DOAG

SIG - Security Day

19.05.2015 - München

CMAN Reloaded

DER ORACLE CONNECTION MANAGER (CMAN) ALS FIREWALL FÜR DAS ROUTING VON DATENBANK VERBINDUNGEN

Gunther Pippèrr - IT-Architekt - Berater

Background

Gunther Pippèrr arbeitet seit mehr als 17 Jahre intensiv mit den Produkten der Firma Oracle im Bereich Datenbanken/Applikationsserver und Dokumenten-Management.

Herr Pippèrr hat sich tiefes Wissen über den Aufbau komplexer IT Architektur aneignen können und hat dieses in der Praxis erfolgreich umgesetzt.

Herr Pippèrr hat eine Abschluss als Dipl. Ing. Technische Informatik (FH) an der FH Weingarten.

Functional Expertise

- IT System Architekt
- Technische Projektleitung
- Design und Implementierung von Datenbank Anwendungen
- Entwurf und Umsetzung von IT Infrastrukturen zum Datenmanagement

Industry Expertise

- High-Tech
- Real Estate
- Utility
- Communications

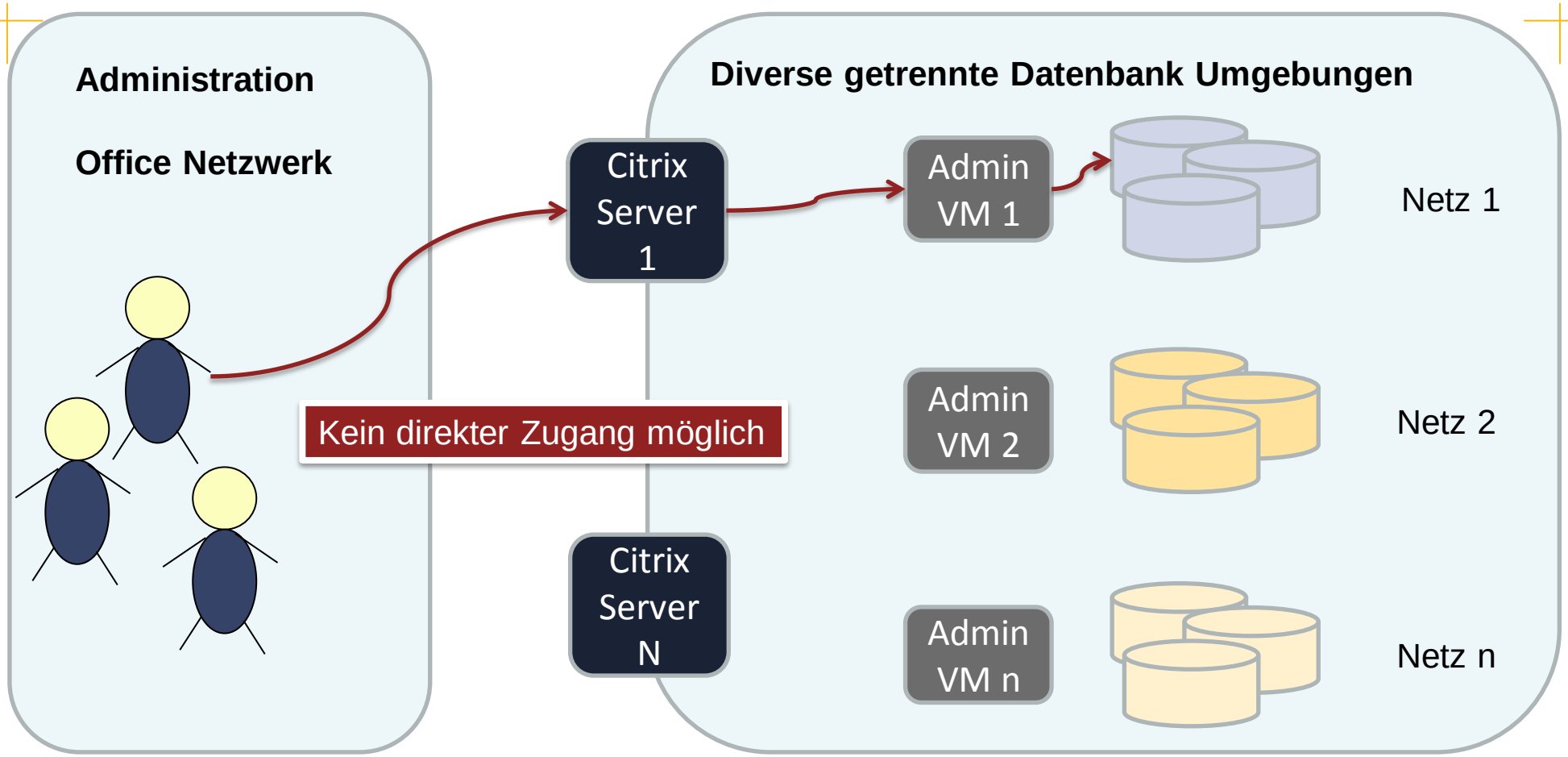
Selected Experience

- Datenbank Architekt für ein Projekt zur Massendatenverarbeitung in der Telekommunikation
