Redpill Linpro

Secure PostgreSQL Deployments

JDCon-East 2010
Philadelphia, PA

Magnus Hagander
Redpill Linpro AB

Redpill Linpro

There's much to security

- Identify the threats
- Apply the *correct* measures
  - Don't do things just because you can

Redpill Linpro

Not in this talk

- Application security
- Data Access Control
- Data Encryption
- etc
- etc

Redpill Linpro

Definitely not in this talk

- Unix vs Windows
- Linux vs BSD
- SELinux/SEPostgreSQL
- Any other religion

Redpill Linpro

In this talk!

- Authentication methods
- Connection security

Redpill Linpro

Authentication methods

- How do we determine who the user is
- *When* do we determine who the user is

Redpill Linpro

pg_hba.conf

- Lets you use different auth methods from different clients
- Not just limited to username/password
- For convenience or security
- Internal or external

Redpill Linpro

pg_hba.conf

```
local     all     all                              trust
host      all     all     127.0.0.1/32             trust
host      webdb   webuser 10.0.0.0/24              md5
host      all     @dba    192.168.0.0/24 gss
```

Redpill Linpro

Trust Authentication

- Any user can be anyone he/she claims to be!

Redpill Linpro

Trust Authentication

- Any user can be anyone he/she claims to be!
- Anyone think this is a bad idea?

Redpill Linpro

Username/password

- Normally, use *md5* method
  - crypt has been removed, avoid plaintext
- What everybody does
- What everybody *expects*

Redpill Linpro

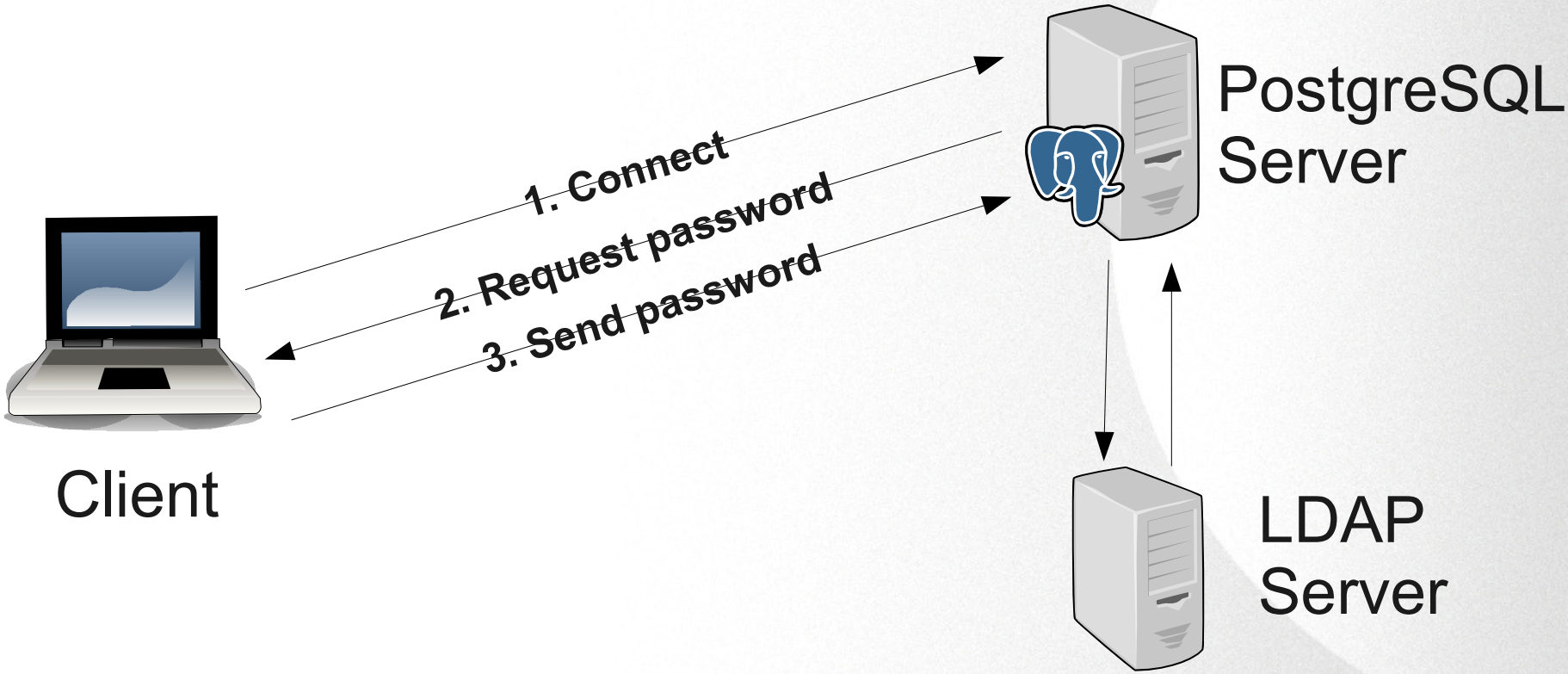
LDAP authentication

- To the client, username/password
- Backend verification is off-loaded to directory server
- Common in enterprise deployments
- Password policies, expiry, etc

