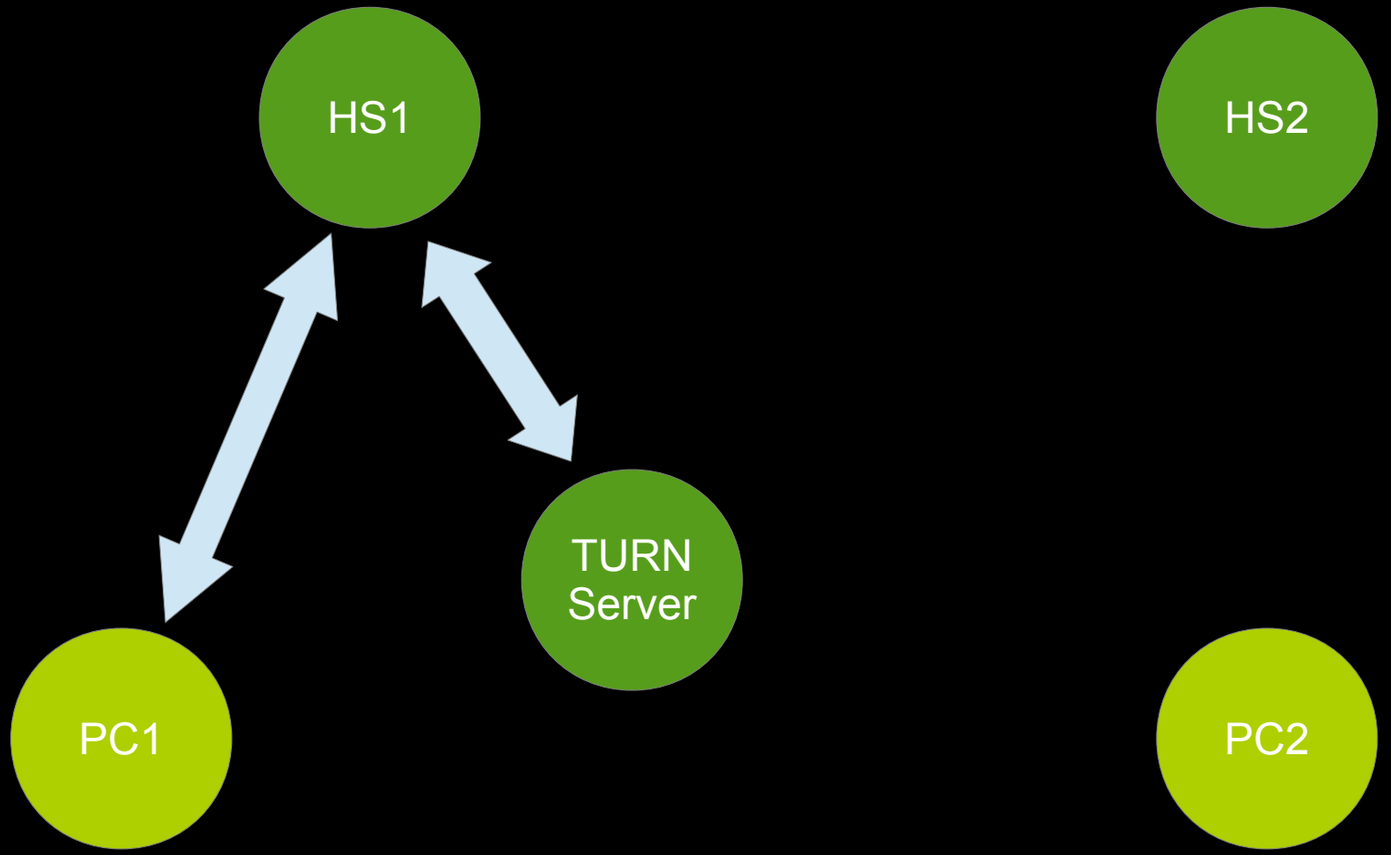
Auch ist es nur dann nötig,
wenn sich min. ein Klient hinter einer Firewall oder einem DSL-Router befindet.

