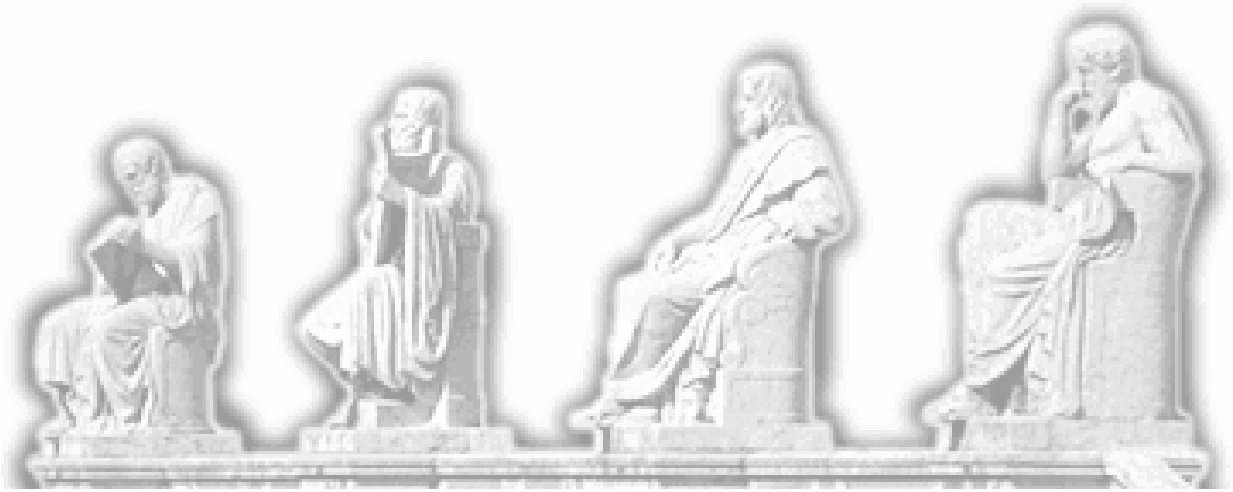
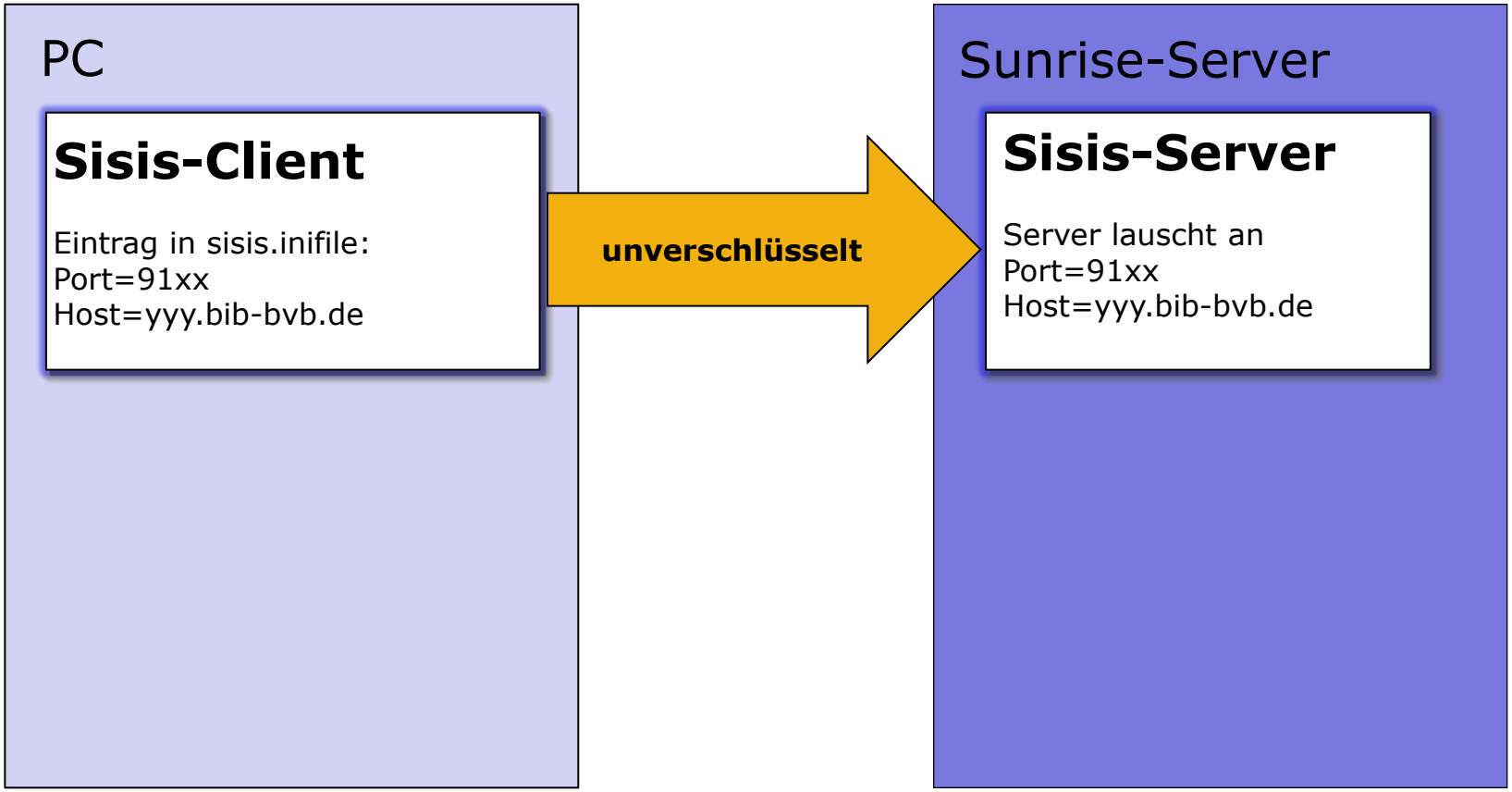
Der Einsatz von stunnel in den Verbund-Bibliotheken

