quick documentation

TO:

FROM: ARND.SPIERING@AS-INFORMATIK.NET

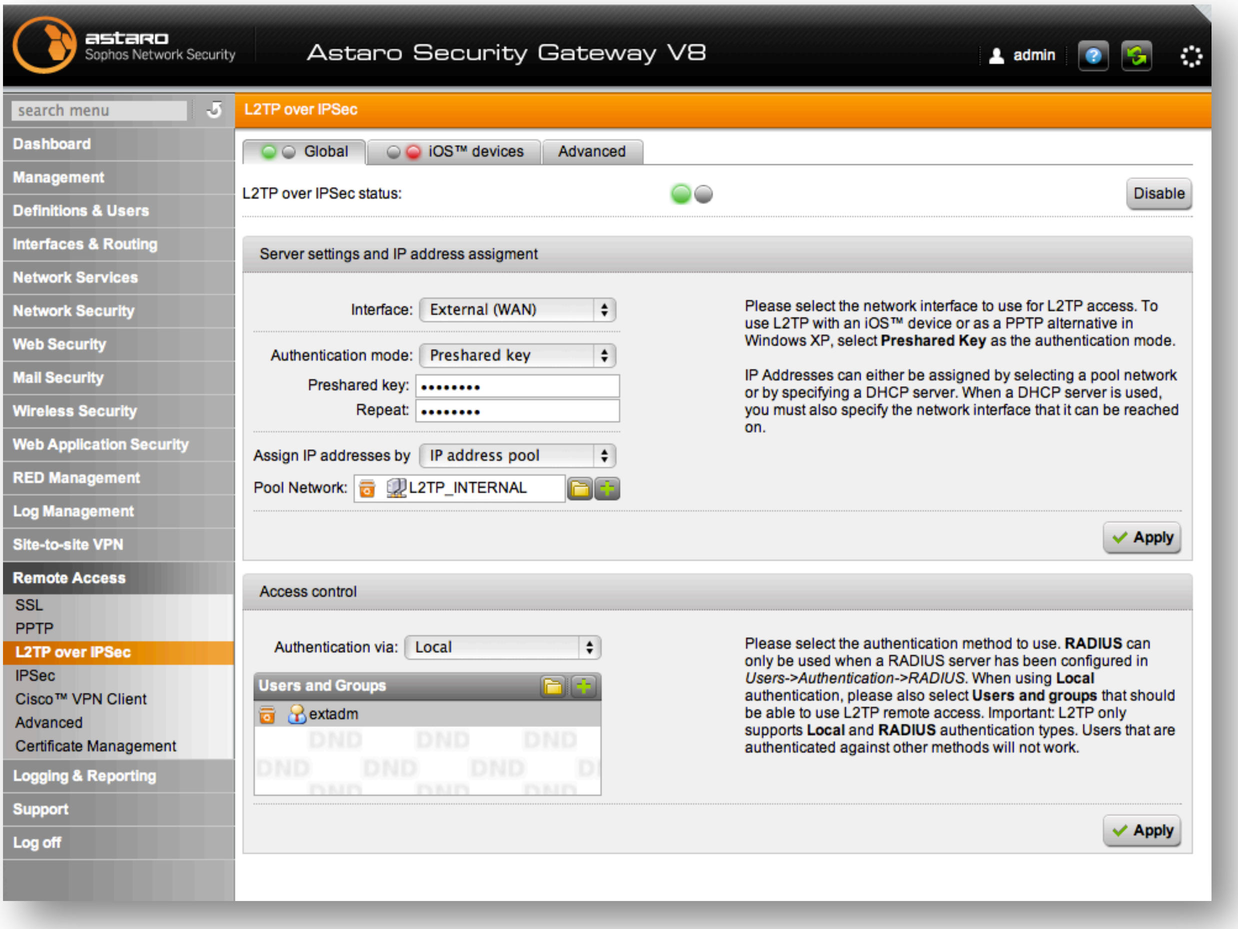
SUBJECT: ASTARO ESSENTIAL FIREWALL L2TP MIT IPSEC

DATE: 27.11.2011

Inhalt

Dieses Dokument beschreibt die Konfiguration der Astaro Essential Firewall für einen L2TP VPN Zugriff.