Redpill Linpro

LDAP authentication

- Single *password* not single *signon*



Redpill Linpro

LDAP news in 9.0

- search/bind combination
- Can use non-cn fields in login
  - Anything that's LDAP searchable
  - Common choice: uid

Redpill Linpro

RADIUS (new in 9.0)

- Remote Authentication Dial In User Service
- Simple single-packet UDP service
- Original use-case: ISP dialup
- Common for one-time passwords, etc
- Good policy frameworks

Redpill Linpro

Kerberos/GSSAPI/SSPI

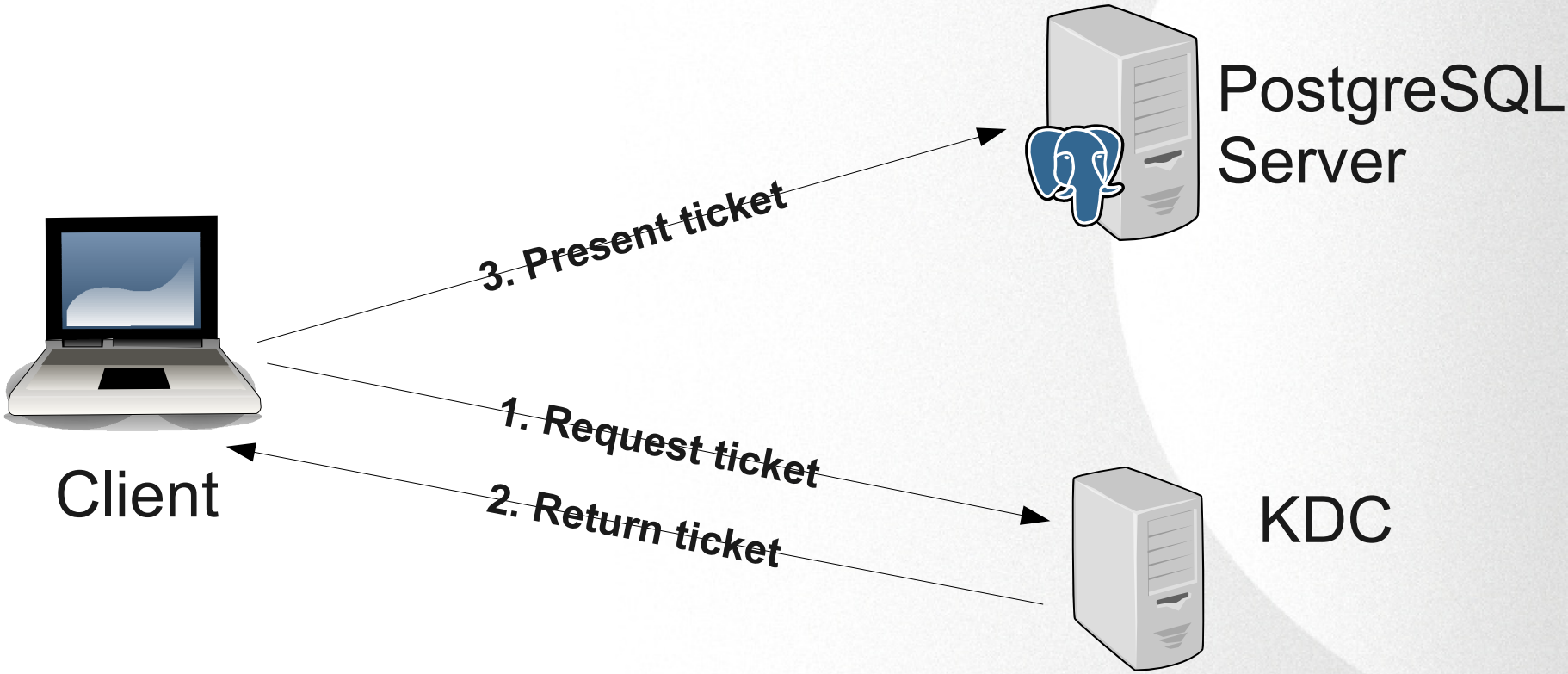
- Single *signon*
- Same benefits as LDAP (mostly)
- Most common: Active Directory