- Architekt und technische Projektverantwortung für ein Smart Metering Portal für das Erfassen von Energiezählerdaten und Asset Management
- Architekt und technische Projektverantwortung für IT Infrastrukturprojekte, z.B.:
  - Unterstützung beim Betrieb der Datenbank Umgebung für das größte deutsche Kunden Bindungsprogramm
  - Zentrale Datenhaltung für Münchner Hotelgruppe mit über 25 Hotels weltweit,
  - Messdaten Erfassung für russischen Kabelnetzbetreiber
  - Redundante Cluster Datenbank Infrastrukturen für diverse größere Web Anwendungen wie Fondplattform und Versicherungsportale
- CRM- und Ausschreibungsportal für großen Münchner Bauträger
- Architekt und Projektleitung , Datenbank Design und Umsetzung für die Auftragsverwaltung mit Steuerung von externen Mitarbeitern für den Sprachdienstleister von deutschen Technologiekonzern

Agenda

1	**Aufgabenstellung**
2	Installation
3	Konfiguration
4	Verwendung
5	Härten – Access Rules – Verschlüsselung - SSL

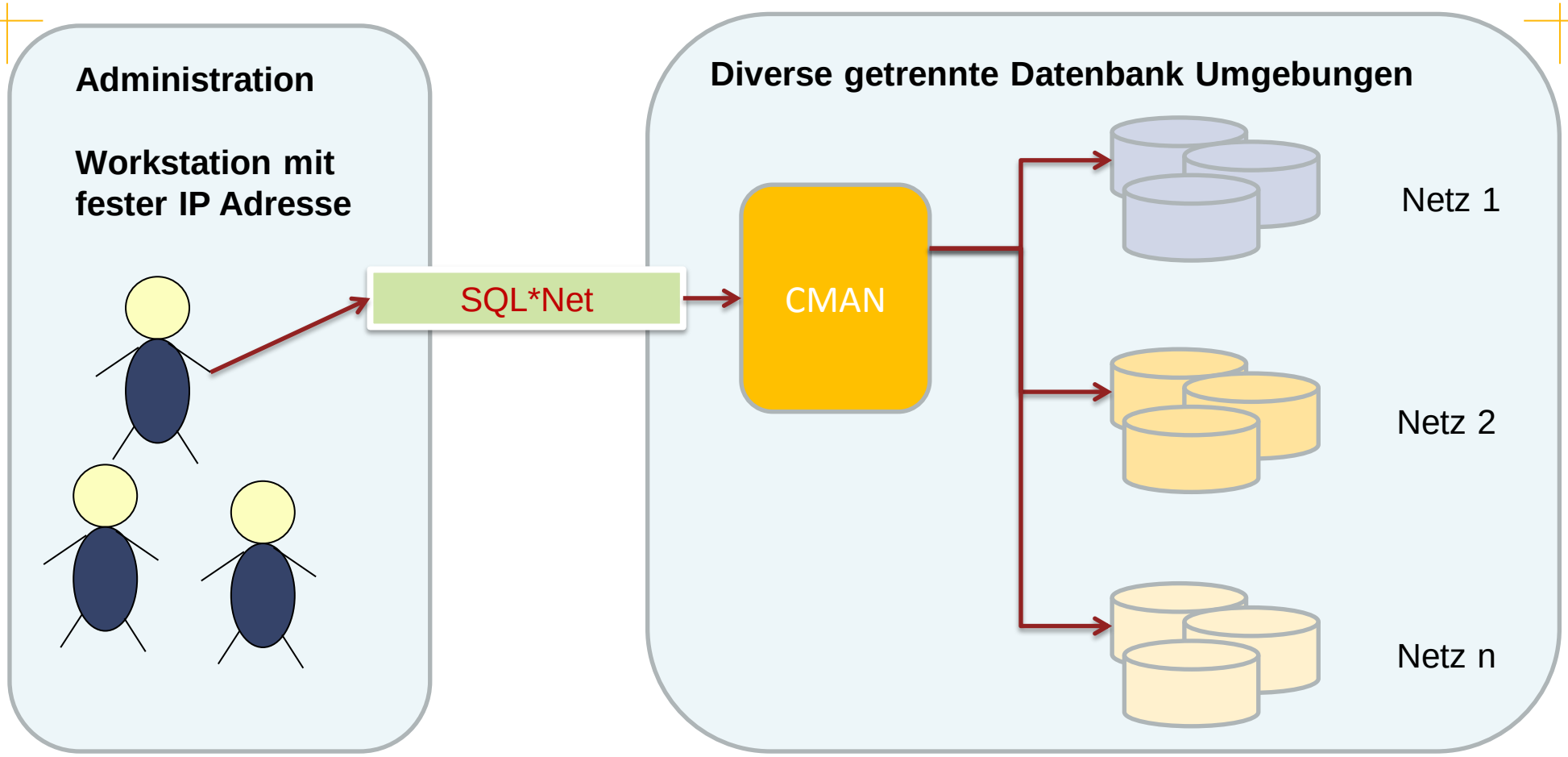
Die Aufgabenstellung - Ist



Sicherheit : Hoch
Bedienbarkeit und Akzeptanz : Gering
Zentrales Deployment : Nicht umsetzbar

