SSL Identifier

Keeping Your Lines of Communication Open and Secure

Aidan Gogarty

HOB Inc

Session ID: SPO1-302

Session Classification: General Interest

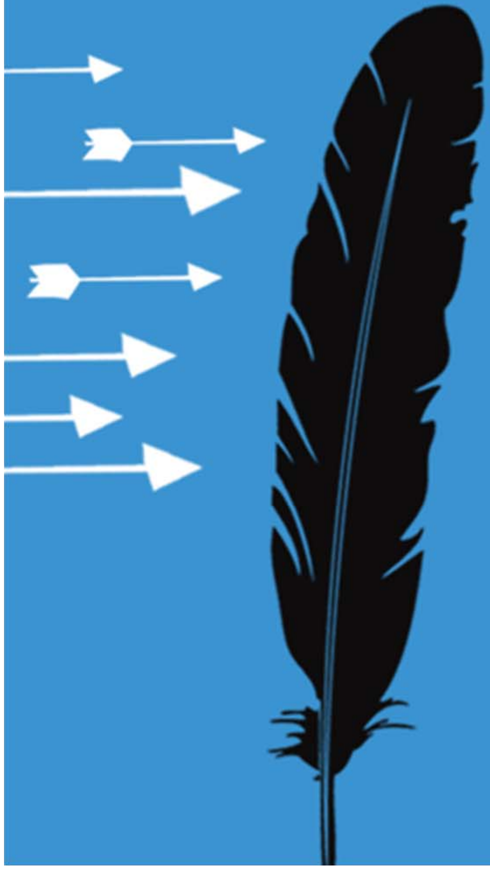
RSACONFERENCE2012

SSL Identifier

- Introduction – What is SSL?
  - Characteristics and drawbacks

- What is the SSL Identifier?
  - How it works
  - Generating Headers
  - The SSL Identifier with MS Windows
  - Users with multiple IP addresses