„Thema: Eine Einführung in Matrix“
Verbindung finden mit Hilfe des TURN-Servers



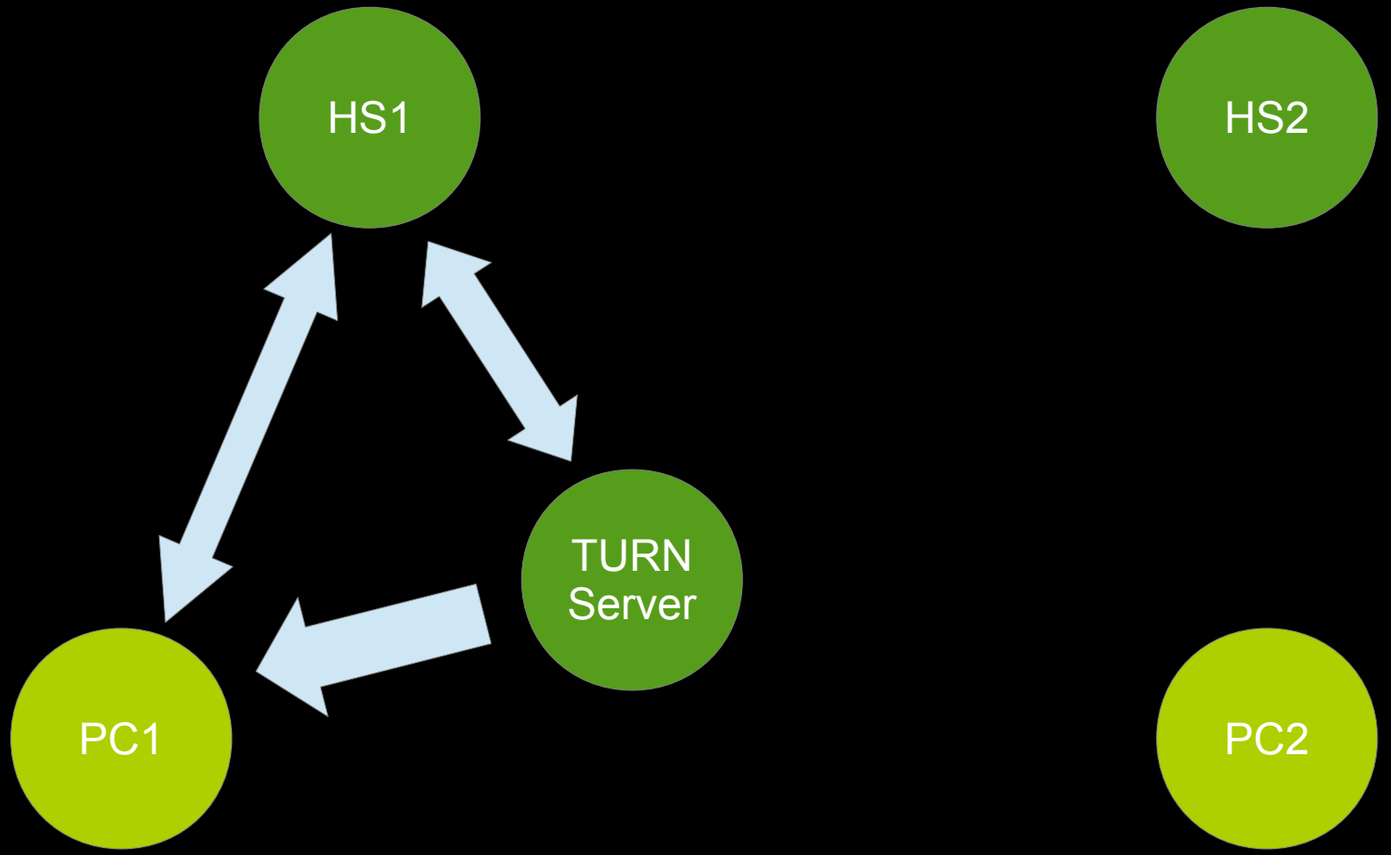
Klient informiert HS über Anrufversuch

„Thema: Eine Einführung in Matrix“
Verbindung finden mit Hilfe des TURN-Servers