Ein Lösungsansatz - CMAN

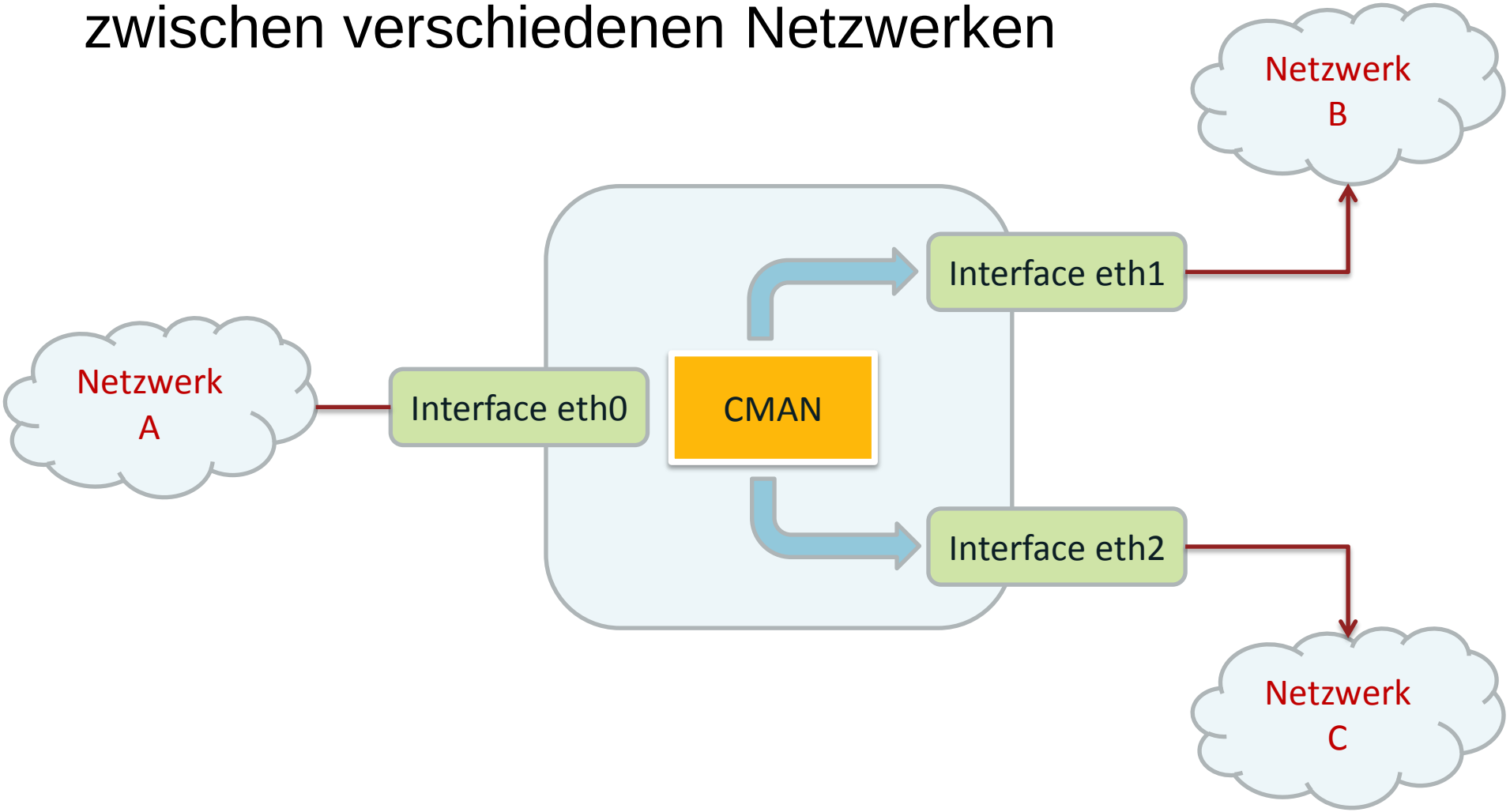
Symmetrische Verschlüsselung möglich
SSL leider nicht unterstützt!