- («krb5» is deprecated)

Redpill Linpro

Kerberos/GSSAPI/SSPI

- Single *password* not single *signon*



Redpill Linpro

PAM

- Provided by OS
- Can do password, LDAP, etc
- Can also do Kerberos & friends
- One-time passwords
  - RSA SecurID, Vasco, etc
  - RADIUS (no need in 9.0)

Redpill Linpro

SSL

Redpill Linpro

SSL secured connections

- Encryption
- Man-in-the-middle protection
- Authentication

Redpill Linpro

SSL secured connections

- Enabled on the server (ssl=yes)
  - Platform quirks!
- Optionally required through pg_hba
- Optionally required in libpq

Redpill Linpro

SSL secured connections

- Need to protect data in *both* directions
- For example username/password
- Must *know* before connection is started
  - Unknown equals unprotected

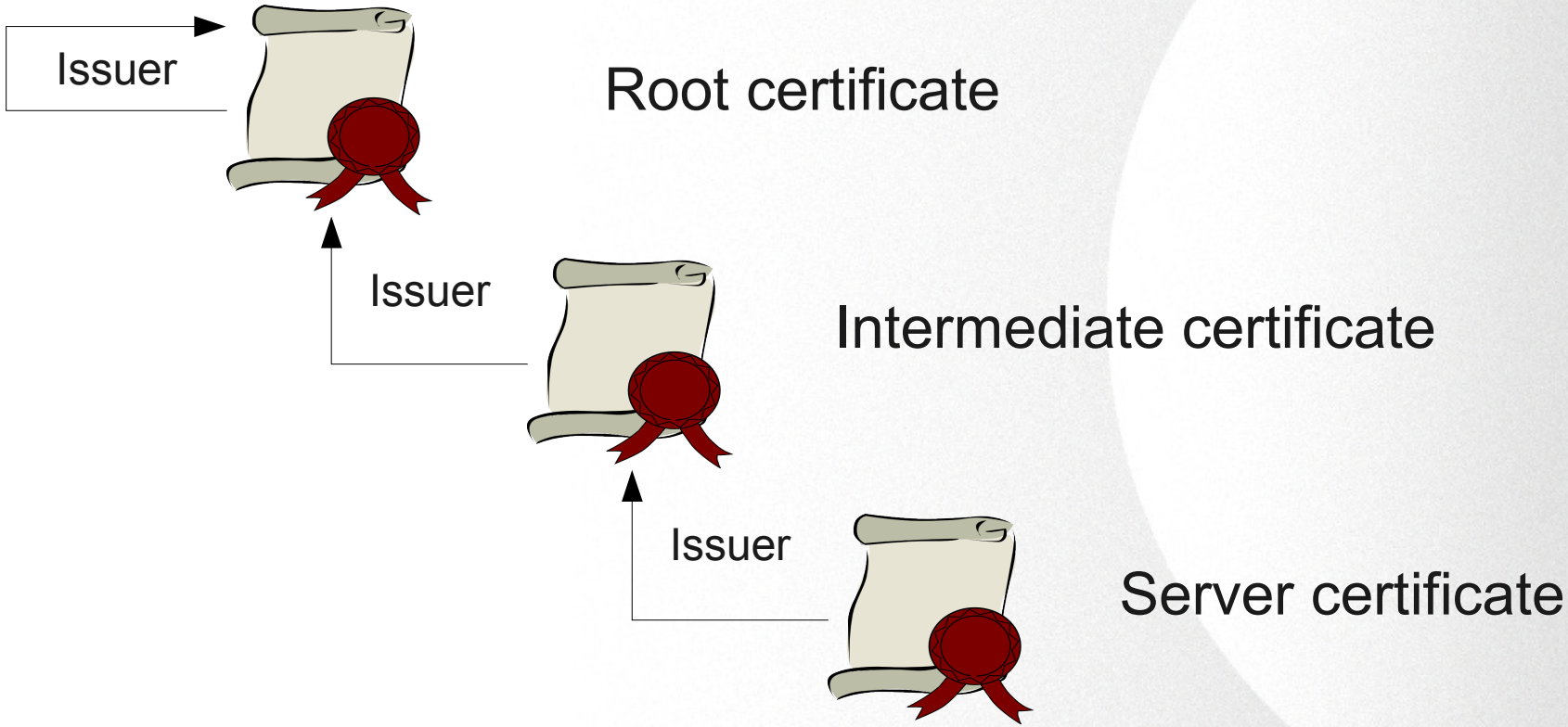
Redpill Linpro

SSL encryption

- SSL *always* requires a server certificate
- Can be self-signed
- Does not need to be known by client