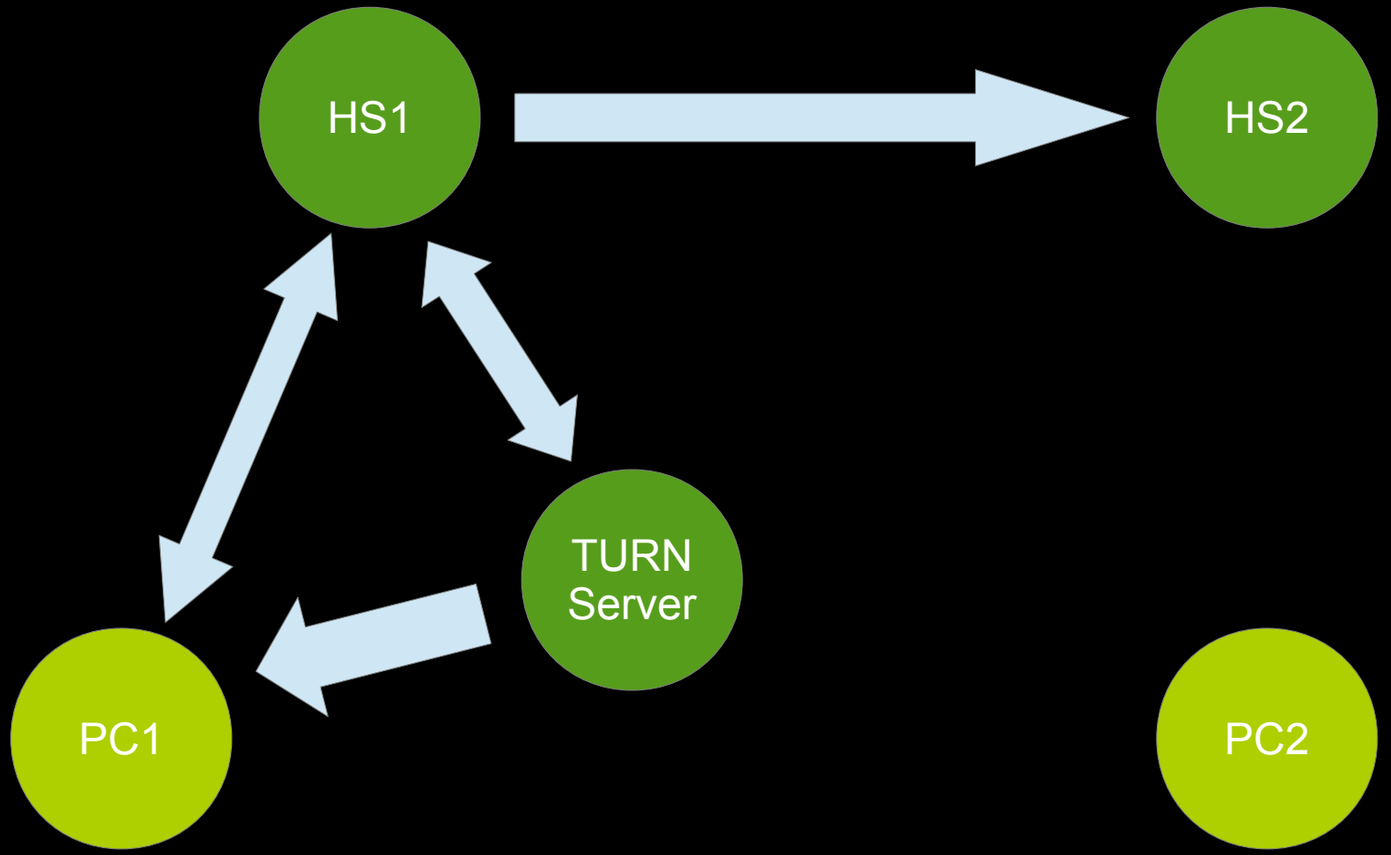
HS initialisiert den TURN-Server

„Thema: Eine Einführung in Matrix“
Verbindung finden mit Hilfe des TURN-Servers



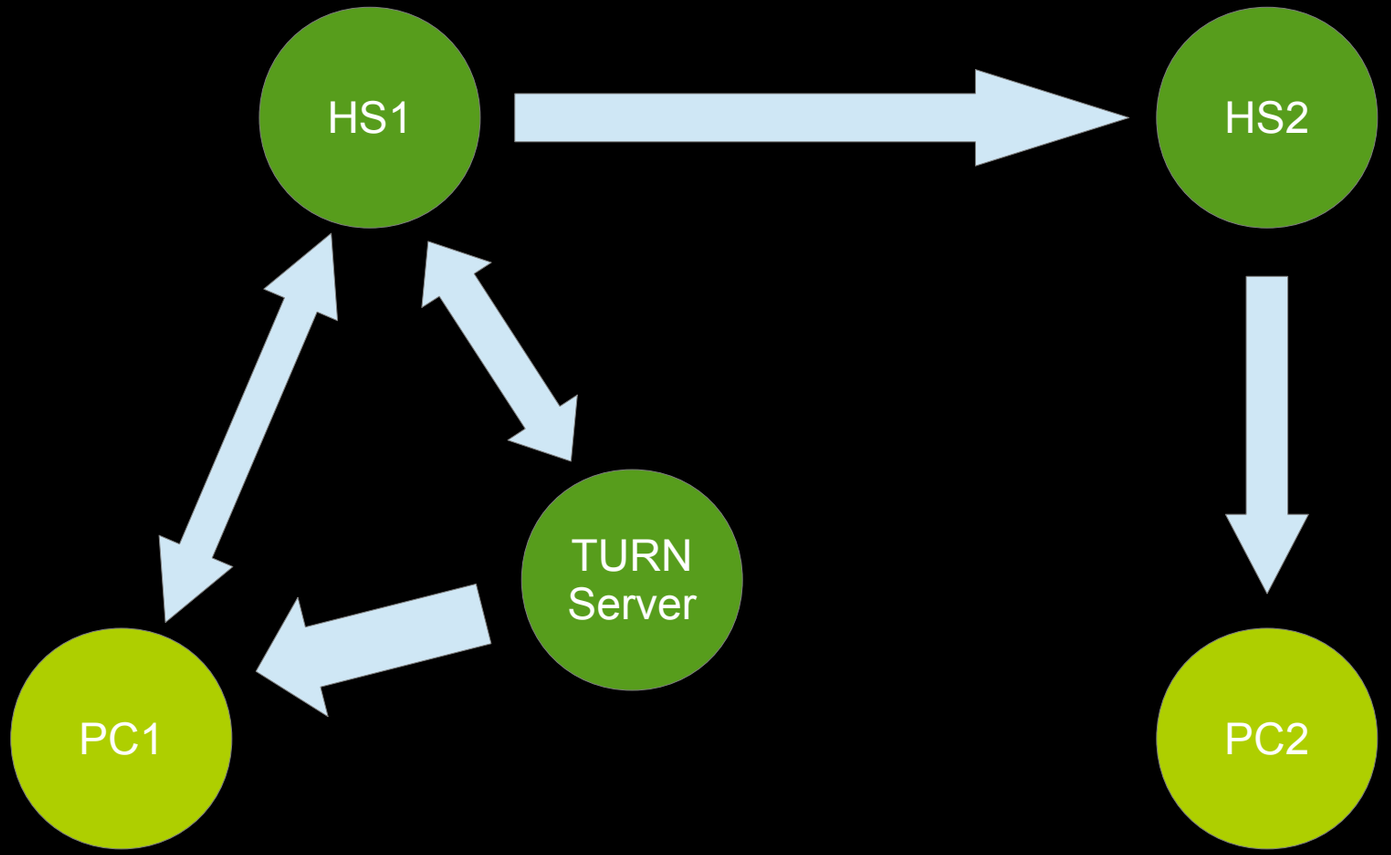
Klient und TURN-Server teilen erste
Details zu Port und IP