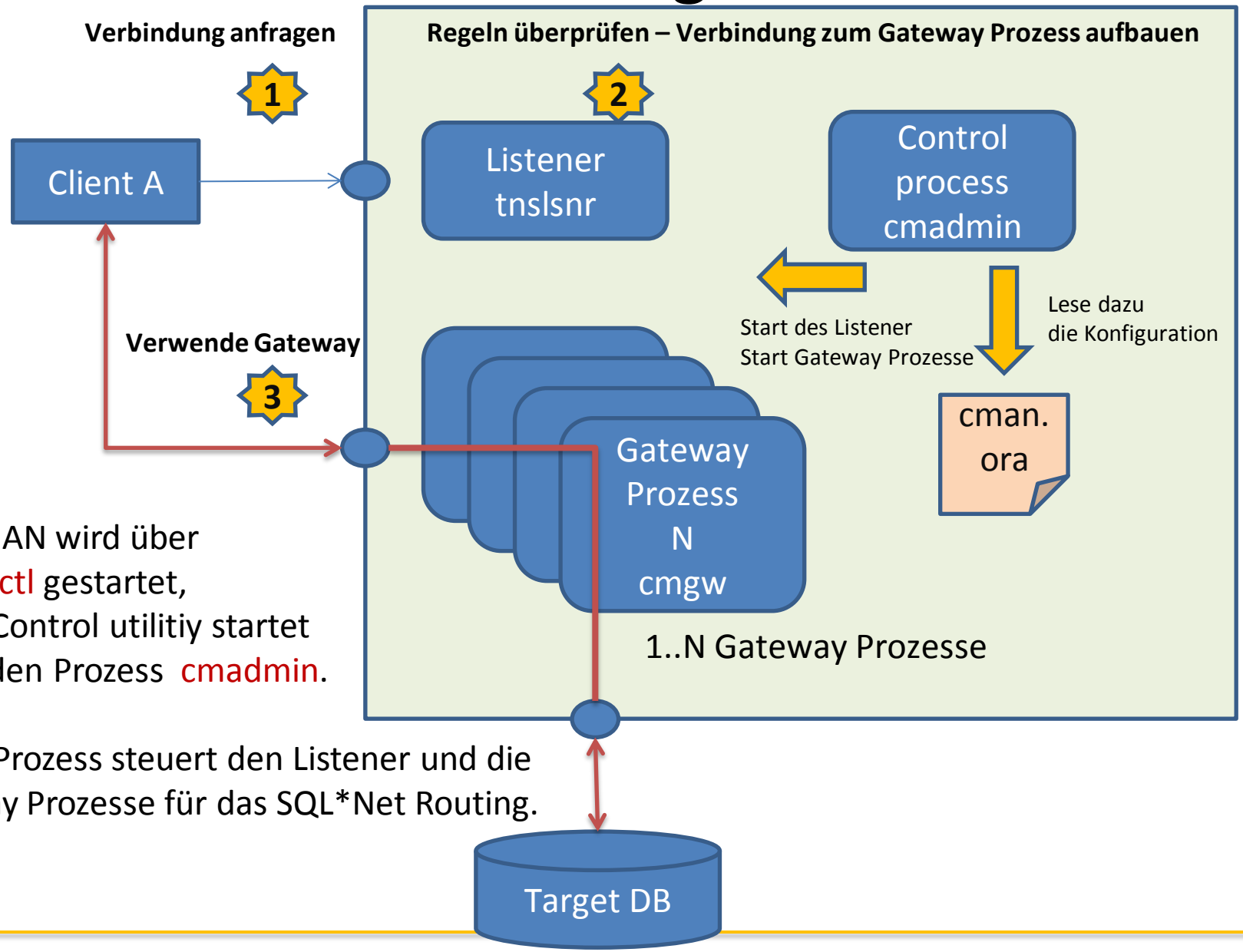
Sicherheit : Mittel
Bedienbarkeit und Akzeptanz : Hoch
Zentrales Deployment : Einfach umsetzbar

Funktionsübersicht Connection Manager

- „Routen“ des SQL*Net Protokolls über einen Rechner zwischen verschiedenen Netzwerken



Übersicht CMAN Verbindungsaufbau



Der CMAN wird über
den cmctl gestartet,
dieses Control utilitiy startet
zuerst den Prozess cmadmin.

Dieser Prozess steuert den Listener und die
Gateway Prozesse für das SQL*Net Routing.

Lizenz 11g – EE Edition Feature

- Oracle® Database Licensing Information 11g Release 2 (11.2) E47877-0
  - https://docs.oracle.com/cd/E11882_01/license.112/e47877.pdf

Table 1–1 (Cont.) Feature Availability for Oracle Database Editions

Feature/Option	SE1	SE	EE	Notes
Networking				
Oracle Connection Manager	N	N	Y	Available via a custom install of the Oracle Database client, usually installed on a separate machine See "Oracle Connection Manager" on page 1-8 for more information

Oracle Connection Manager

Oracle Connection Manager can be installed and used on a machine different from the machine where the Oracle Database is installed and used. It is not necessary to obtain a separate license for the machine running Oracle Connection Manager.