- Conclusion – How the SSL Identifier can be used

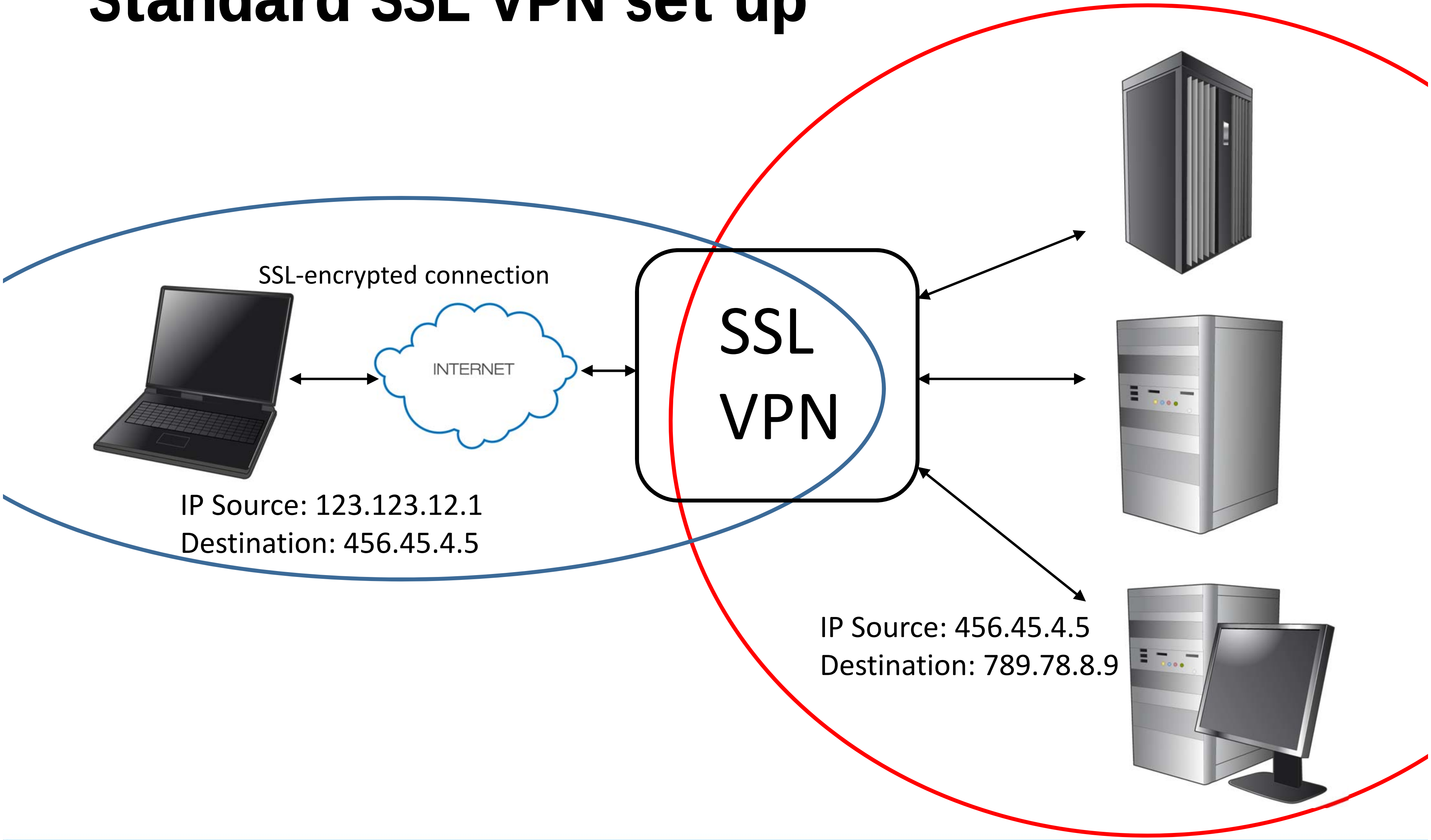


Introduction - What is SSL?

What is SSL?

- Industry standard security protocol for message transmission
- Application layer protocol
- Based on exchange of certificates with known source and destination machines

Standard SSL VPN set up



SSL-encrypted connection

SSL
VPN

IP Source: 123.123.12.1
Destination: 456.45.4.5

IP Source: 456.45.4.5
Destination: 789.78.8.9

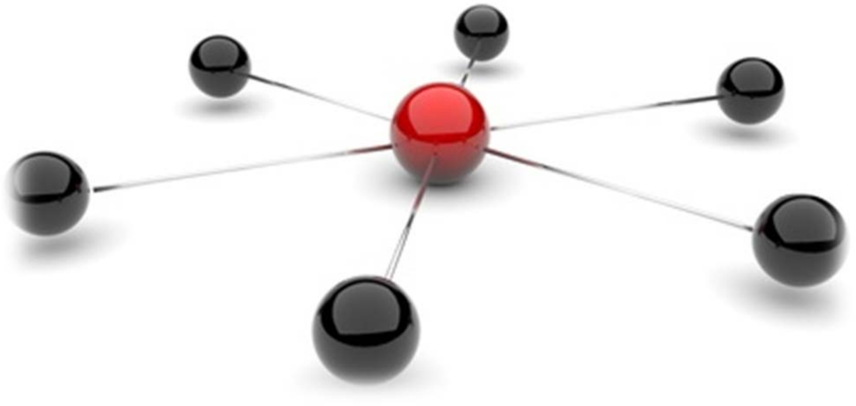
Who talks to whom?

Client IP Address (Source):	123.123.12.1
SSL VPN IP (Destination):	456.456.4.5

SSL VPN IP (Source):	456.456.4.5
Internal LAN IP (Destination):	789.78.8.9

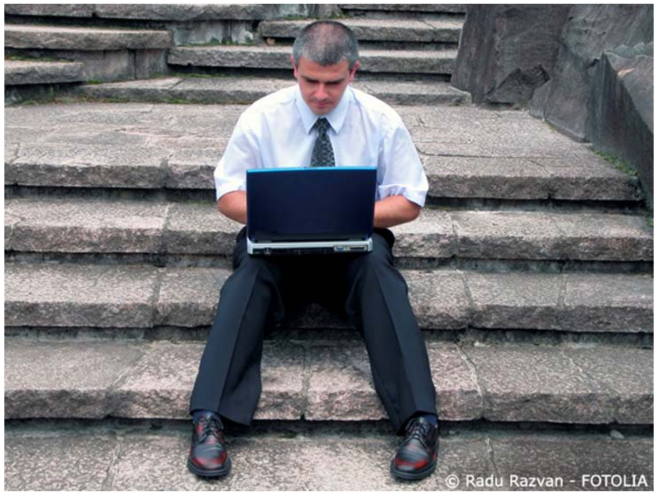
Drawbacks of a standard SSL VPN network - 1