„Thema: Eine Einführung in Matrix“
Verbindung finden mit Hilfe des TURN-Servers



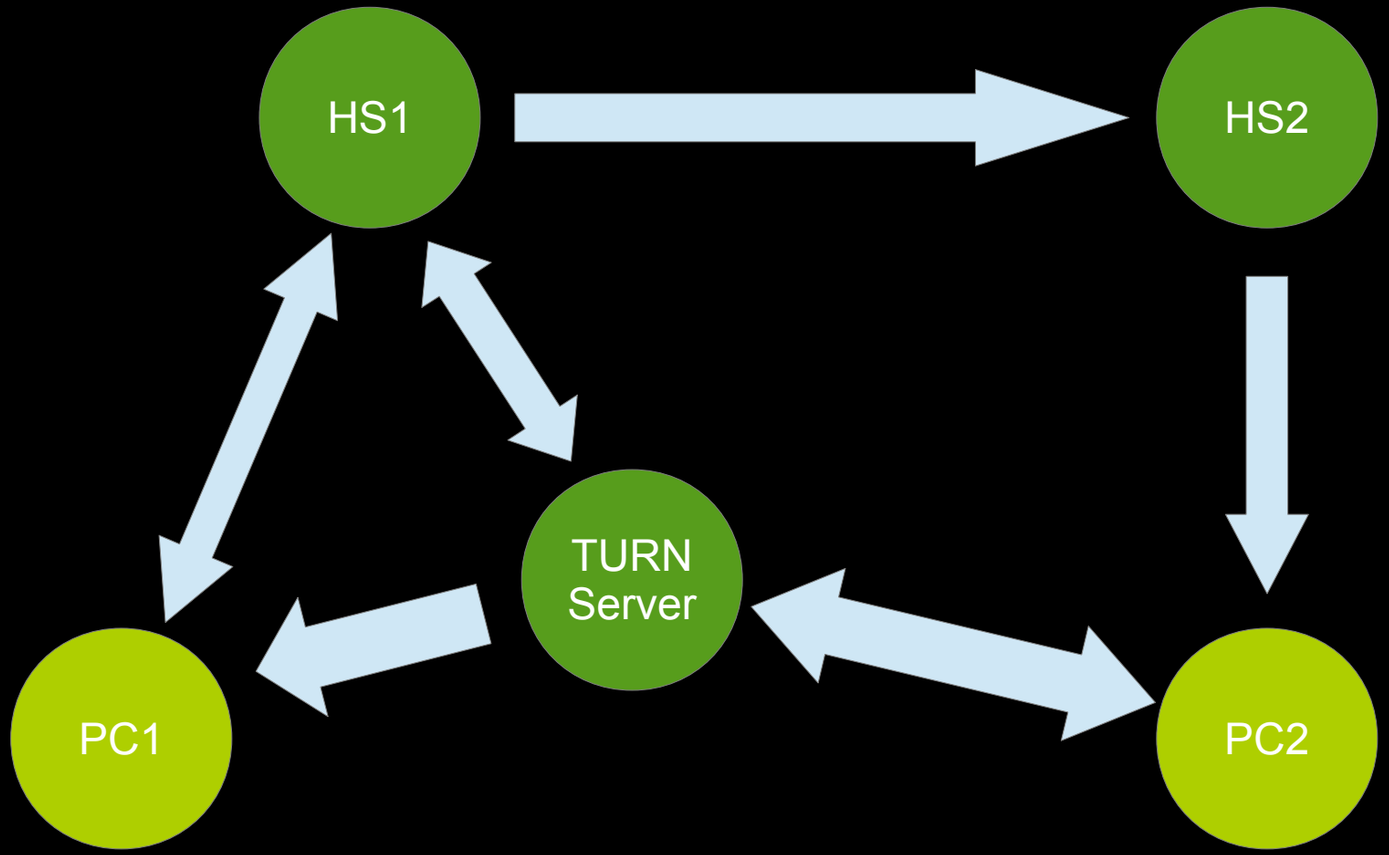
HS des Anrufers informiert HS des Angerufenen
über die Zugangsdaten zum TURN-Server

„Thema: Eine Einführung in Matrix“