Konfiguration der Firewall



L2TP over IPSec

L2TP over IPSec status: ●●

Server settings and IP address assigment

Interface: External (WAN)

Authentication mode: Preshared key

Preshared key: ••••••••

Repeat: ••••••••

Assign IP addresses by IP address pool

Pool Network: L2TP_INTERNAL

Please select the network interface to use for L2TP access. To use L2TP with an iOS™ device or as a PPTP alternative in Windows XP, select **Preshared Key** as the authentication mode.

IP Addresses can either be assigned by selecting a pool network or by specifying a DHCP server. When a DHCP server is used, you must also specify the network interface that it can be reached on.

Access control

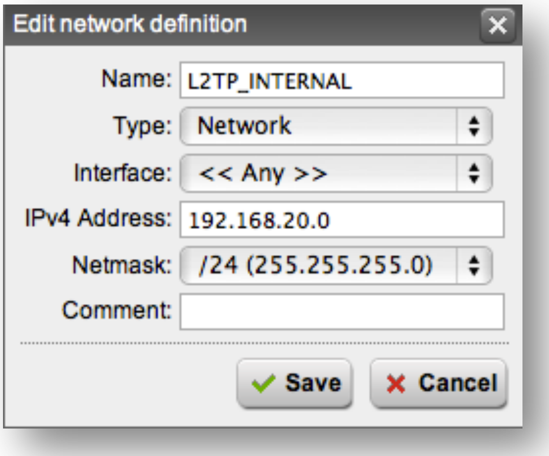
Authentication via: Local

Users and Groups

extadm

Please select the authentication method to use. **RADIUS** can only be used when a RADIUS server has been configured in *Users->Authentication->RADIUS*. When using **Local** authentication, please also select **Users and groups** that should be able to use L2TP remote access. Important: L2TP only supports **Local** and **RADIUS** authentication types. Users that are authenticated against other methods will not work.

Ein Pool Network mit folgenden Einstellungen wird angelegt:



Edit network definition

Name: L2TP_INTERNAL

Type: Network

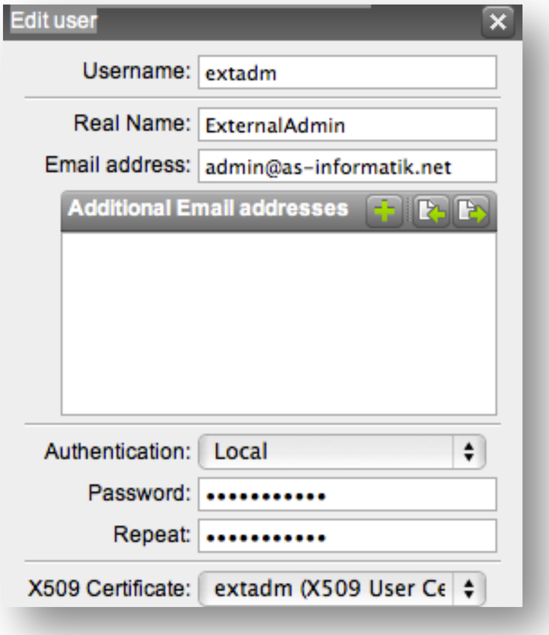
Interface: << Any >>

IPv4 Address: 192.168.20.0

Netmask: /24 (255.255.255.0)

Comment:

Ein Benutzer für den externen Zugriff wird angelegt:



Edit user

Username: extadm

Real Name: ExternalAdmin

Email address: admin@as-informatik.net

Additional Email addresses

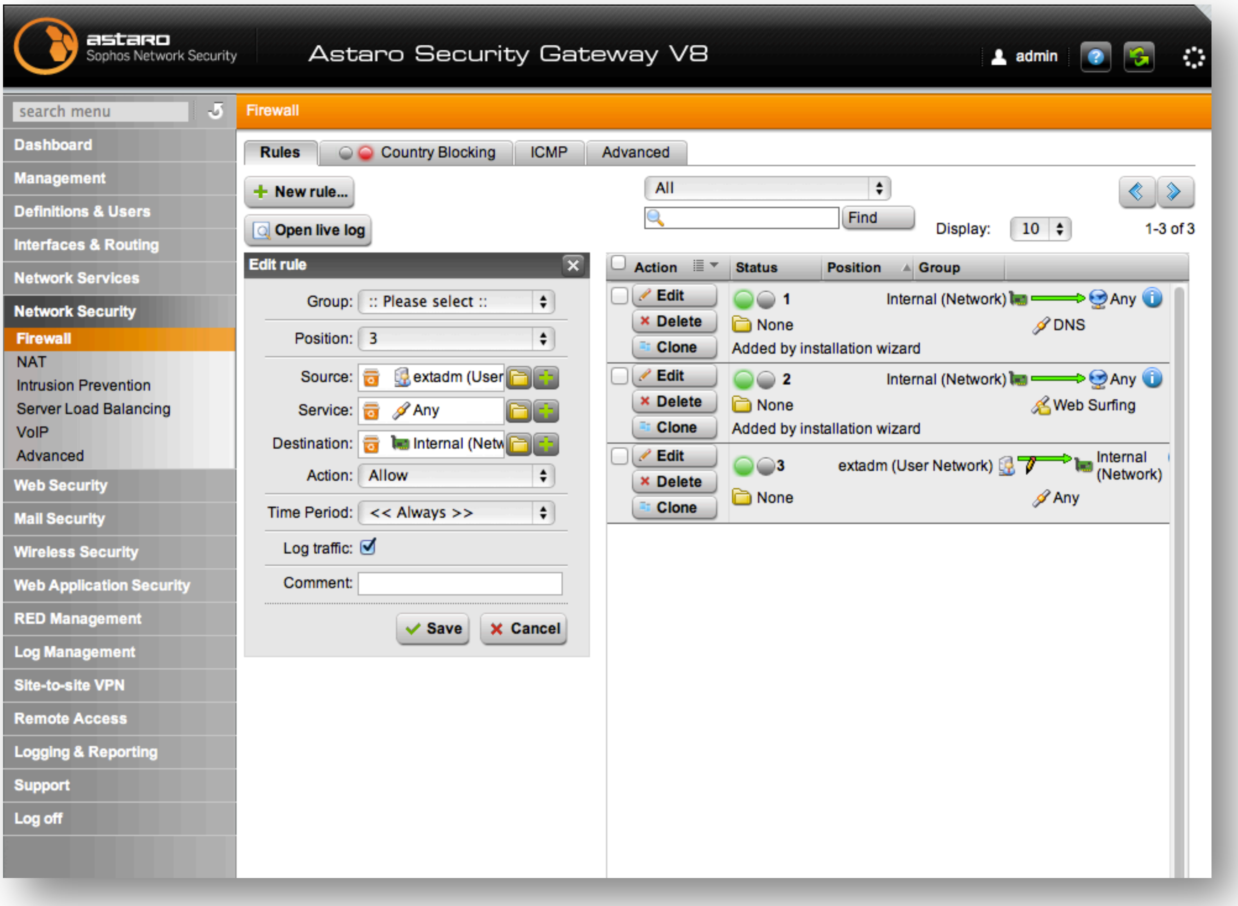
Authentication: Local

Password: ●●●●●●●●●●●

Repeat: ●●●●●●●●●●●

X509 Certificate: extadm (X509 User Ce

Mit diesen Einstellungen kann sich ein Client verbinden, hätte aber keinen Zugriff auf das interne Netz. Dafür muss auf der Firewall noch eine entsprechende Regel eingerichtet werden:



Edit rule

Group: :: Please select ::

