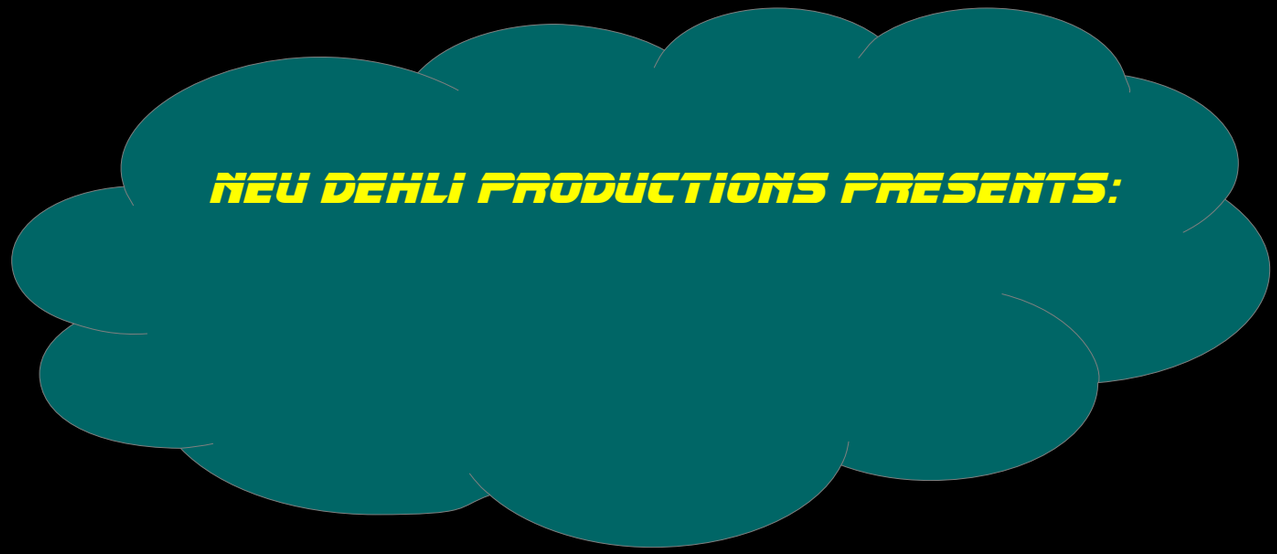
„Kommunikationssicherheit im Feindterritorium“

VPN mit SSH

Ein Vortrag im Rahmen des

Sicherheitsabends 2020.9

„Kommunikationssicherheit im Feindterritorium“



„Kommunikationssicherheit im Feindterritorium“

„Kommunikationssicherheit im Feindterritorium“

Das Internet ist voll von …

„Kommunikationssicherheit im Feindterritorium“

Das Internet ist voll von … Leuten

„Kommunikationssicherheit im Feindterritorium“

Gangster Icons - © Free Icons Library

„Kommunikationssicherheit im Feindterritorium“

Leuten wie diesen ;)

Gangster Icons - © Free Icons Library

„Kommunikationssicherheit im Feindterritorium“

Leuten wie diesen ;)

Gangster Icons - © Free Icons Library

„Kommunikationssicherheit im Feindterritorium“

Leuten wie diesen ;)

Gangster Icons - © Free Icons Library

„Kommunikationssicherheit im Feindterritorium“

Gegen diese Leute brauchen wir

„Kommunikationssicherheit im Feindterritorium“

Einen Linux PC mit ROOT-Rechten!