- You have no way to match LAN internal traffic to the client or user sending it, as all data are sent from the SSL VPN into the LAN



Drawbacks of a standard SSL VPN network - 2

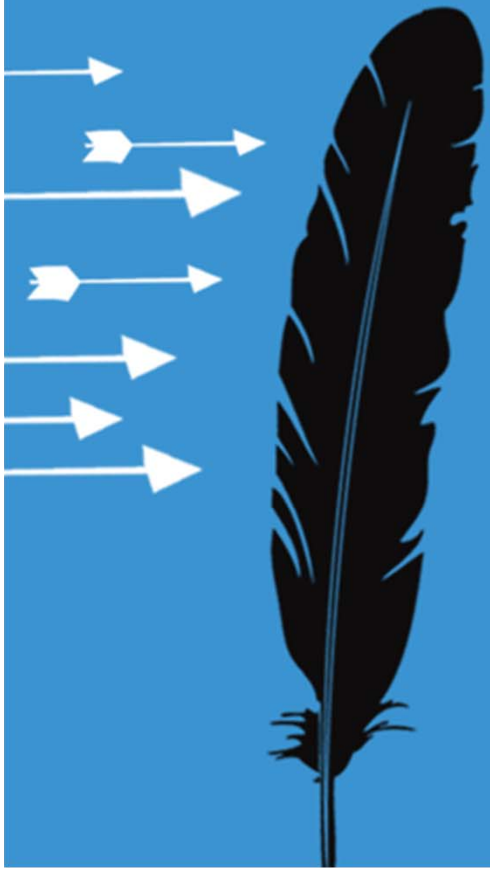
- Anonymous network traffic
  - All traffic goes through the VPN, can never be sure where any data comes from
  - Can never be sure if data goes to intended target



© Radu Razvan - FOTOLIA

Drawbacks of a standard SSL VPN network - 3

- A valid client IP address is needed for many LAN-based applications
  - Monitoring of software licenses
  - Allocating costs