Position: 3

Source: extadm (User

Service: Any

Destination: Internal (Netw

Action: Allow

Time Period: << Always >>

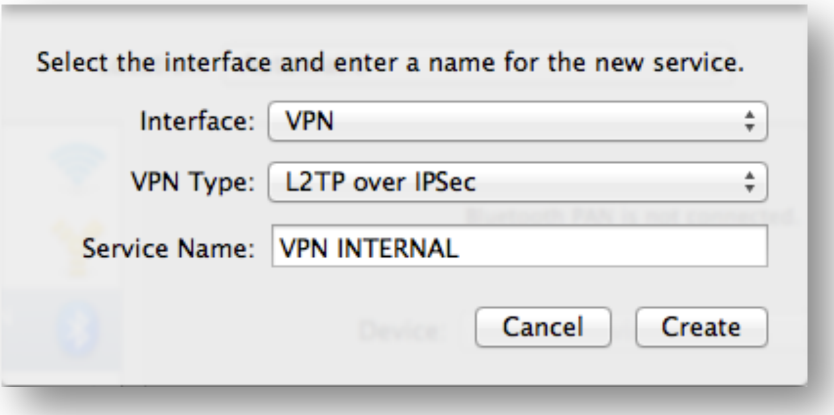
Log traffic: ☑

Comment:

Action	Status	Position	Group	
Edit Delete Clone	● ○	1 None Added by installation wizard		Internal (Network) → Any DNS
Edit Delete Clone	● ○	2 None Added by installation wizard		Internal (Network) → Any Web Surfing
Edit Delete Clone	● ○	3 None		extadm (User Network) → Internal (Network) Any

VPN Konfiguration auf dem MAC

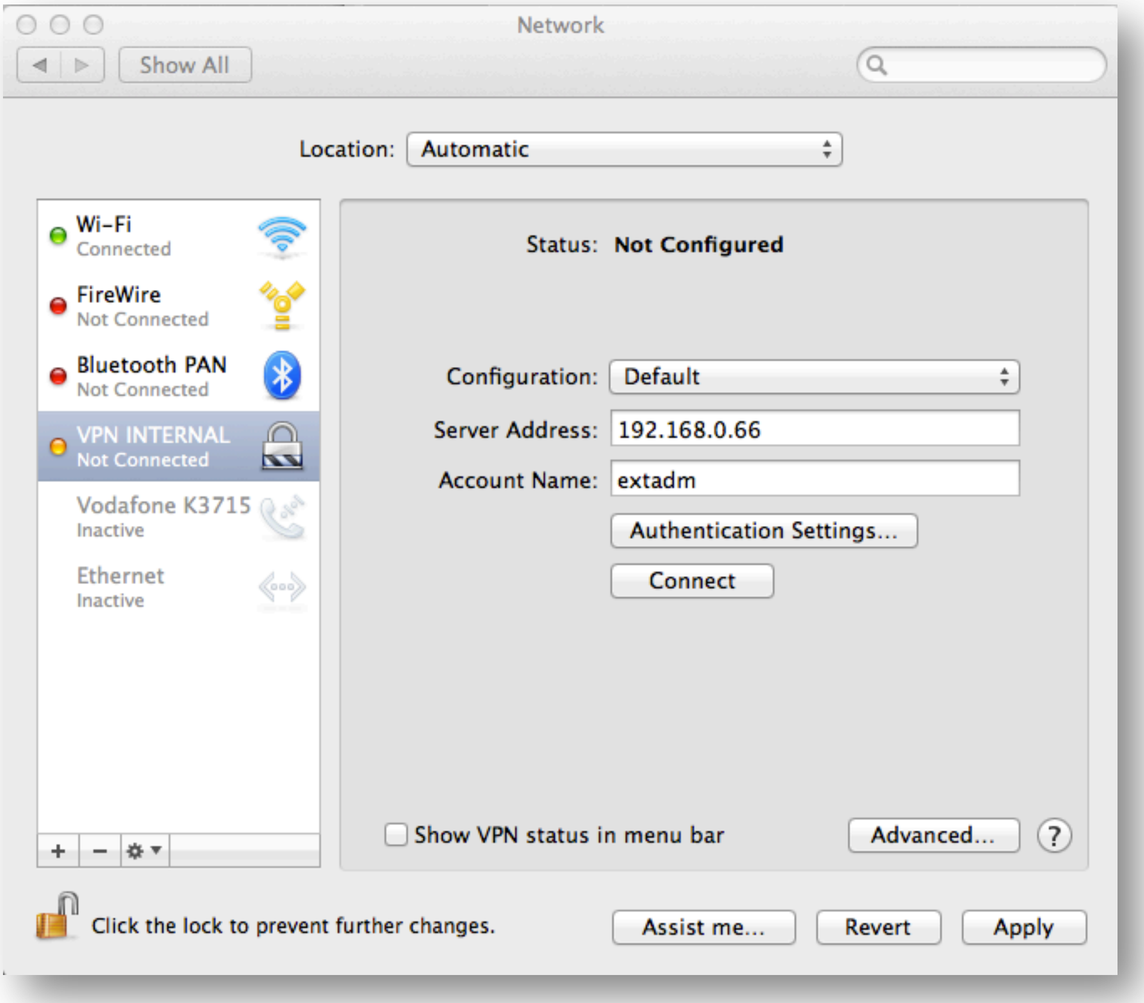
Jetzt kann auf einem Client (hier ein MAC OS X Lion) eine VPN Verbindung eingerichtet werden:


Select the interface and enter a name for the new service.

Interface: VPN

VPN Type: L2TP over IPSec

Service Name: VPN INTERNAL



Location: Automatic

Wi-Fi
Connected

FireWire
Not Connected

Bluetooth PAN
Not Connected

VPN INTERNAL
Not Connected

Vodafone K3715
Inactive

Ethernet
Inactive

Status: **Not Configured**

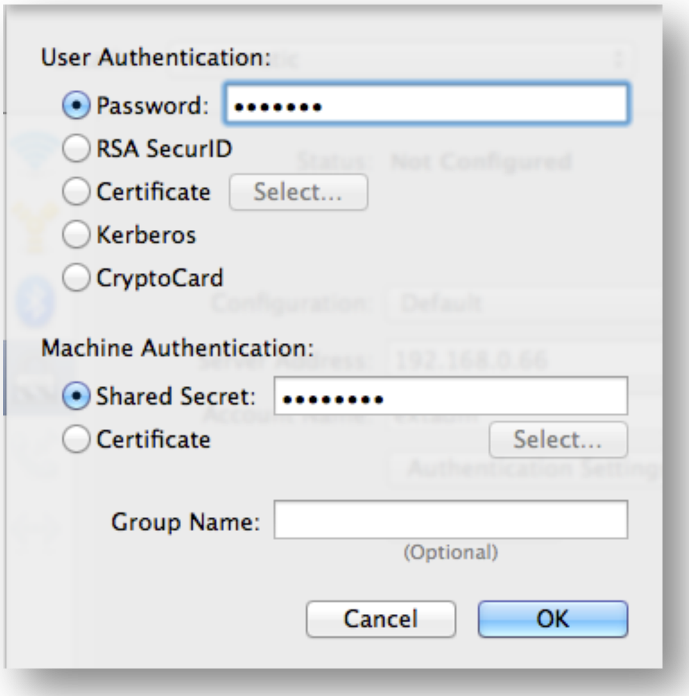
Configuration: Default

Server Address: 192.168.0.66

Account Name: extadm

□ Show VPN status in menu bar

Click the lock to prevent further changes.



User Authentication:

● Password: •••••••

○ RSA SecurID

○ Certificate

○ Kerberos

○ CryptoCard

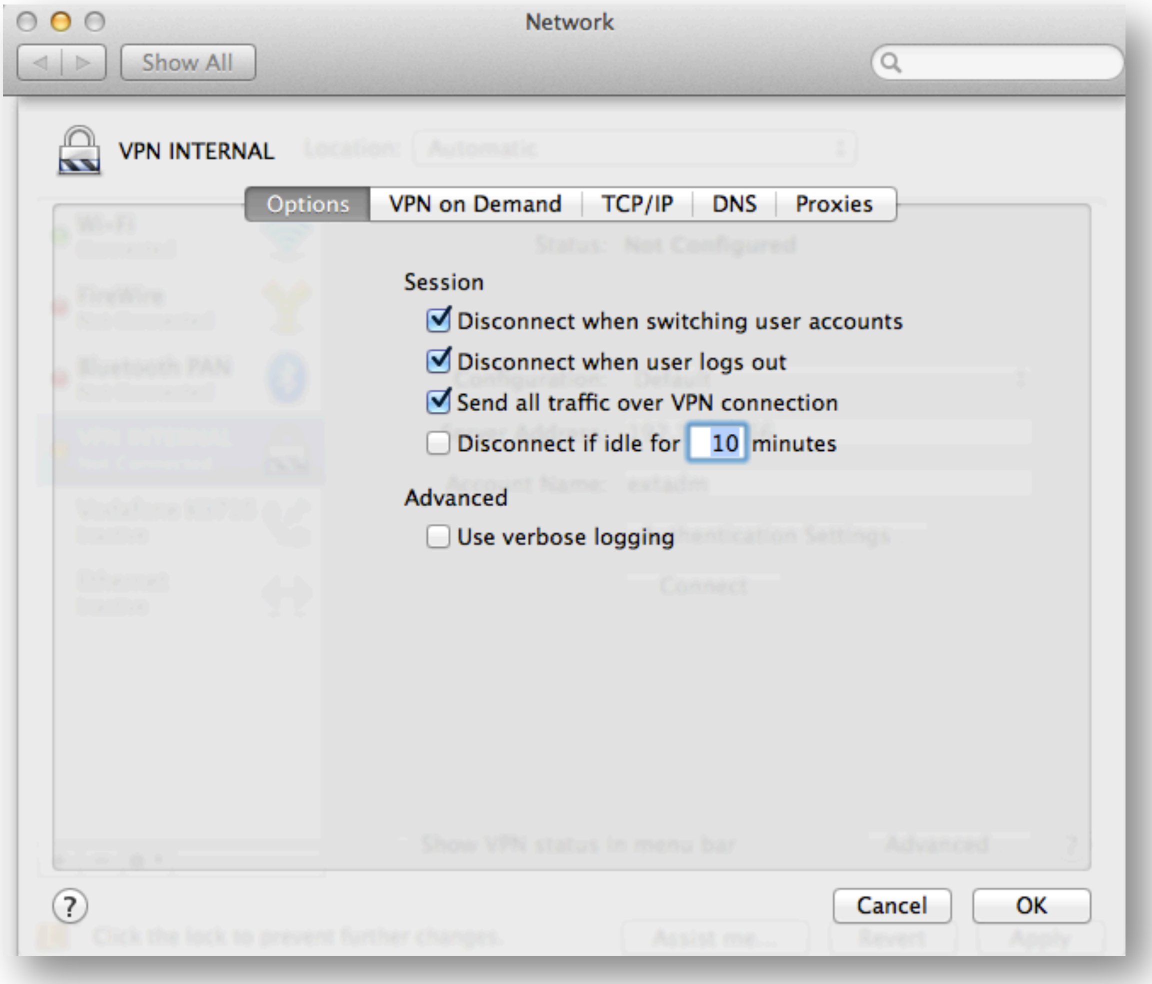
Machine Authentication:

● Shared Secret: •••••••••

○ Certificate

Group Name:

(Optional)