„Kommunikationssicherheit im Feindterritorium“

Einen Linux-Server im Internet mit Root-Zugang

„Kommunikationssicherheit im Feindterritorium“

Einen SSH Server auf dem Server

„Kommunikationssicherheit im Feindterritorium“

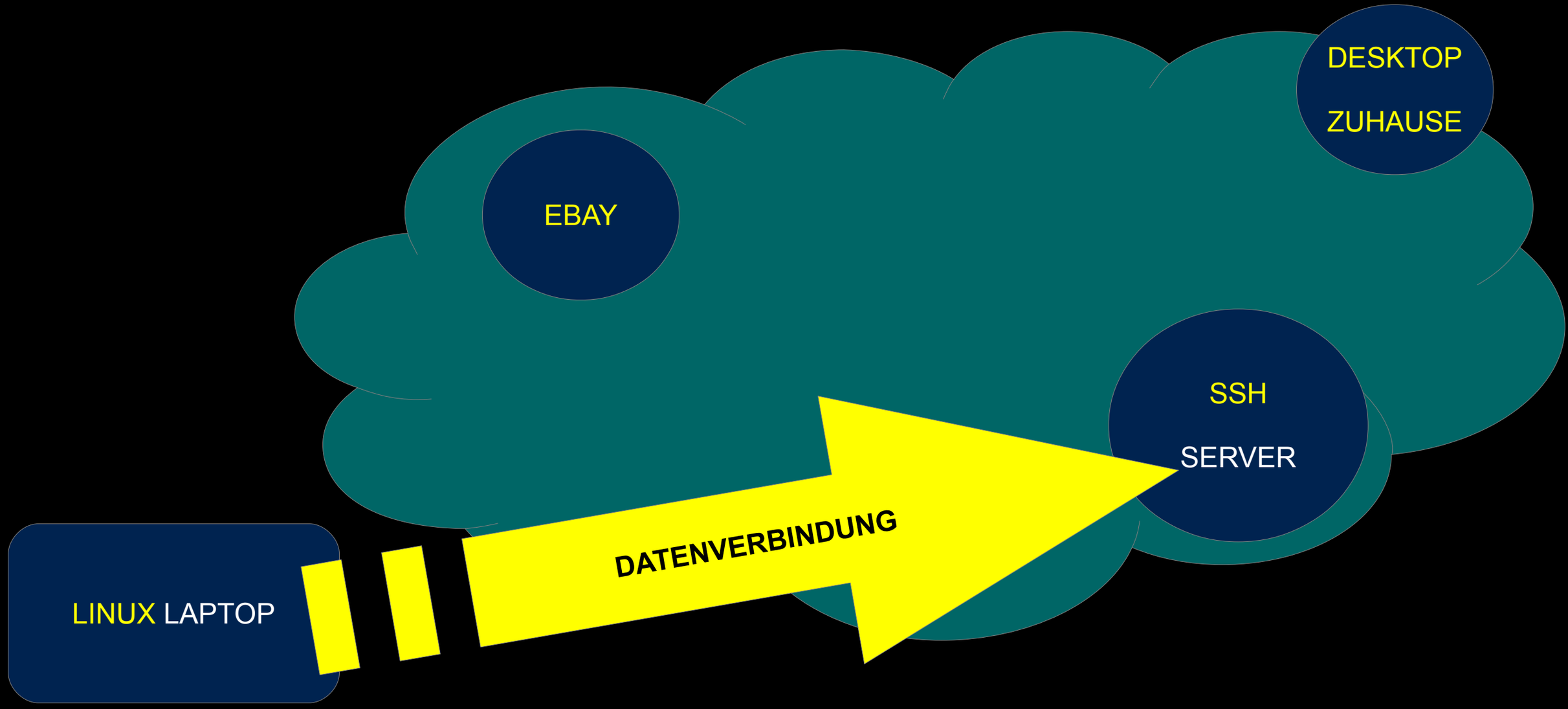
Was wir machen wollen

„Kommunikationssicherheit im Feindterritorium“

Wir bauen ein