Verbindung finden mit Hilfe des TURN-Servers



HS informiert den Klienten des
Angerufenen über TURN-Serverdaten

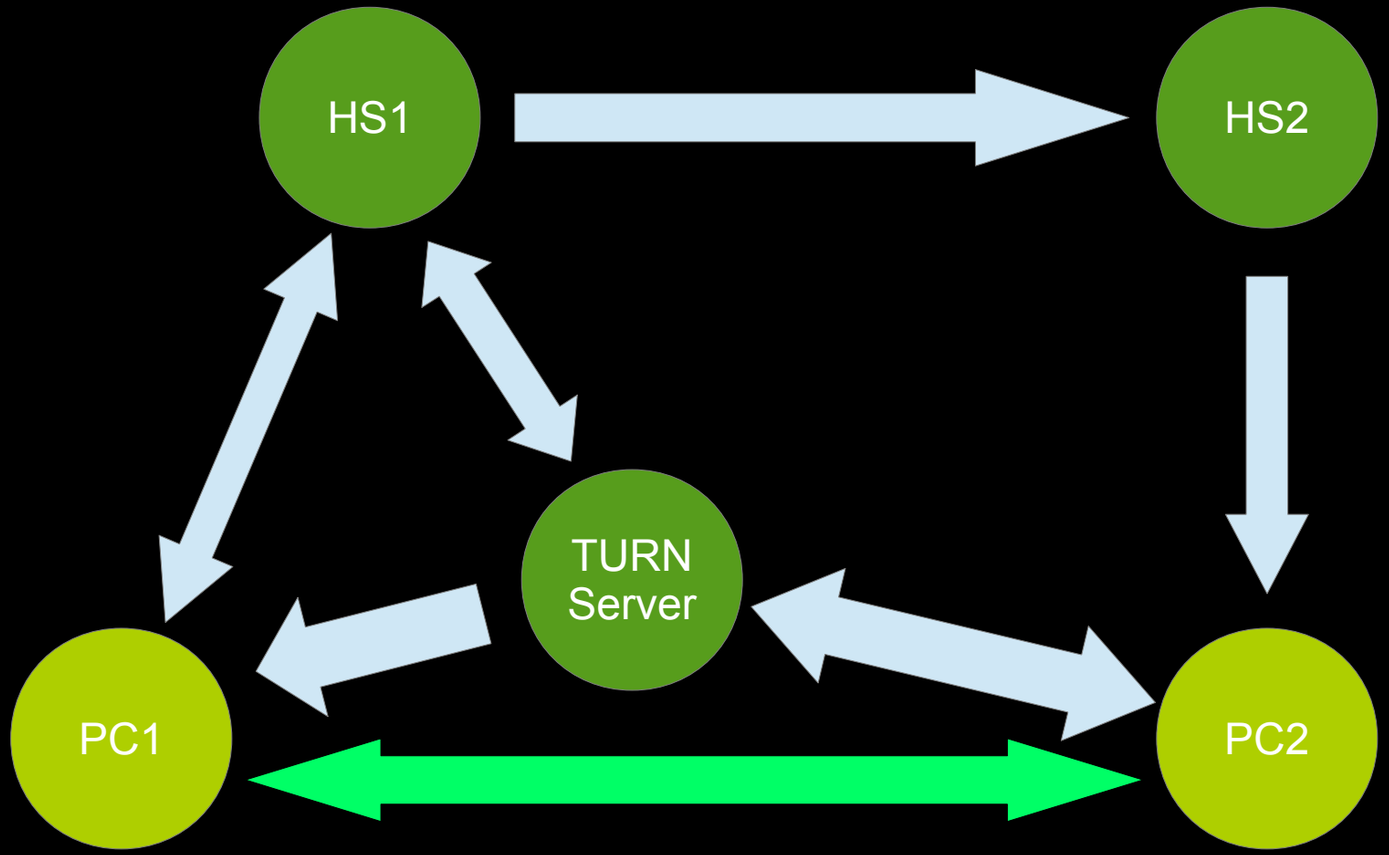
„Thema: Eine Einführung in Matrix“
Verbindung finden mit Hilfe des TURN-Servers