Lizenz 12c – EE Edition Feature

- Oracle Database Licensing Information 12c Release 1 (12.1)
  - https://docs.oracle.com/database/121/DBLIC/editions.htm#DBLIC116

Networking

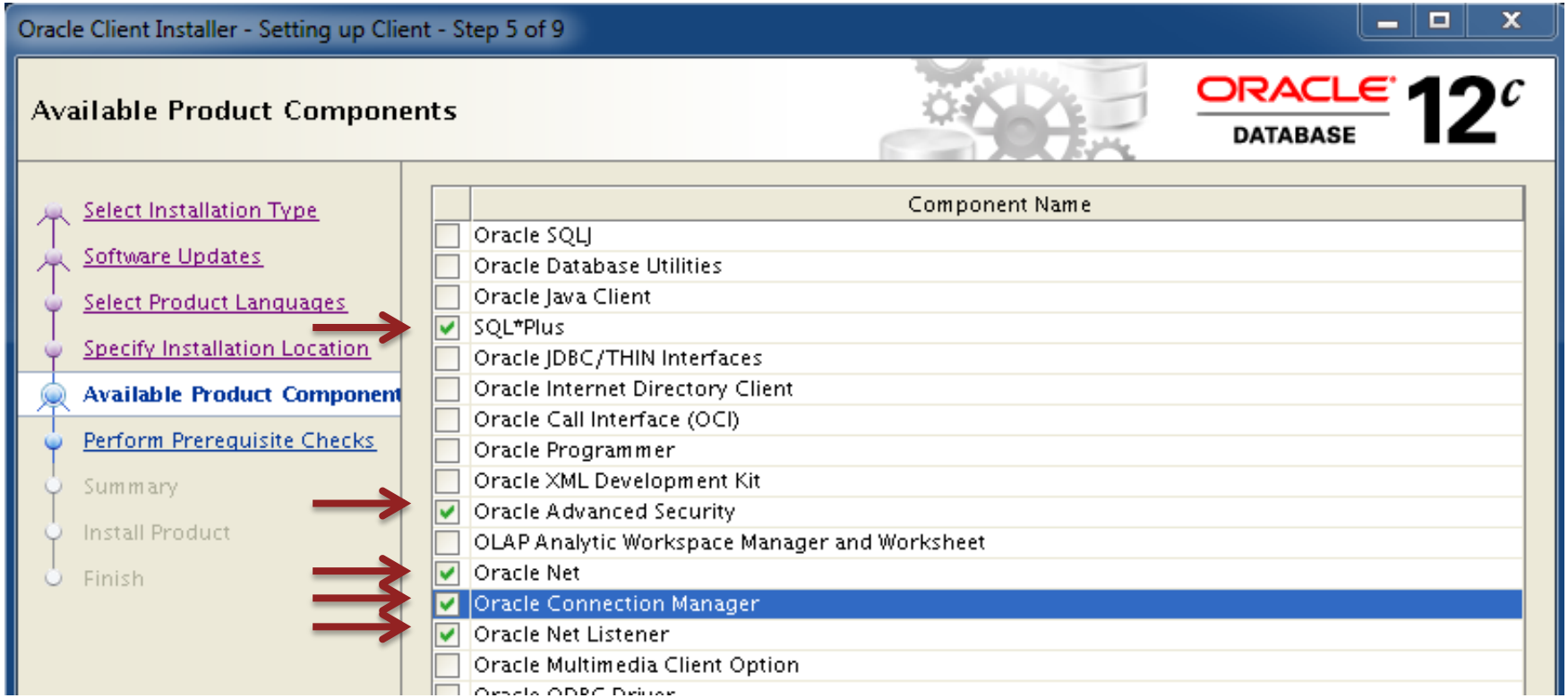
Oracle Connection Manager	N	N	Y	Available via a custom install of the Oracle Database client, usually installed on a separate machine See "Oracle Connection Manager" for more information

Oracle Connection Manager

Oracle Connection Manager can be installed and used on a machine different from the machine where the Oracle Database is installed and used. It is not necessary to obtain a separate license for the machine running Oracle Connection Manager.

Installation – CMAN Oracle 12c – (1)

- Im **Client** Installations-Packet enthalten!
  - Muss zusammen mit dem Oracle Listener installiert werden!



Installation – CMAN Oracle 12c – (2)

- Nach der Installation DB PSU einspielen!
  - opatch austauschen (Patch 6880880)
  - PSU mit „ opatch apply“ einspielen