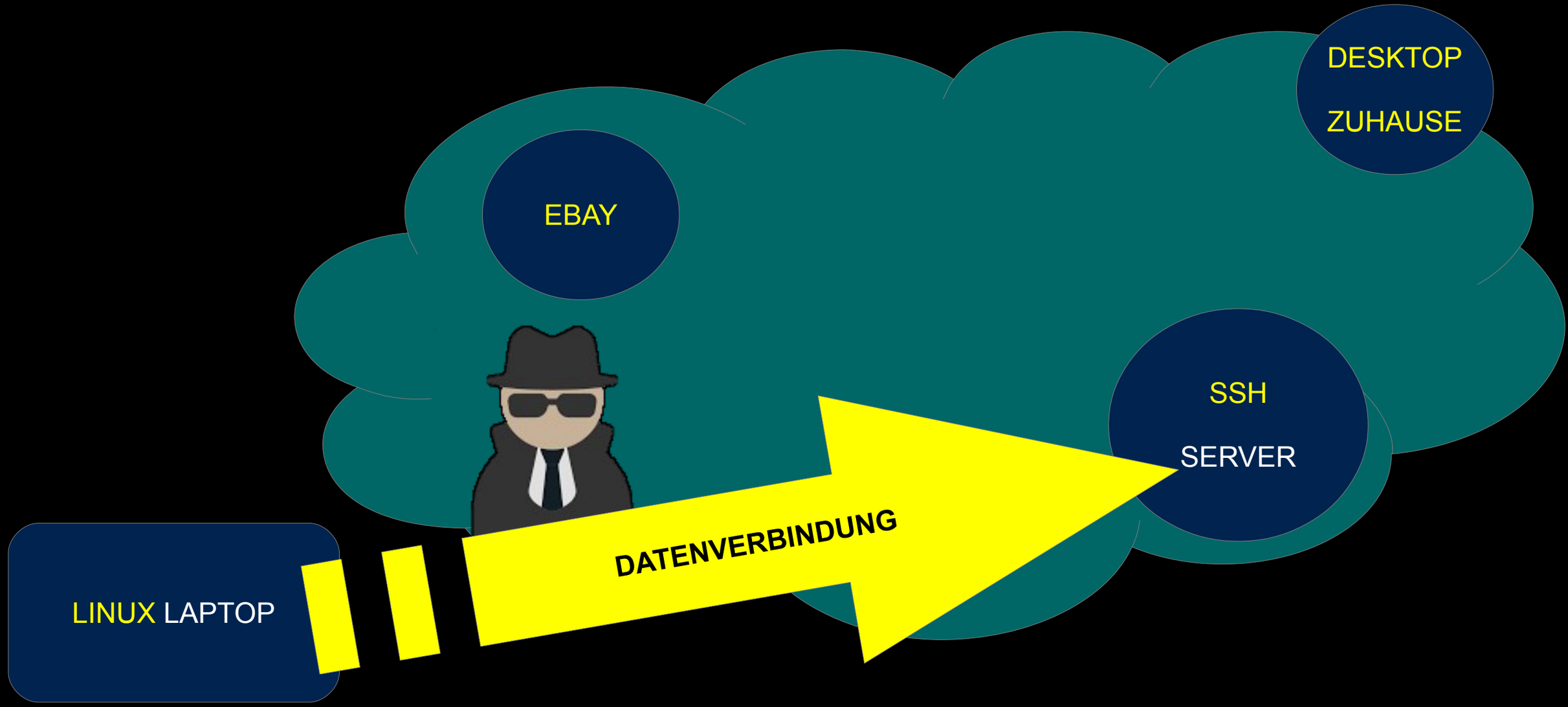
SSH - Virtual Private Network

„Kommunikationssicherheit im Feindterritorium“



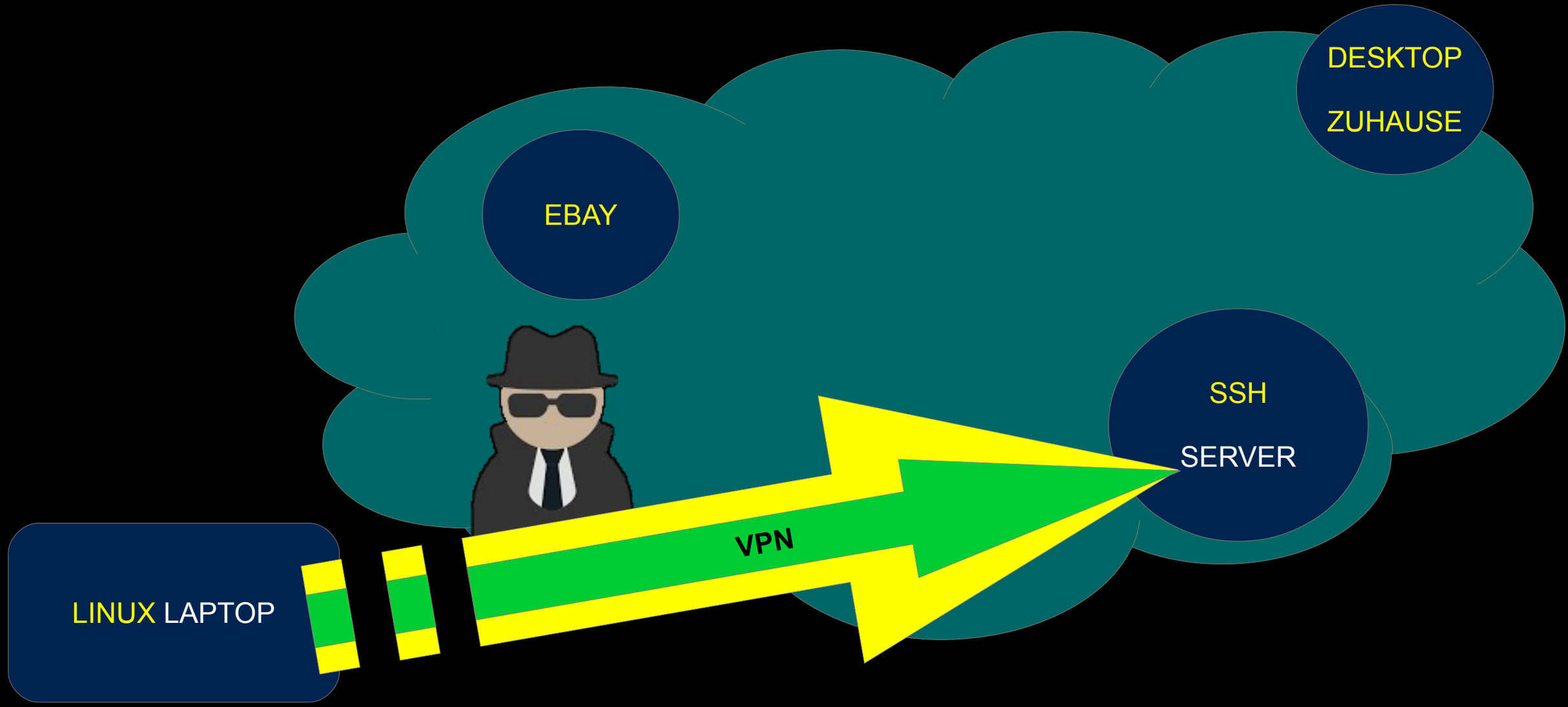
Gangster Icons - © Free Icons Library

„Kommunikationssicherheit im Feindterritorium“



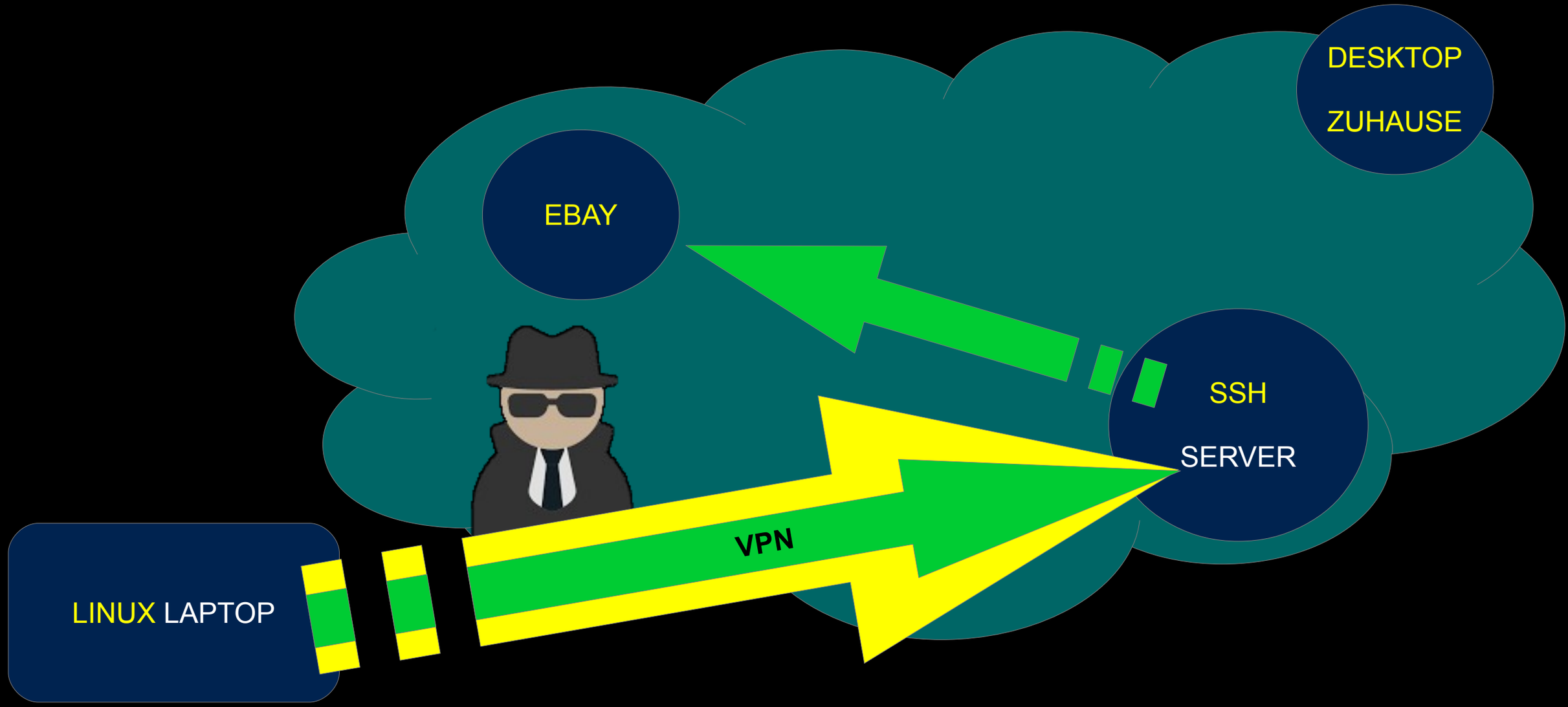
Gangster Icons - © Free Icons Library

„Kommunikationssicherheit im Feindterritorium“