Der angerufene Klienten kontaktiert den TURN-Server und handelt die Verbindung aus.

„Thema: Eine Einführung in Matrix“

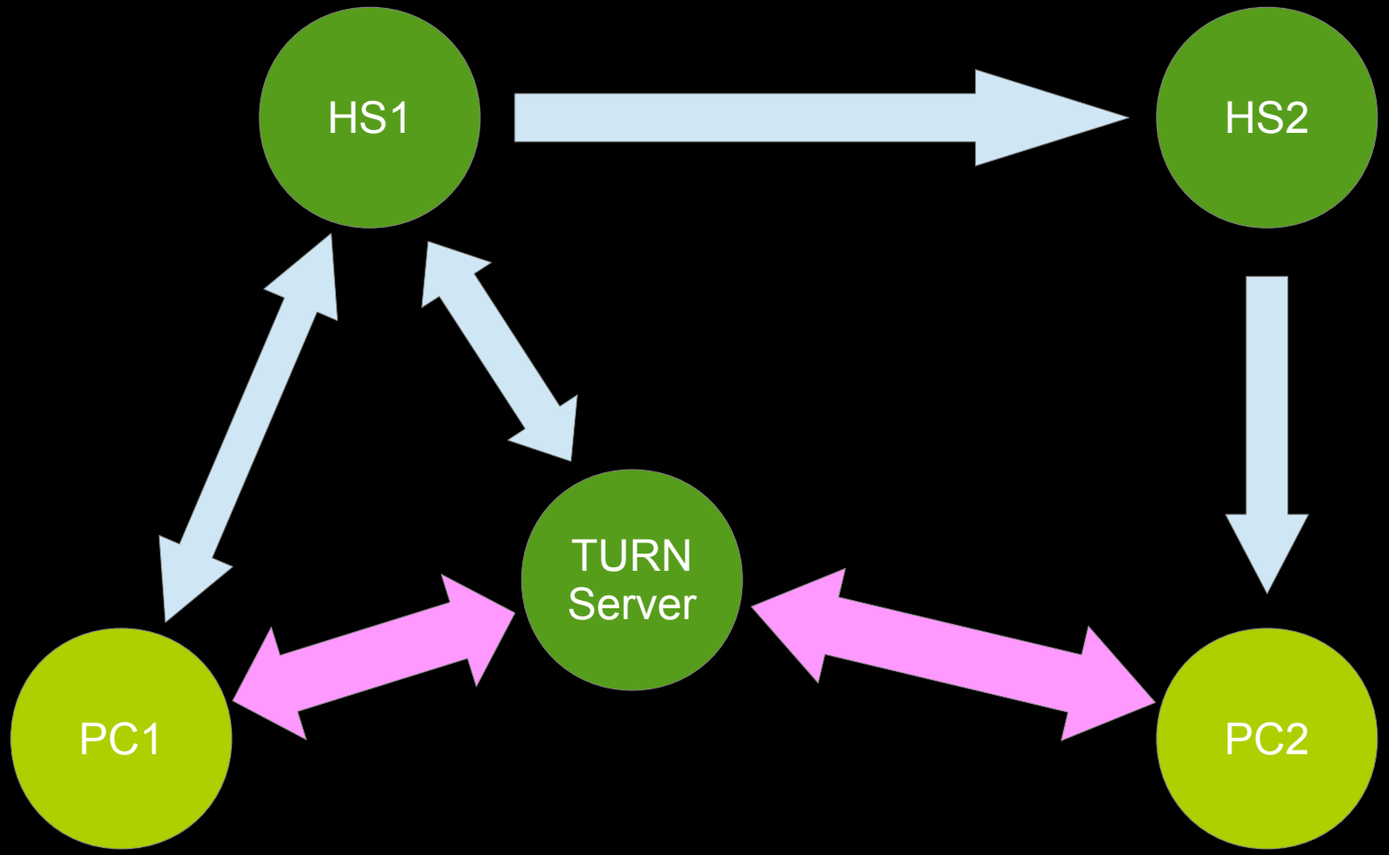
Verbindung finden mit Hilfe des TURN-Servers