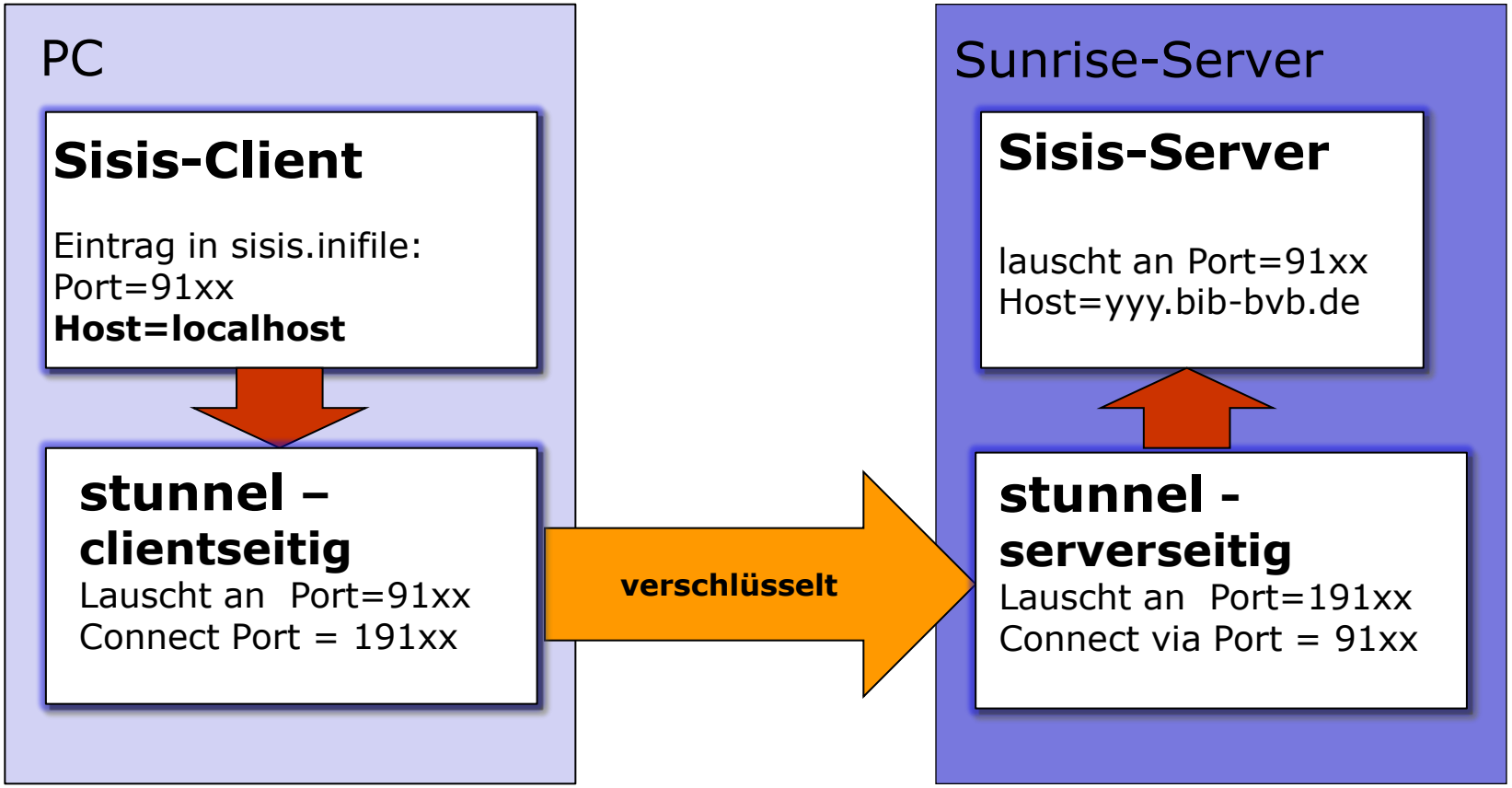
Von Frank Dietz (BVB/A)