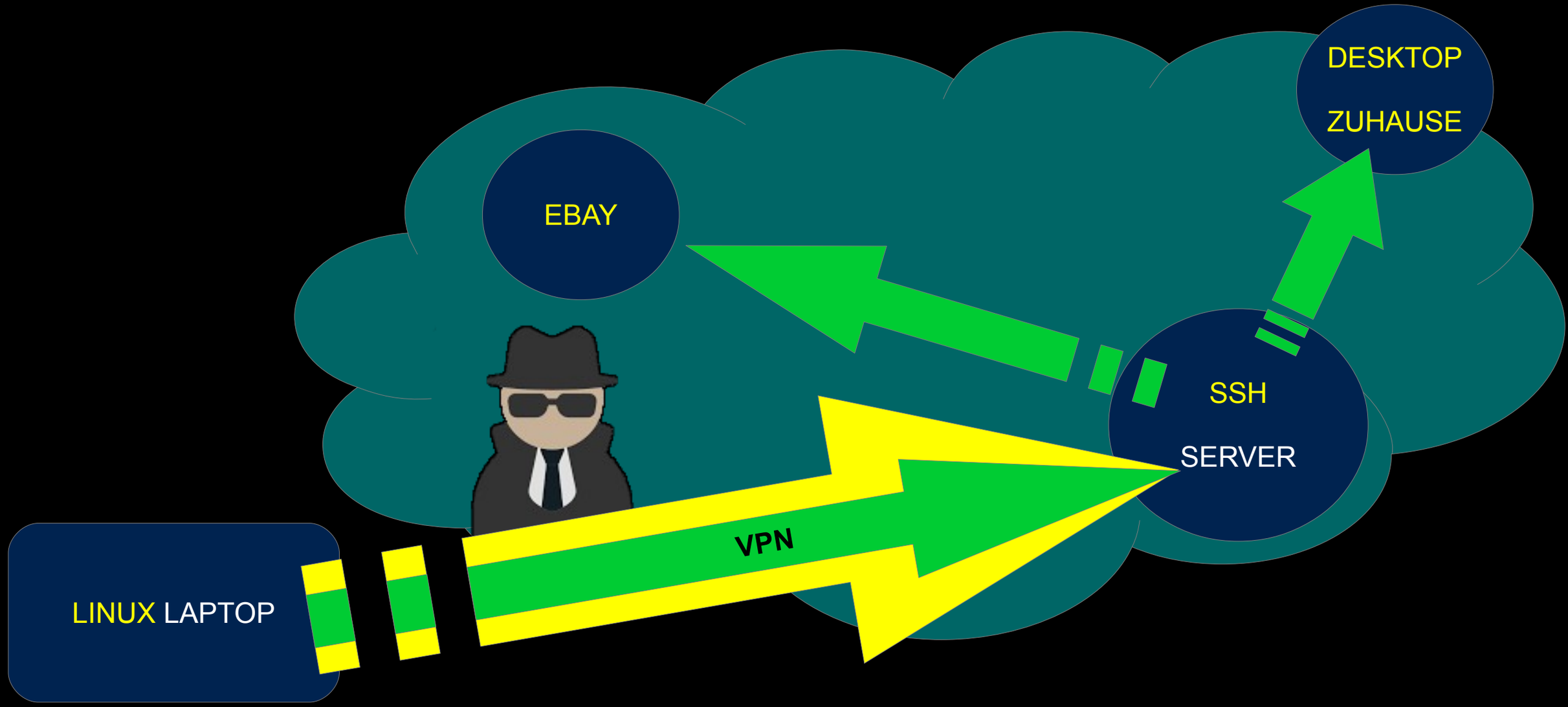
Gangster Icons - © Free Icons Library

„Kommunikationssicherheit im Feindterritorium“



Gangster Icons - © Free Icons Library

„Kommunikationssicherheit im Feindterritorium“



Gangster Icons - © Free Icons Library

„Kommunikationssicherheit im Feindterritorium“

SSH SERVER SETUP

„Kommunikationssicherheit im Feindterritorium“

/etc/ssh/sshd_config muß enthalten:

GatewayPorts clientspecified
PermitTunnel yes

„Kommunikationssicherheit im Feindterritorium“

Schritt 1 – Tunnel etablieren

„Kommunikationssicherheit im Feindterritorium“

```
ssh -NTCf -w 0:0 root@ssh.server.de
```

„Kommunikationssicherheit im Feindterritorium“

Schritt 2 – SERVERINTERFACE hochfahren

„Kommunikationssicherheit im Feindterritorium“

alles als root User machen

```
modprobe tun

ip link set tun0 up

ip addr add 10.0.1.1/32 peer 10.0.1.2 dev tun0

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

„Kommunikationssicherheit im Feindterritorium“

Schritt 3 – VPN PC – INTERFACE - hochfahren

„Kommunikationssicherheit im Feindterritorium“

als root User auf dem PC starten