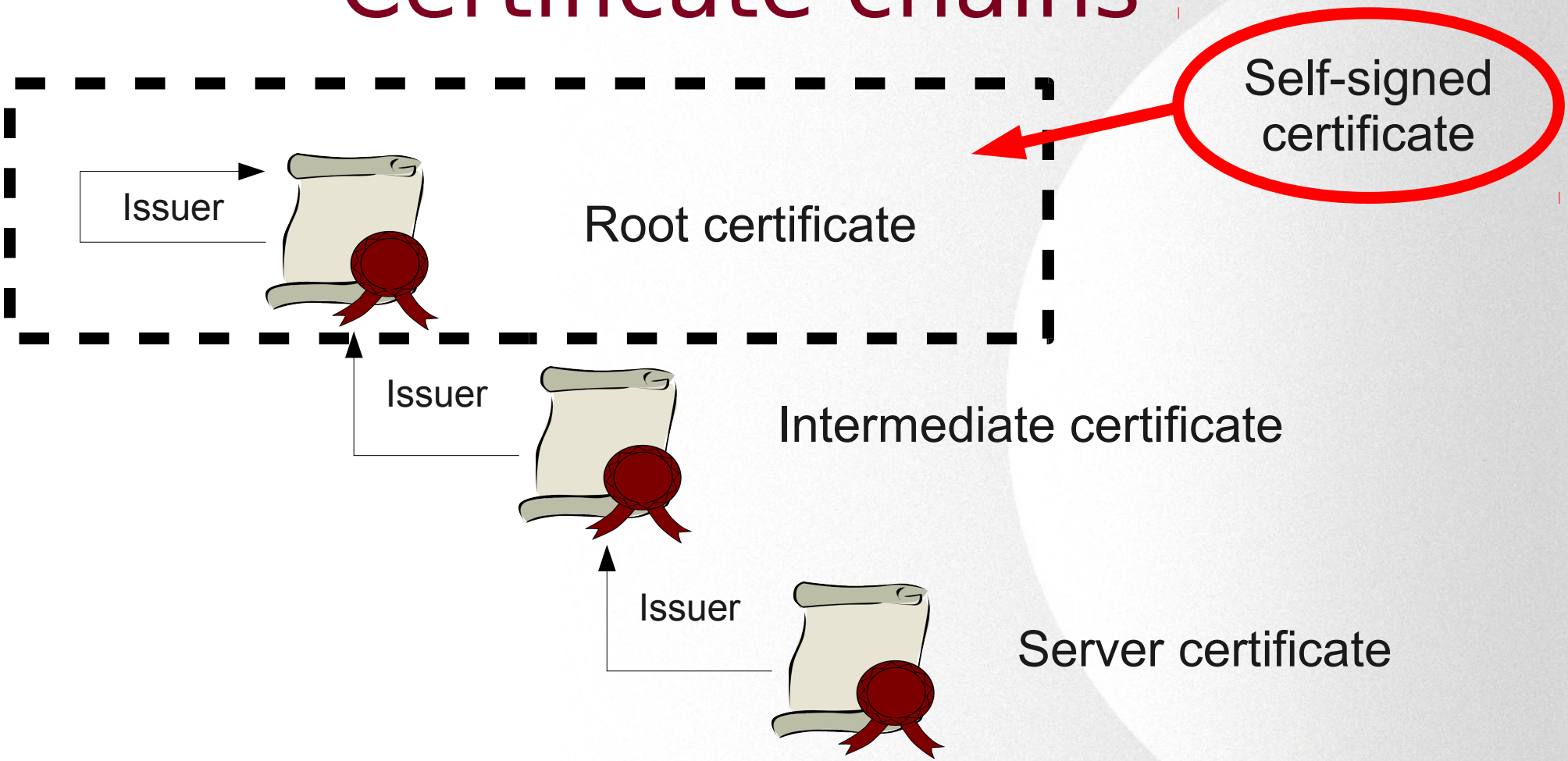
Redpill Linpro

Certificate chains



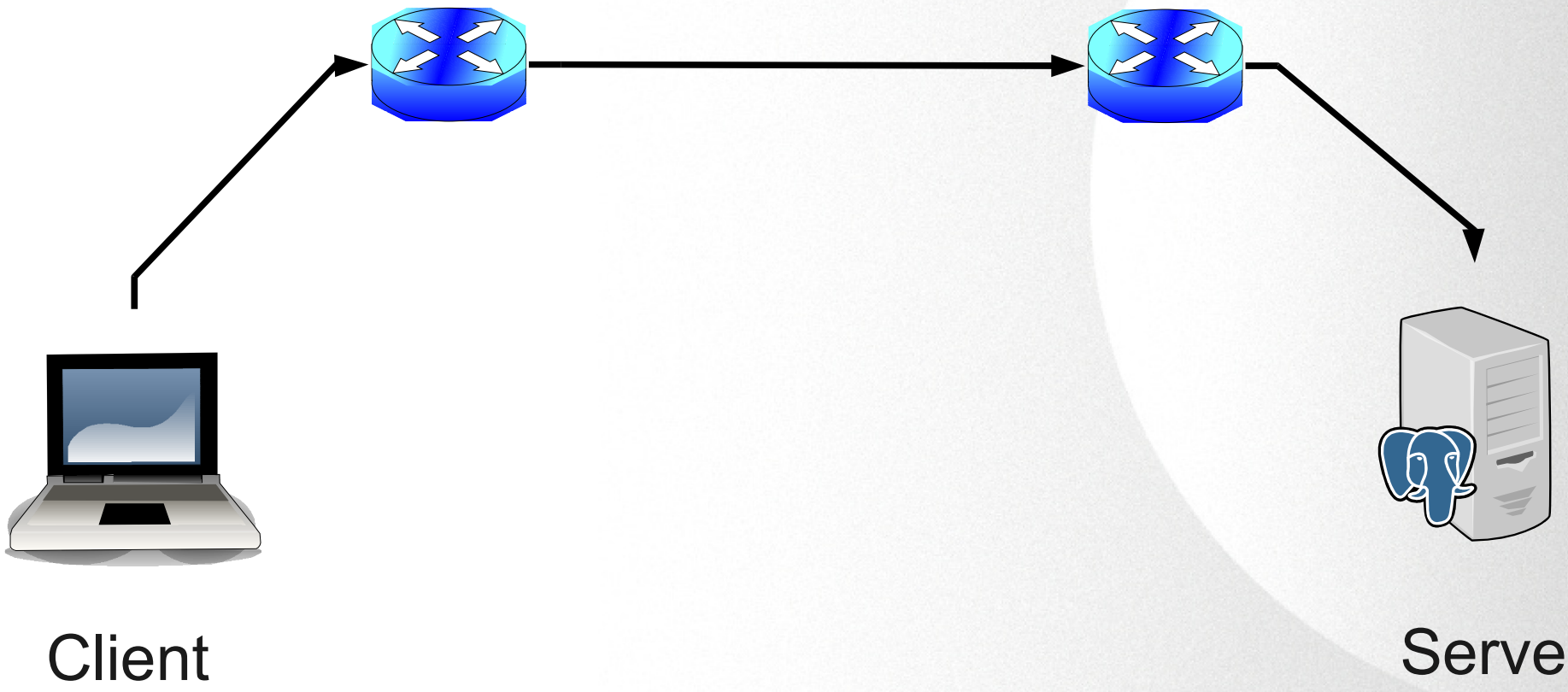
Redpill Linpro

Certificate chains