Nach Möglichkeit wird direkt
kommuniziert …

„Thema: Eine Einführung in Matrix“

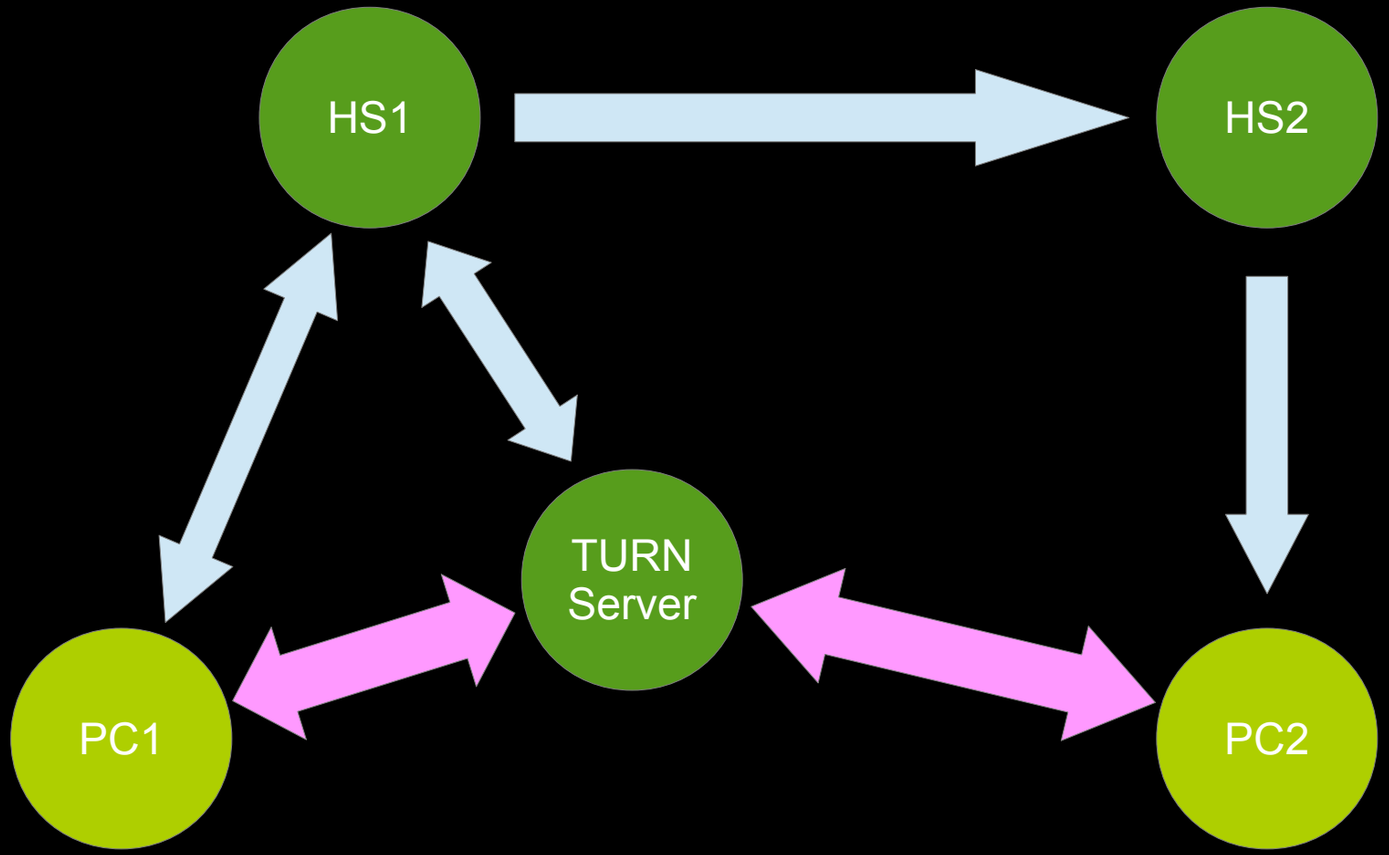
Verbindung finden mit Hilfe des TURN-Servers