```
echo "1" >/proc/sys/net/ipv6/conf/all/disable_ipv6
modprobe tun
ip link set tun0 up
ip addr add 10.0.1.2/32 peer 10.0.1.1 dev tun0
route add ssh.server.de gw 192.168.178.1
route del default gw 192.168.178.1
route add default gw 10.0.1.1 dev tun0
```

„Kommunikationssicherheit im Feindterritorium“

DAS WARS SCHON

„Kommunikationssicherheit im Feindterritorium“

HABEN DAS JETZT ALLE VERSTANDEN?!!

„Kommunikationssicherheit im Feindterritorium“

NA GUT... OK

„Kommunikationssicherheit im Feindterritorium“

Das TUNNEL Modul des Kernel laden

modprobe tun

Ein Netzwerkinterface für den Tunnel hochfahren

ip link set tun0 up

Dem Tunnelinterface die passende IP geben

ip addr add 10.0.1.1/32 peer 10.0.1.2 dev tun0

„Kommunikationssicherheit im Feindterritorium“

Dem Server sagen, daß er Pakete von einem Interface (eth0)
zum Anderen (tun0) verschieben darf. Das macht er normalerweise nicht.

echo 1 > /proc/sys/net/ipv4/ip_forward

Dem Kernel sagen, er soll die LAN IP Adresse an die vom Server anpassen (NAT)

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

„Kommunikationssicherheit im Feindterritorium“

Abschalten von IPV6

```
echo "1" >/proc/sys/net/ipv6/conf/all/disable_ipv6
```

„Kommunikationssicherheit im Feindterritorium“

Das TUNNEL Modul des Kernel laden

modprobe tun

Das Netzwerkinterface hochfahren

ip link set tun0 up

Dem Netzwerkinterface die passende IP geben

ip addr add 10.0.1.2/32 peer 10.0.1.1 dev tun0

„Kommunikationssicherheit im Feindterritorium“

Eine Route zum SSH Server setzen, damit er nicht durch sein eigenes Interface gehen muß, was nicht funktionieren würde:

route add ssh.server.de gw 192.168.178.1;

Die alte „da müssen alle Pakete lang“ Gateway entfernen:

route del default gw 192.168.178.1;

Die neue „da müssen alle Pakete lang“ Gateway auf den Tunnel setzen:

route add default gw 10.0.1.1 dev tun0;

„Kommunikationssicherheit im Feindterritorium“

OK, DAS wars jetzt aber ….

„Kommunikationssicherheit im Feindterritorium“

OK, DAS wars jetzt aber …. oder?

„Kommunikationssicherheit im Feindterritorium“

Der PC wird jetzt durch den TUNNEL,

der von SSH verschlüsselt wurde,

alle Anfrage ins Internet erst an den SSH Server senden,

von dort gehen diese dann ans Ziel.

„Kommunikationssicherheit im Feindterritorium“

Dank NAT (Network Adress Translation) werden die Datenpakete des Clienten so umgeschrieben, daß Sie am Ende mit der IP vom Server gesendet werden.

Der Server merkt sich welche LAN IP welche Verbindung aufgebaut hat, und baut die Pakete auf dem Rückweg (Antwort) wieder korrekt zurück.

Weder der LAN PC noch der ZIEL-Server merken etwas davon!

„Kommunikationssicherheit im Feindterritorium“

Da es sich um ein natives Netzwerkinterface (TUN0) handelt,

merkt keine der Anwendungen etwas davon, denn denen ist es egal,

wo die Daten im Netz entlang wandern, solange diese am Ziel ankommen.

„Kommunikationssicherheit im Feindterritorium“

Das bedeutet auch,

daß PING(ICMP) und Videokonferenzen (UDP) nicht anders

als TCP behandelt werden müssen.