Konfiguration über die cman.ora

- Datei **$ORACLE_HOME/network/admin/cman.ora**.
  - Jeder Fehler führt zu einem: „TNS-04012: Unable to start Oracle Connection Manager instance" !

```
cman_gpi =
(configuration=
    (address=(protocol=tcp)(host=oradb12c01.pipperr.local)(port=1999))
    (parameter_list =
        (aso_authentication_filter=off)
        (connection_statistics=yes)
        (log_level=user)
        (max_connections=256)
        (idle_timeout=0)
        (inbound_connect_timeout=0)
        (session_timeout=0)
        (outbound_connect_timeout=0)
        (max_gateway_processes=16)
        (min_gateway_processes=2)
        (remote_admin=on)
        (trace_level=off)
        (trace_timestamp=off)
        (trace_filelen=1000)
        (trace_fileno=1)
        (max_cmctl_sessions=4)
        (event_group=init_and_term,memory_ops)
    )
    (rule_list=
        (rule=
            (src=*)(dst=*)(srv=*)(act=accept)
            (action_list=(aut=off)(moct=0)(mct=0)(mit=0)(conn_stats=on))
        )
    )
)
```

siehe Support Node - Doc ID 733421.1

SQL*Net Konfiguration – Variante A - Routen

- Im SQL*Net Connect String ist die Routing Information enthalten

```
cman_gpi_db=
  (DESCRIPTION =
    (SOURCE_ROUTE = YES)
    (ADDRESS =
      (PROTOCOL = TCP)(HOST = 192.168.178.110 )(PORT = 1999)
    )
    (ADDRESS =
      (PROTOCOL = TCP)(HOST = 10.10.10.57)(PORT = 1521)
    )
    (CONNECT_DATA = (SERVICE_NAME=GPI)
    )
  )
```

CMAN IP Adresse und Port

DB Listener IP Adresse und Port

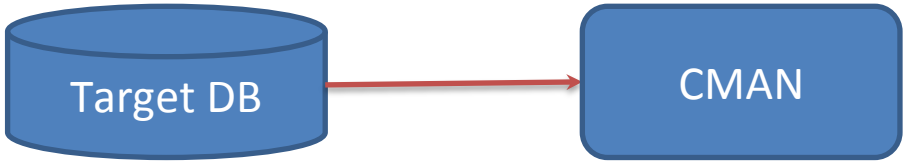
SQL*Net Konf. – Variante B - DB registriert (1)

- DB hat sich am CMAN angemeldet und CMAN kennt über den Servicenamen die richtige DB Verbindung
  - Init.ora - REMOTE_LISTENER Parameter

CMAN IP Adresse und Port

```
Alter system set REMOTE_LISTENER=192.168.178.110:1999
scope=both sid='*';
```

Registriert sich selbständig – Parameter REMOTE_LISTENER



Für RAC => Scan Listener IP Adressen + CMAN IP Adresse registrieren
Siehe auch Doc ID 1375897.1

SQL*Net Konf. – Variante B - DB registriert (2)

- Im SQL*Net Connect String steht nur der Connection Manager

```
gpi_db =
  (DESCRIPTION =
    (ADDRESS =
      (PROTOCOL = TCP)(HOST = 192.168.178.110 )(PORT = 1999)
    )
       (CONNECT_DATA = (SERVICE_NAME=GPI)
    )
  )
```

CMAN IP Adresse und Port

Nachteil : Eindeutige Servicenamen im Unternehmen notwendig

Lösung : Nur der Service für die Administration wird pro DB mit eindeutigen Namen registriert

Connection Manager härten

- Zugriffsregeln (Access Rules) einführen
  - Datei **$ORACLE_HOME/network/admin/cman.ora**

```
(RULE_LIST=
  (RULE=
    (SRC=host)
    (DST=host)
    (SRV=service_name)
    (ACT={accept|reject|drop})
    (ACTION_LIST=AUT={on|off}
    ((CONN_STATS={yes|no})(MCT=time)(MIT=time)(MOCT=time)))
  (RULE= ...))
```

Problem TNS-04011: … instance not yet started.

- Der Fehler:

```
CMCTL> administer cman_pb
Current instance cman_pb is not yet started
Connections refer to (address=(protocol=tcp)(host=oradb12c01.pipperr.local)(port=1999)).
The command completed successfully.

CMCTL:cman_pb> show all
TNS-04011: Oracle Connection Manager instance not yet started.
```

- Die Lösung:
  - Falls Access Rules => der lokale Client muss mit dem Connection Manager Admin Prozess kommunizieren dürfen

```
(rule=(src=oradb12c01.pipperr.local)
 (dst=*)(srv=cmon)(act=accept)
 )
```

Regel Parameter

- See https://docs.oracle.com/database/121/NETRF/cman.htm#NETRF337

Additional Parameters

The `RULE` parameter filters a connection or group of connections using the following parameters:

`SRC` : The source host name or IP address of the client.

`DST` : The destination server host name or IP address of the database server.

`SRV` : The database **service name** of Oracle Database obtained from the `SERVICE_NAME` parameter in the initialization parameter file.

`ACT` : The action for the connection request. Use `accept` to accept incoming requests, `reject` to reject incoming requests, or `drop` to reject incoming requests without sending an error message.

`ACTION_LIST` : The rule-level parameter settings for some parameters. These parameters are as follows:

- `AUT` : Oracle Database security authentication on client side.
- `CONN_STATS` : Log input and output statistics.
- `MCT` : Maximum connect time.
- `MIT` : Maximum idle timeout.
- `MOCT` : Maximum outbound connect time.