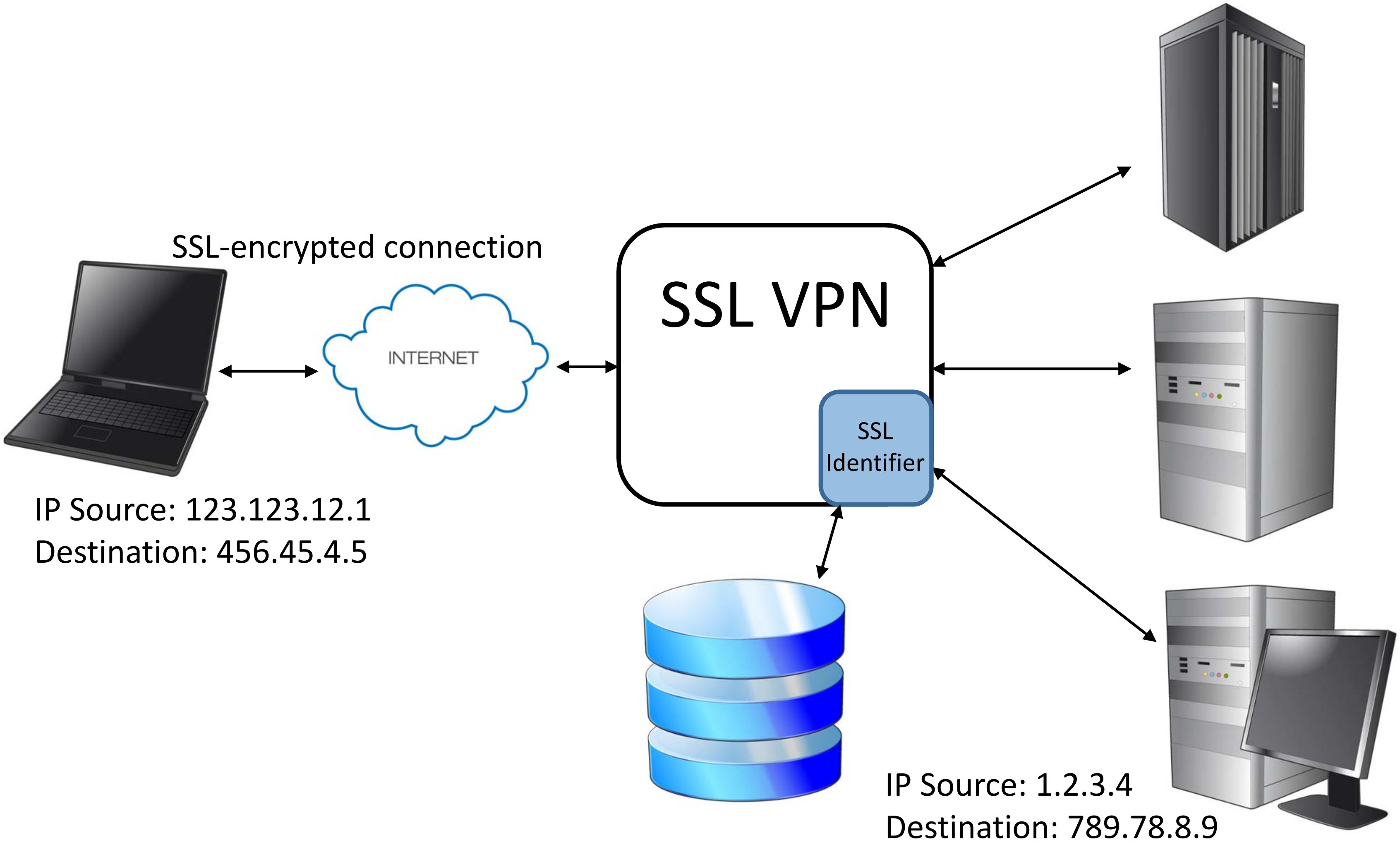


What IS the SSL Identifier?

What is an SSL Identifier?

- Optional feature for an SSL VPN
- The SSL Identifier assigns an individual and specific identifying address to all incoming traffic based on the user’s identity
- Each SSL Identifier address is assigned from a database
- This SSL Identifier address is sent with all traffic from this user into the LAN

How the SSL Identifier works



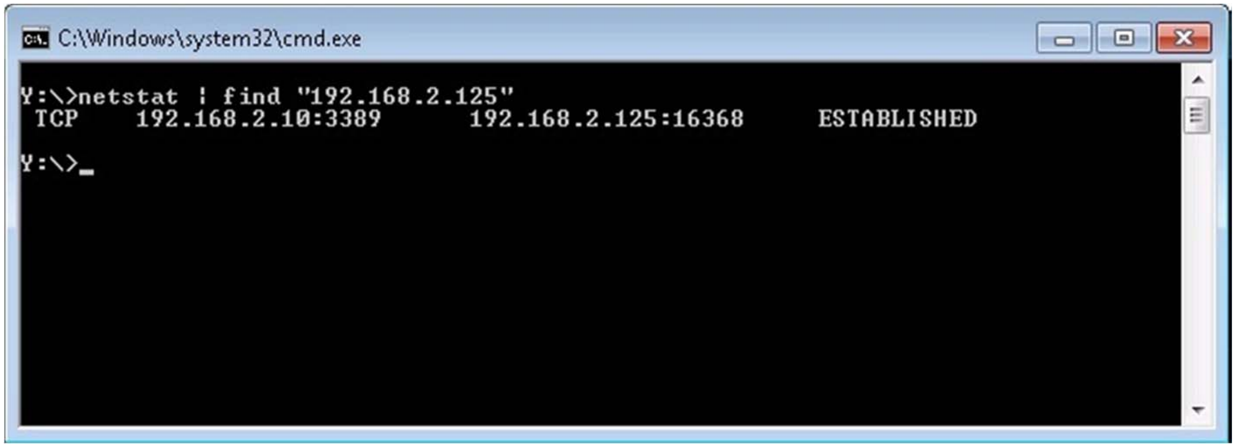
Assigning SSL Identifier addresses

- Original message:
  - Source IP: 123.123.12.1
  - Destination IP: 456.45.4.5 (SSL VPN)