Beispiel: Client-Server Verbindung ohne stunnel



Beispiel: verschlüsselte Client-Server Verbindung mit stunnel



Status stunnel-Verfügbarkeit im ASP

Serverseitig ist stunnel auf allen ASP-Rechnern für Echt- und Testsysteme eingerichtet

- stunnel-Installation und Zertifikate: LRZ
- stunnel-Konfiguration: BVB-A
- Eingerichtet ist stunnel für die Verschlüsselung zu AV- und CATserver
- Firewall-Freischaltung für Ihren stunnel auf Serverseite: erfolgt standardmässig für alle Benutzer, die schon bisher den unverschlüsselten Zugang zu AV- und CATserver haben
- Ablaufdatum der für die Verschlüsselung verwendeten Zertifikate: 2019

Wenn Sie die Sicherheit von stunnel nutzen möchten ….

…. müssen Sie nur noch die **clientseitige** Installation von stunnel durchführen.

Die Installationsdateien können Sie per Mail anfordern von Frank.Dietz@bsb-muenchen.de
Sie erhalten dann

- Installationsanleitung für Win7
- Installationsanleitung für Win XP
- Zertifikatsdatei stunnel_client_chain.pem
- Ihre (fertige) Konfigurationsdatei stunnel.conf

Was Sie noch tun müssen (und in den Anleitungen beschrieben wird)

- Download und Installation der aktuellsten stunnel-SW (stunnel-n.mm-installer.exe)
- stunnel_client_chain.pem und stunnel.conf ins Installations-directory kopieren
- stunnel als Dienst einrichten
- Reboot ihres PC
- vielleicht müssen die serverseitigen stunnel Ports (181xx, 191xx) in ihrem Netz noch freigeschaltet werden

Test Ihrer stunnel Installation

- der Mischbetrieb von Client-Server Verbindungen mit und ohne stunnel ist möglich
- Sie können sukzessive Ihre Clients auf Betrieb unter stunnel umstellen

Test Ihrer stunnel Installation

Ihre Installation ist erfolgreich, wenn sich Ihr Client über localhost mit dem Sisis-Server verbinden kann.

Screenshot aus der Info eines Clients:

Änderung in der Protokollierung

Ohne stunnel enthält die Serverlogdatei die IP-Adresse des Client-Anwenders

06.06.2013 14:56:02.033 SLNP-Demon CATServer <12586> : New connection. **Origin address=194.95.59.37**

Diese Info geht an dieser Stelle durch den Einsatz von stunnel verloren

07.06.2013 08:09:34.532 SLNP-Demon CATServer <14373> : New connection. **Origin address=localhost**

und wird stattdessen nun in stunnel.log protokolliert:

bash-3.2$ tail /var/opt/csw/lib/stunnel/stunnel.log
…….
2013.06.07 08:09:34 LOG5[19014:2]: catserver-fhmsis accepted connection from **194.95.59.37**:40201

Zum Schluss

- zur Zeit wird stunnel von 16 ASP-Biblioheken genutzt
- … vielen Dank für Ihre Aufmerksamkeit