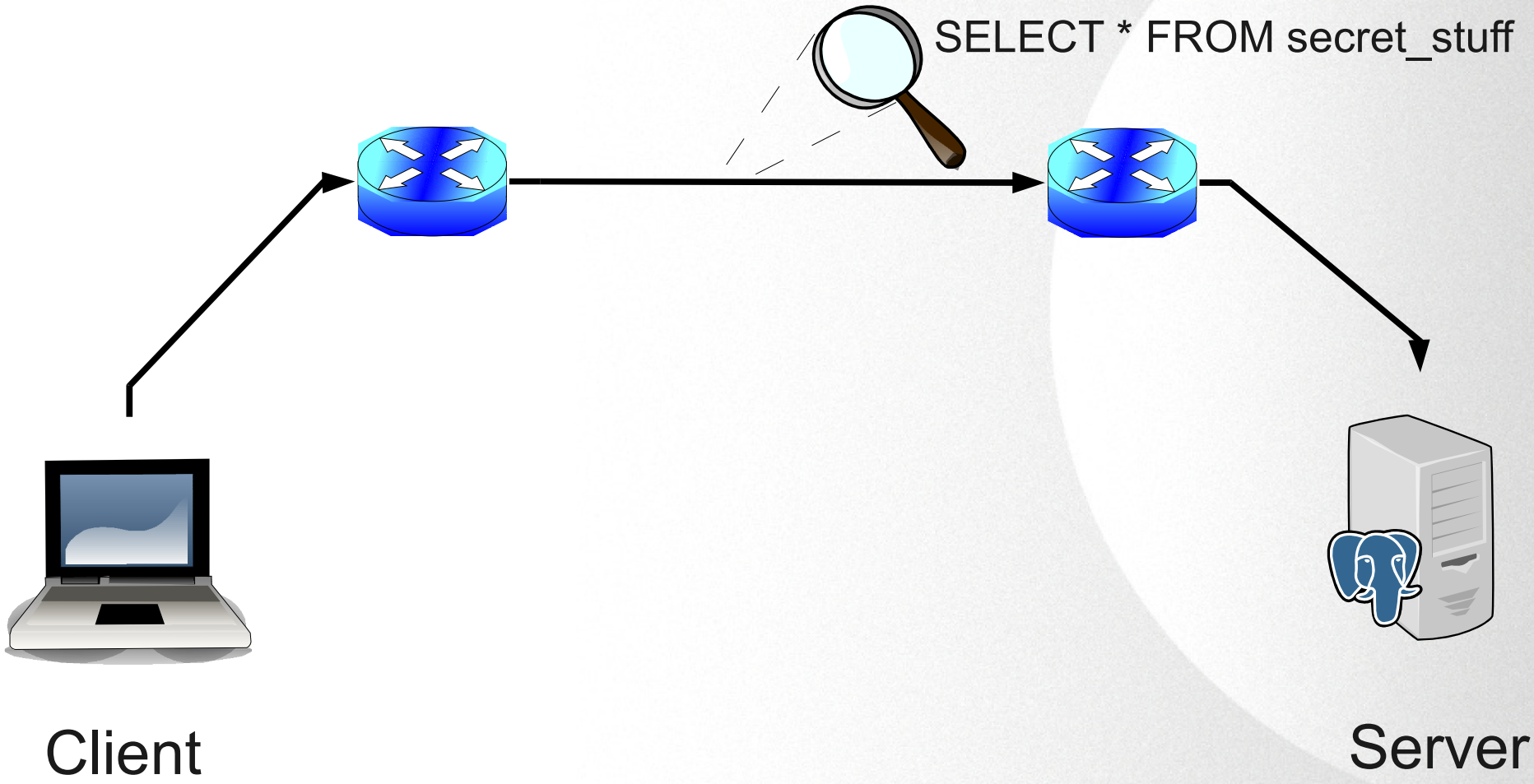
Redpill Linpro

SSL secured connections



Redpill Linpro

Threats handled by SSL: Eavesdropping



Redpill Linpro

Eavesdropping

- Prevented by encrypting all data
- Key negotiation is automatic
  - On initial connection
  - After 512Mb traffic
- Server certificate used but not verified