- SSL Identifier:
  - User: JohnSmith = 1.2.3.4
  - By name assignment

- New address for the message:
  - Source IP: 1.2.3.4
  - Destination IP: 789.78.8.9

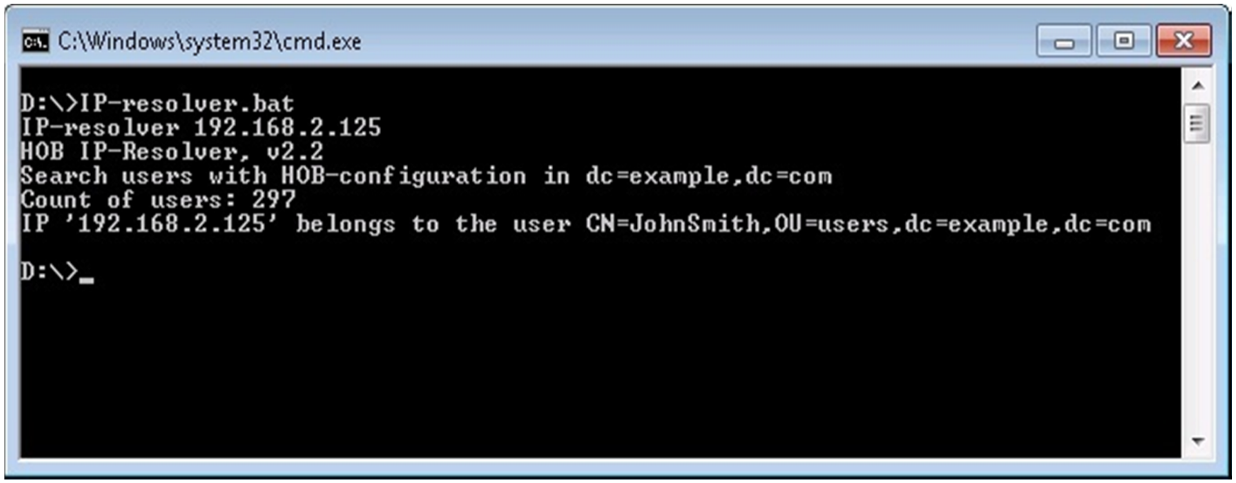
Tracing the users



```
Y:\>netstat | find "192.168.2.125"
  TCP    192.168.2.10:3389      192.168.2.125:16368     ESTABLISHED

Y:\>_
```

- Identify the connection in use
  - e.g. Netstat command



```
D:\>IP-resolver.bat
IP-resolver 192.168.2.125
HOB IP-Resolver, v2.2
Search users with HOB-configuration in dc=example,dc=com
Count of users: 297
IP ’192.168.2.125’ belongs to the user CN=JohnSmith,OU=users,dc=example,dc=com

D:\>_
```

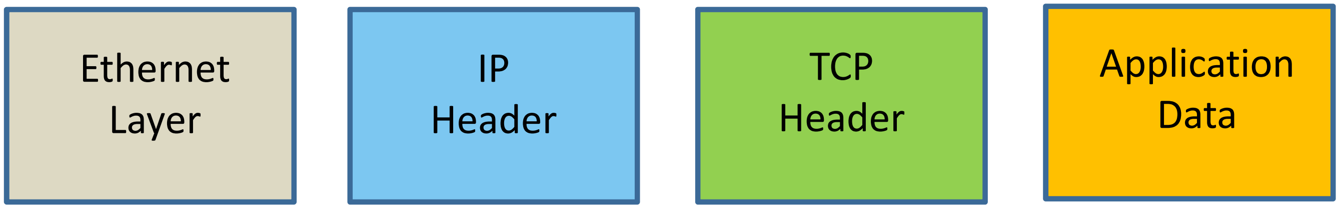
- Identify who is using this connection
  - e.g. Search database command

A bit more detail

- The SSL Identifier assigns a pre-defined Virtual IP address for each user
- The Source IP address is replaced for all internal communication
- The Virtual IP address assigned by the SSL Identifier is used for each individual user
- This Virtual IP address is used to identify the user for ALL connections (even if simultaneous)

About Headers

- TCP/IP headers are normally created automatically by the operating system of the source machine