Rule-level parameters override their global counterparts.

Mit CMCTL: cman_gpi> reload
Neu laden!

SQL*Net Verschlüsselung

- Symmetrische Verschlüsselung
  - Ehemals Teil von ASO – Advanced Security Option
    - Die native Verschlüsselung scheint nun keine ASO Option mehr zu sein
    - Siehe http://docs.oracle.com/database/121/DBLIC/editions.htm#DBLIC119

Oracle Wallet

An Oracle Wallet is a PKCS#12 container used to store authentication and encryption keys. The Oracle database secure external password store feature stores passwords in an Oracle Wallet for password-based authentication to the Oracle database. The Oracle Wallet may also be used to store credentials for PKI authentication to the Oracle Database, configuration of network encryption (SSL/TLS), and Oracle Advanced Security transparent data encryption (TDE) master encryption keys. Strong authentication services (Kerberos, PKI, and RADIUS) and network encryption (native network encryption and SSL/TLS) are no longer part of Oracle Advanced Security and are available in all licensed editions of all supported release of the Oracle database.

  - Wird auf dem Client/Server konfiguriert – CMAN leitet das transparent jeweils weiter!

Im Detail siehe
http://www.pipperr.de/dokuwiki/doku.php?id=dba:sql_net_security

SSL unter SQL*Net verwenden (1)

- SQL*Net über SSL
  - Wird nicht vom CMAN unterstützt!
  - Etwas mehr Rechenleistung (und damit etwas weniger Performance) notwendig
  - In allen Editionen ohne weitere Lizenz enthalten

Vorteil: Zertifikat identifiziert die Clients bei Bedarf

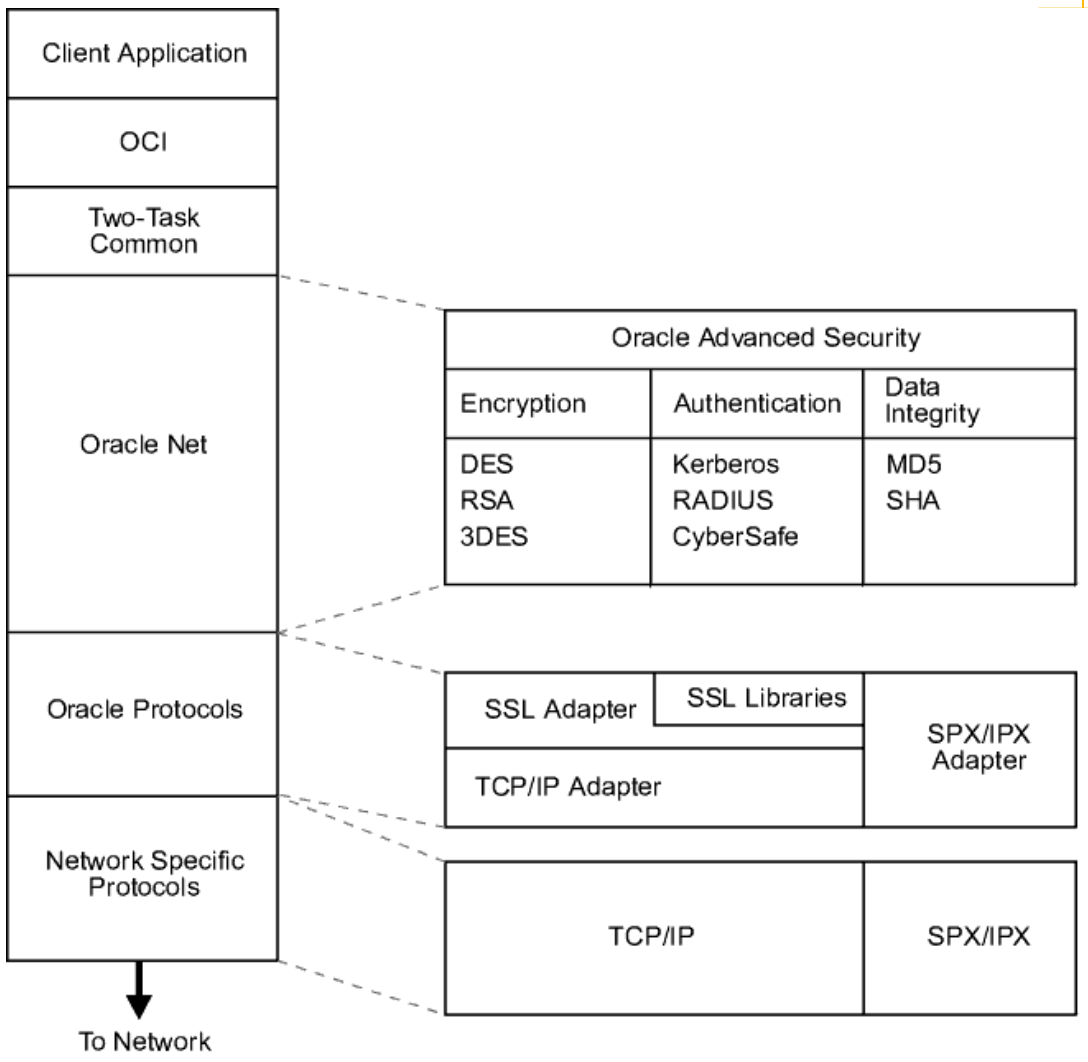


Abbildung aus http://docs.oracle.com/cd/B10501_01/network.920/a96573/asossl.htm

SSL unter SQL*Net verwenden (2)