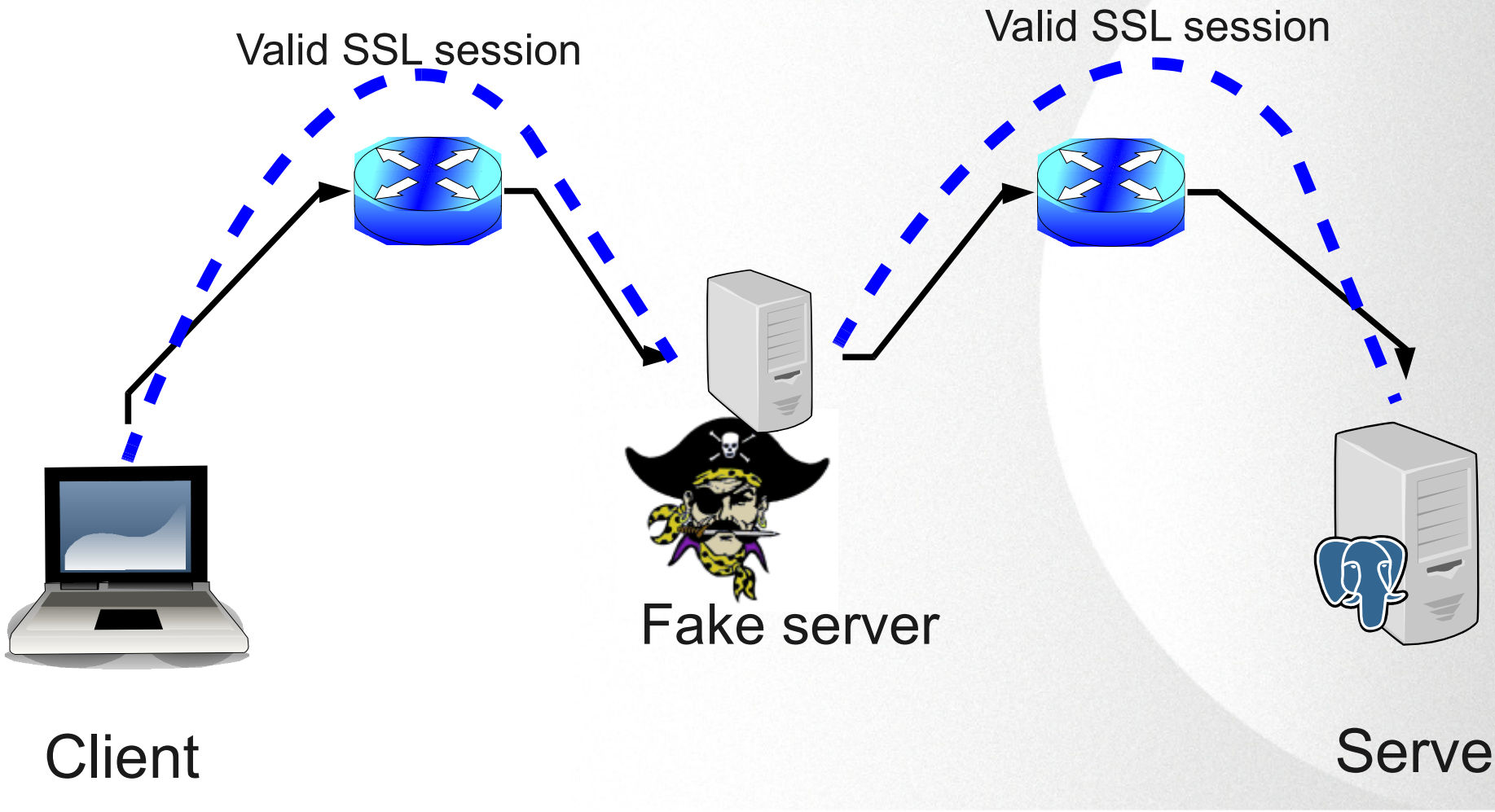
Redpill Linpro

Key renegotiation

- *Broken in the SSL protocol – OOPS!*
- Fixed SSL libraries *are* available
- Broken fixes were pushed by vendors
- ssl_renegotiation_limit = 512MB