Ethernet Layer

IP Header

TCP Header

Application Data

- New TCP/IP headers must be generated by the SSL Identifier

Components of the SSL Identifier

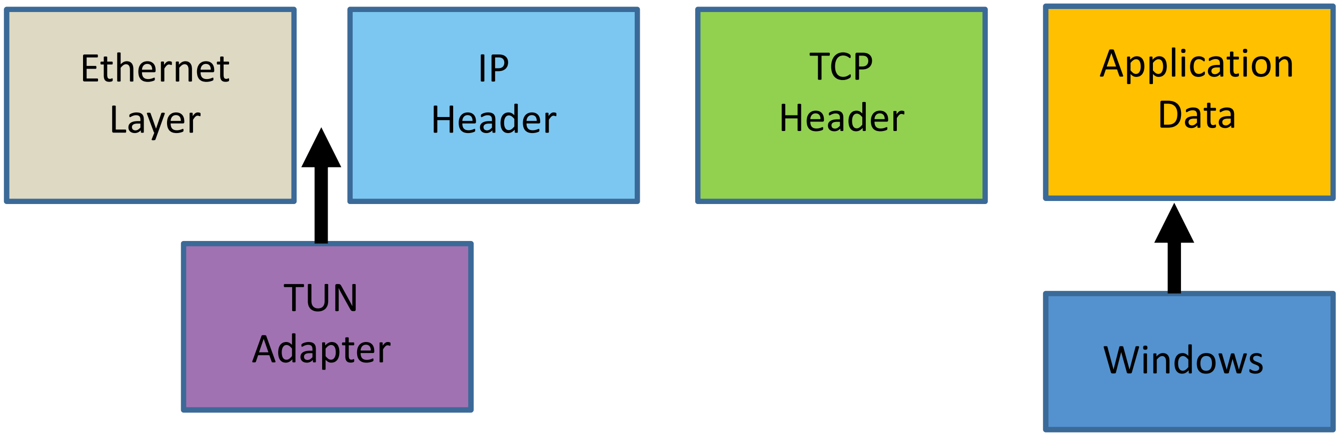
- Userspace TCP Stack
  - Generates new TCP/IP headers