- Ablauf
  - Wallet muss auf Client und dem Server Listener eingerichtet werden
  - Zertifikate werden dann in die jeweiligen Wallets ausgetauscht
  - Sqlnet.ora und listener.ora anpassen
  - In SQL*Plus überprüfen mit :

```
SELECT SYS_CONTEXT('USERENV','NETWORK_PROTOCOL') AS connect_protocol FROM dual;

CONNECT_PROTOCOL
 -------------------
tcps
```

Im Detail siehe
http://www.pipperr.de/dokuwiki/doku.php?id=dba:sql_net_ssl

Weitere Härtung – DB Listener einschränken

- Nur noch über den Connection Manager sind Anmeldungen zulässig
  - sqlnet.ora des Listener anpassen

```
TCP.VALIDNODE_CHECKING=YES

TCP.INVITED_NODES=(10.10.10.110)
```

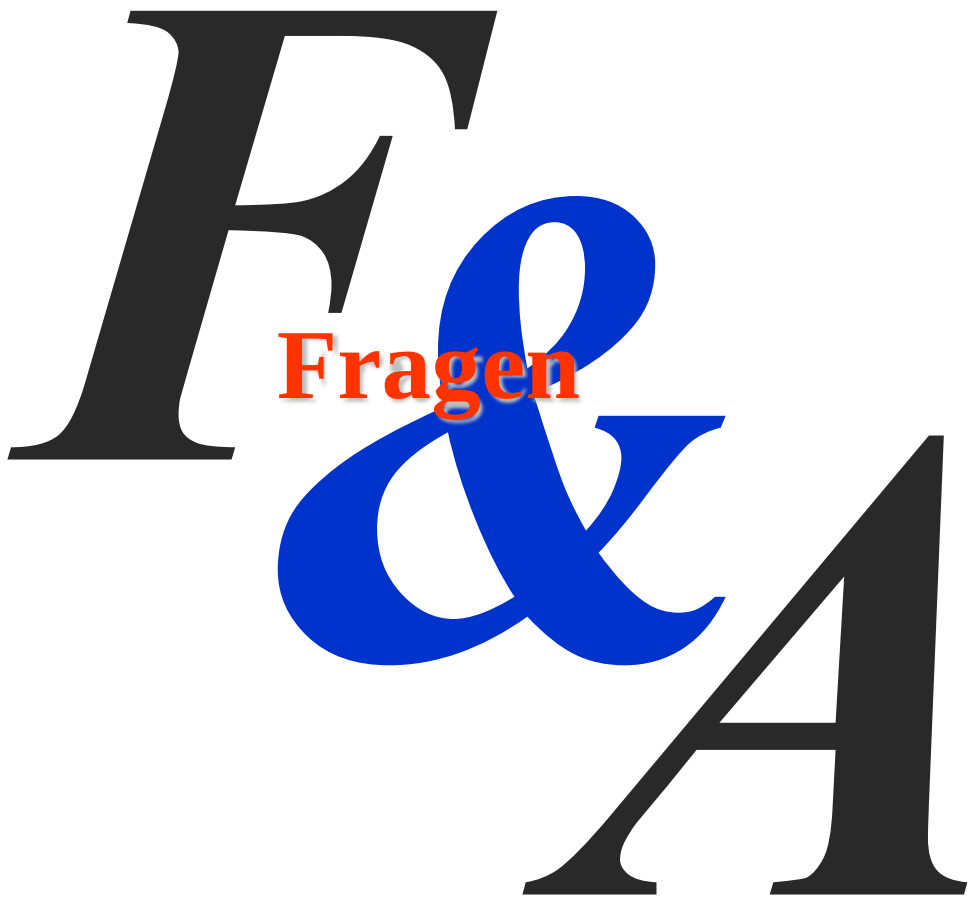
CMAN IP Adresse

Vorteil: Zusätzliche Sicherung

Fazit

- CMAN – Ein Baustein für die organisatorische Trennung von Zugriffen auf Datenbanken
- Für vollständige Implementierung des Konzepts SQL*Net Verschlüsselung mit implementieren
- SSL leider zur Zeit nicht unterstützt

Installation im Detail siehe:
http://www.pipperr.de/dokuwiki/doku.php?id=dba:sqlnet_cman_connection_manager



Der Oracle Connection Manager (CMAN)
als Firewall für das Routing von Datenbank Verbindungen