… oder indirekt über den TURN-Server

„Thema: Eine Einführung in Matrix“

Verbindung finden mit Hilfe des TURN-Servers



… oder indirekt über den TURN-Server

„Thema: Eine Einführung in Matrix“

Bis auf Gruppen-Audio/Video-Chats,

kann mit einem vollständigen Klienten wie Element oder Schildichat

direkt und vollständig alle gängigen Mediendateien ausgetauscht und

direkt mit dem Gesprächspartner kommuniziert werden.

„Thema: Eine Einführung in Matrix“

Gruppen-Audio/Video-Chats können mithilfe von Widgets wie

Meet Jitsi oder Big Blue Button

spontan abgehalten werden.

„Thema: Eine Einführung in Matrix“

Einzig das Teilen von Bildschirminhalten

ist noch einer Videokonferenzlösung vorbehalten.

„Thema: Eine Einführung in Matrix“

Gruppenräume

„Thema: Eine Einführung in Matrix“

Matrixclienten können auch in Gruppenräumen

die Verschlüsselung und Authentizität garantieren.

„Thema: Eine Einführung in Matrix“

Wenn es um Gruppenchats geht,

kann Matrix mit wahrlich großen Zahlen aufwarten:

45.000+ Leute in einem Raum

„Thema: Eine Einführung in Matrix“

Der Nachteil eine solchen übervölkerten Raumes sind Unmengen an unnützen Daten die zwischen Homeservern ausgetauscht werden müssen.

„Thema: Eine Einführung in Matrix“

Beispiele:

Person A geht aus dem Raum
Person Z betritt den Raum
Server X antwortet nicht

usw.

„Thema: Eine Einführung in Matrix“

Dies führt auf einem Handy i.d.R. zu einem schnellen Entladen des Akkus.

„Thema: Eine Einführung in Matrix“

Angriffsszenarien

„Thema: Eine Einführung in Matrix“

Da es sich bei allen auf „Element“ basierenden Clienten

um Webanwendungen handelt,

besteht die latente Gefahr,

daß ein CSS oder CSRF durch eine Nachricht eingeschleust wird.

CSS = Cross-Site-Scripting CSRF = Cross-Site-Request-Forgery

„Thema: Eine Einführung in Matrix“

Alle Multimediadateien die mit anderen geteilt werden

und sofort zur Ansicht kommen,

können für RCE und/oder DOS Angriffe genutzt werden.

RCE = Remote-Code-Execution DOS = Denial-of-Service (Buffer Overflow in Bildbibliotheken)

„Thema: Eine Einführung in Matrix“

Da jeder seinen eigenen Homeserver betreiben kann,

kann dieser so manipuliert werden,

nicht-protokollgemäße Datenpakete zu erzeugen.

„Thema: Eine Einführung in Matrix“

Wie bei allen Anwendungen,

halten regelmäßige Updates ein System sicherer.

Deswegen ist es wichtig einen gepflegten Matrixklienten einzusetzen.

„Thema: Eine Einführung in Matrix“

Fazit

„Thema: Eine Einführung in Matrix“

Nachteile:

kein Screensharing
ggf. Hoher Energiebedarf
Nicht-Abstreibarkeit* der Kommunikation

*) ist generell ein Problem bei nicht geschlossenen Systemen

„Thema: Eine Einführung in Matrix“

Vorteile:

Authentizität
Gruppenchats
Klientenvielfalt
E2E-Audiochats
E2E-Videochats
Multimediainhalte
E2E-Verschlüsselung
dezentrale Serverarchitektur
Freie Wahl des Betriebssystems
Unabhängigkeit von Zentralen Einrichtung/Firma
verschlüsselte Datenhaltung auf dem Homeserver

„Thema: Eine Einführung in Matrix“

Mehr Informationen auf **Matrix.org**

„Thema: Eine Einführung in Matrix“

Danke für Ihre Aufmerksamkeit