- TUN Adapter
  - Inserts new TCP/IP headers into the message

Also required is a database for storing Usernames and Passwords

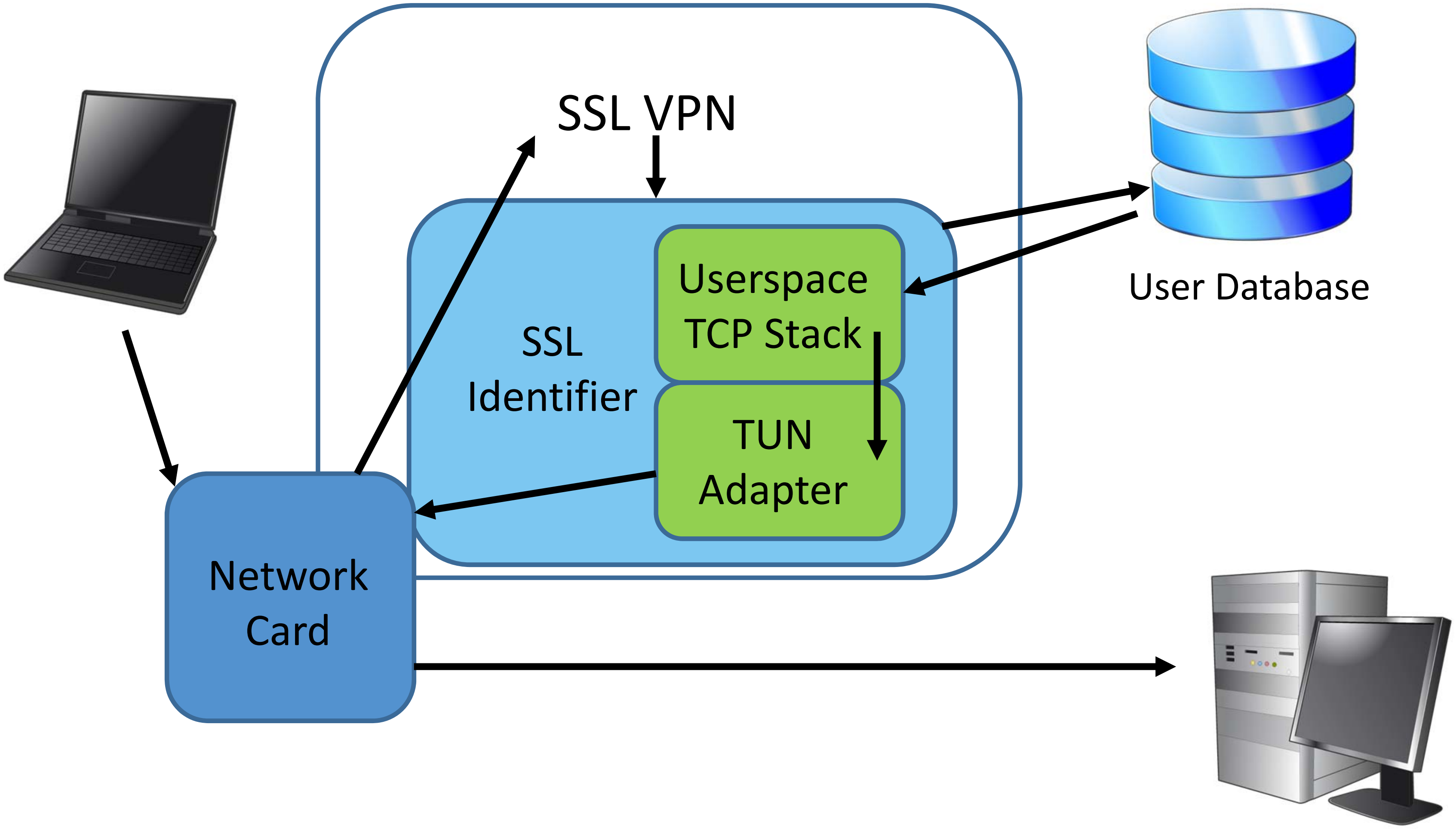
The situation with Windows

- Windows does not allow self-created TCP/IP packets to be sent – they can only be modified in the User Space of your machine



- Using a TUN Adapter allows the IP and TCP headers to be replaced

The TCP/IP Header generation process



What does the Userspace TCP Stack do?

- Receives the SSL Identifier address for each user from the user data base

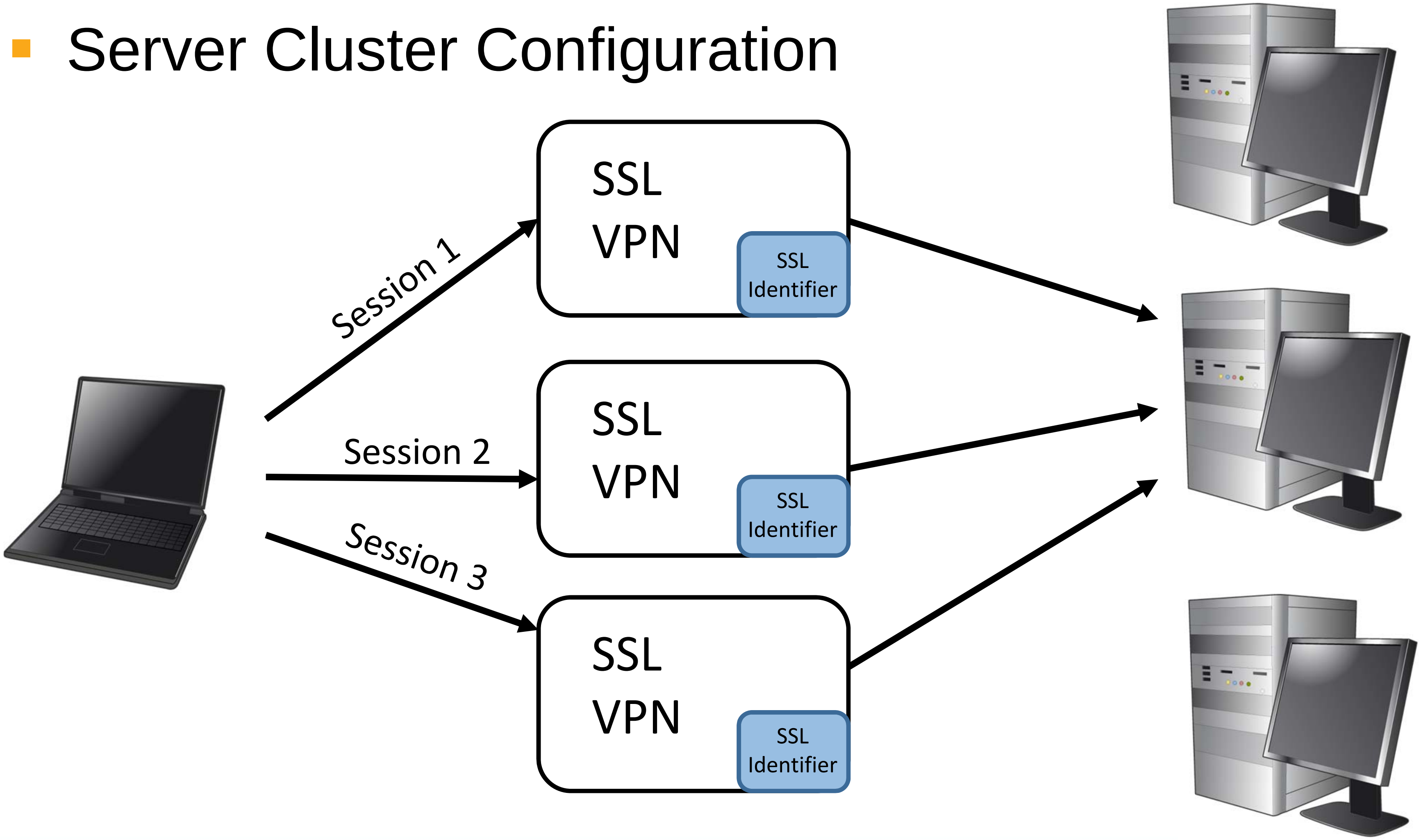
- Generates a set of TCP and IP headers that can be added to any message being sent