Session

☑ Disconnect when switching user accounts

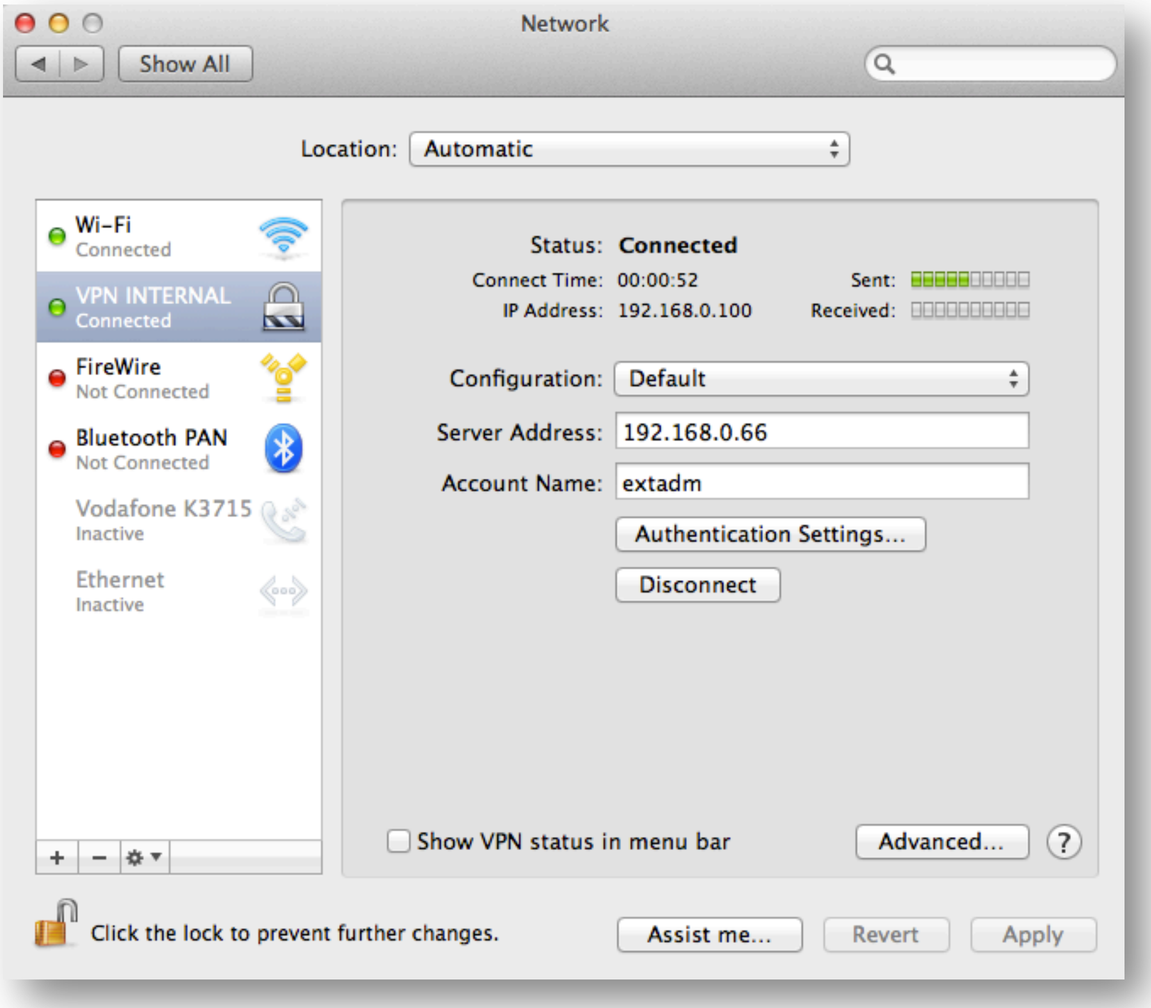
☑ Disconnect when user logs out

☑ Send all traffic over VPN connection

☐ Disconnect if idle for 10 minutes

Advanced

☐ Use verbose logging



Network

Location: Automatic

Wi-Fi
Connected

VPN INTERNAL
Connected

FireWire
Not Connected

Bluetooth PAN
Not Connected

Vodafone K3715
Inactive

Ethernet
Inactive

Status: **Connected**

Connect Time: 00:00:52

IP Address: 192.168.0.100

Sent:

Received:

Configuration: Default

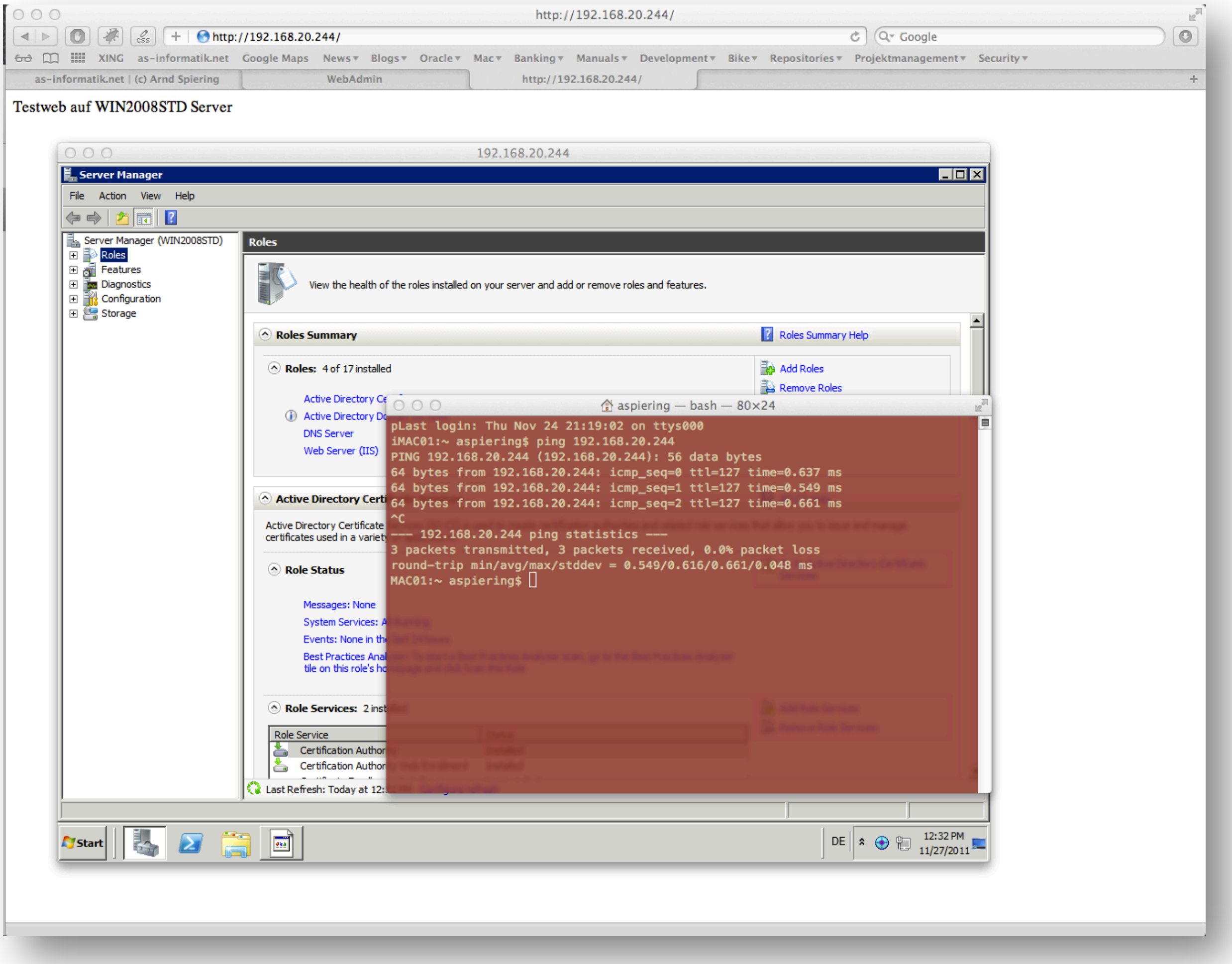
Server Address: 192.168.0.66

Account Name: extadm

□ Show VPN status in menu bar

Click the lock to prevent further changes.

Zugriffe über VPN



http://192.168.20.244/

Testweb auf WIN2008STD Server

Server Manager

View the health of the roles installed on your server and add or remove roles and features.

Roles: 4 of 17 installed

```
pLast login: Thu Nov 24 21:19:02 on ttys000
iMAC01:~ aspiering$ ping 192.168.20.244
PING 192.168.20.244 (192.168.20.244): 56 data bytes
64 bytes from 192.168.20.244: icmp_seq=0 ttl=127 time=0.637 ms
64 bytes from 192.168.20.244: icmp_seq=1 ttl=127 time=0.549 ms
64 bytes from 192.168.20.244: icmp_seq=2 ttl=127 time=0.661 ms
^C
--- 192.168.20.244 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.549/0.616/0.661/0.048 ms
MAC01:~ aspiering$ 
```

Nach der Verbindung stehen jetzt alle internen Ressourcen über VPN aus dem externen Netz zur Verfügung.

HINWEIS: Die Firewall ist nach einem Nessus Scan immer noch in dem Zustand, dass nur HTTP Zugriff auf das interne Netz geöffnet sind.

Die neue Portfreigabe wird nur für den angemeldeten Benutzer extadm geöffnet.