Redpill Linpro

Threats handled by SSL: Man in the middle



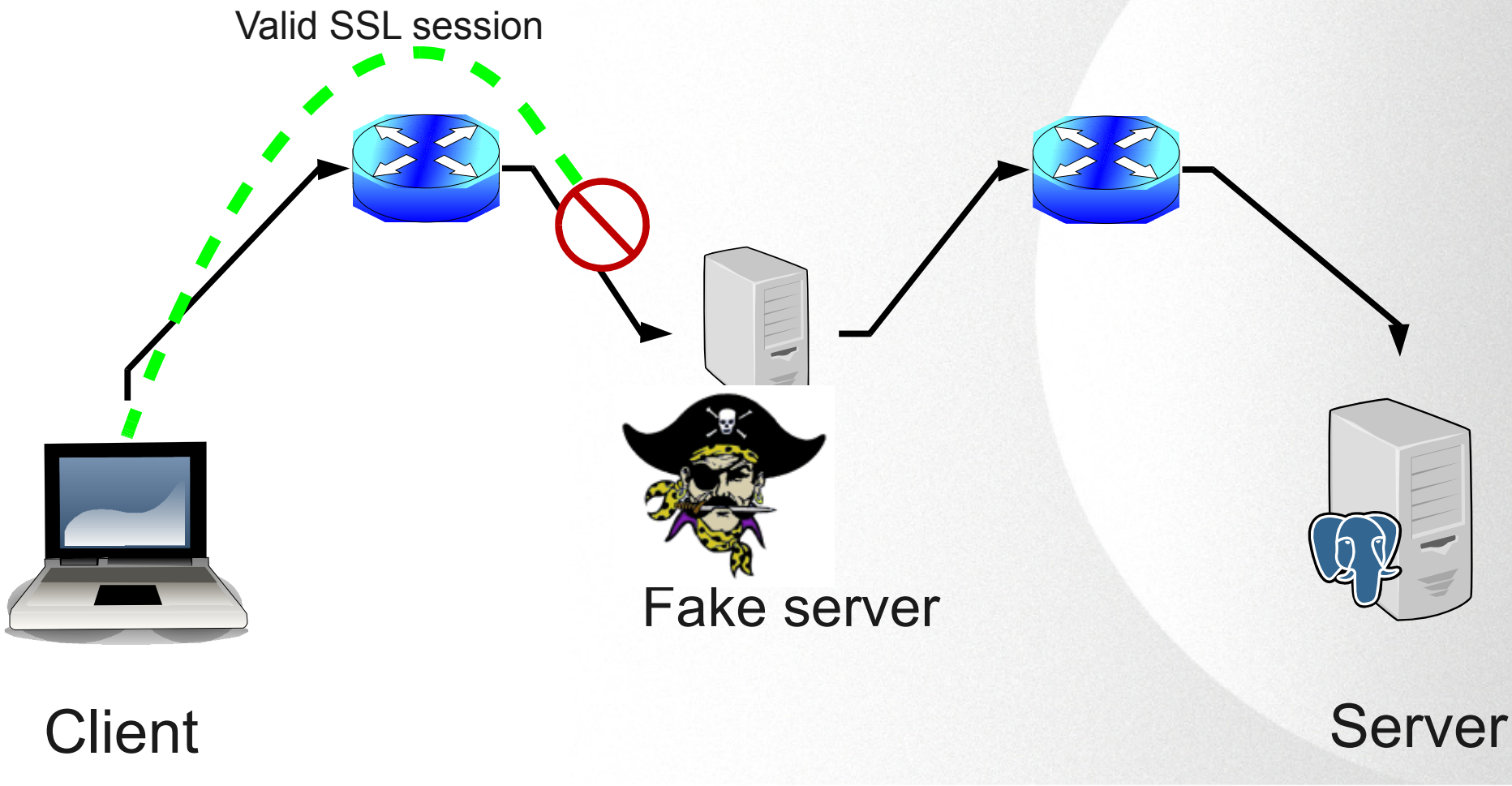
Redpill Linpro

SSL server verification

- On top of encryption
- Validate that the server is who it claims to be
- CA issues certificate, can be self-signed
- CA certificate known by client

Redpill Linpro

Threats handled by SSL: Man in the middle



Redpill Linpro

SSL client authentication

- On top of encryption
- Normally on top of server verificateion, but not necessary
- CA issued certificate on *client*
- Match *CN* on certificate to user id
- Protect client certificate!

Redpill Linpro

SSL client authentication

Redpill Linpro

SSL client certificates

- Can also be used *together* with other authentication
- Require client certificate
- *Also* require e.g. username/password

Redpill Linpro

SSL in libpq

- Controlled by *sslmode* parameter
- Or environment *PGSSLMODE*
- For security, must be set on client
  - Remember, *unknown = unsecure*

Redpill Linpro

Summary of libpq SSL modes

Client Mode	Protect against		Compatible with server set to		Performance overhead
	Eavesdrop	MITM	SSL required	SSL disabled	
disable	no	no	FAIL	works	no
allow	no	no	works	works	If necessary
prefer	no	no	works	works	If possible
require	yes	no	works	FAIL	yes
verify-ca	yes	yes	works	FAIL	yes
verify-full	yes	yes	works	FAIL	yes

Redpill Linpro

Summary of libpq SSL modes

Client Mode	Protect against		Compatible with server set to		Performance overhead
	Eavesdrop	MITM	SSL required	SSL disabled	
disable	no	no	FAIL	works	no
allow	no	no	works	works	If necessary
prefer	no	no	works	works	If possible
require	yes	no	works	FAIL	yes
verify-ca	yes	yes	works	FAIL	yes
verify-full	yes	yes	works	FAIL	yes

Redpill Linpro

Summary of libpq SSL modes

	Protect against		Compatible with server set to		Performance
Client Mode	Eavesdrop	MITM	SSL required	SSL disabled	overhead
disable	no	no	FAIL	works	no
allow	no	no	works	works	If necessary
prefer	no	no	works	works	If possible
require	yes	no	works	FAIL	yes
verify-ca	yes	yes	works	FAIL	yes
verify-full	yes	yes	works	FAIL	yes

Redpill Linpro

Summary of libpq SSL modes

Client Mode	Protect against		Compatible with server set to		Performance overhead
	Eavesdrop	MITM	SSL required	SSL disabled	
disable	no	no	FAIL	works	no
allow	no	no	works	works	If necessary
prefer	no	no	works	works	**If possible**
require	yes	no	works	FAIL	yes
verify-ca	yes	yes	works	FAIL	yes
verify-full	yes	yes	works	FAIL	yes

Redpill Linpro

Not a bad idea: ipsec

- If already deployed
- Application transparent
- Global policies
- Integrated management
- Somebody Elses Problem?

Redpill Linpro

Secure PostgreSQL Deployments

Questions?

magnus@hagander.net
Twitter: @magnushagander
http://blog.hagander.net