What does the TUN Adapter do?

- TUN is a virtual network kernel device used for routing IP Packets
- The TUN adapter allows self-generated IP and TCP headers to be added
- Automatically creates TCP/IP headers when using the TUN protocol

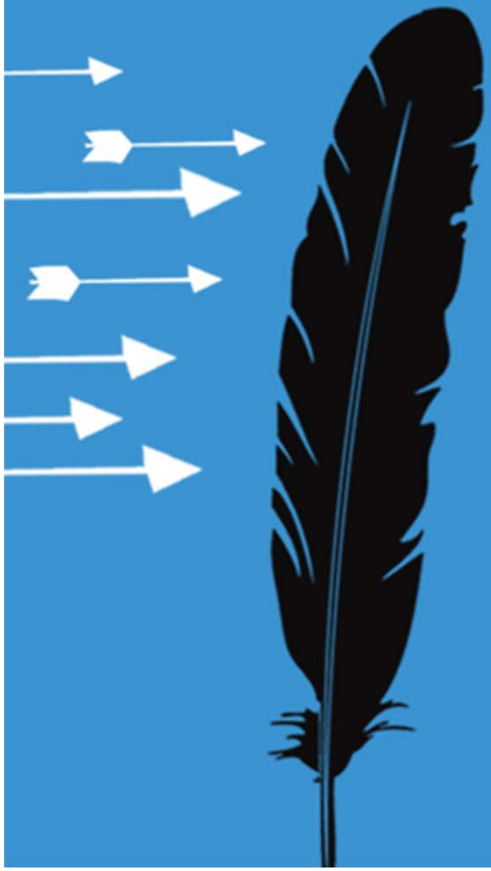
A user with multiple Virtual IP Addresses

- Server Cluster Configuration



A user with multiple Virtual IP Addresses

- New session = new user
- New user = new SSL Identifier address
- Ensures that the origin of each communication can be clearly identified
- Also works with users on virtual machines



Conclusion - How the SSL Identifier can be used

Using the SSL Identifier

- Implement on the SSL VPN – one instance for all users and traffic
- Allow enough database space for storage of Identifier addresses for all potential users
- Usable for other gateway or proxy solutions

Thank you very much for your attention

Any questions?

Picture Credit:
Seite 8 © Radu Razvan - Fotolia.com