

SSL VPN

Virtual Private Networks based on
Secure Socket Layer

Mario Baldi

Politecnico di Torino

**Dipartimento di Automatica e
Informatica**

mario.baldi[at]polito.it

staff.polito.it/mario.baldi

Nota di Copyright

This set of transparencies, hereinafter referred to as slides, is protected by copyright laws and provisions of International Treaties. The title and copyright regarding the slides (including, but not limited to, each and every image, photography, animation, video, audio, music and text) are property of the authors specified on page 1.

The slides may be reproduced and used freely by research institutes, schools and Universities for non-profit, institutional purposes. In such cases, no authorization is requested.

Any total or partial use or reproduction (including, but not limited to, reproduction on magnetic media, computer networks, and printed reproduction) is forbidden, unless explicitly authorized by the authors by means of written license.

Information included in these slides is deemed as accurate at the date of publication. Such information is supplied for merely educational purposes and may not be used in designing systems, products, networks, etc. In any case, these slides are subject to changes without any previous notice. The authors do not assume any responsibility for the contents of these slides (including, but not limited to, accuracy, completeness, enforceability, updated-ness of information hereinafter provided).

In any case, accordance with information hereinafter included must not be declared.

In any case, this copyright notice must never be removed and must be reported even in partial uses.

SSL VPN: What is that?

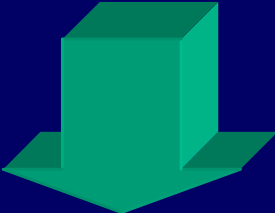
SSL as the central mechanism on which to base secure access

- **Site-to-site VPN**
- **Remote access VPN**
- **Secure service access**
 - **Loose interpretation of VPN**
 - **SSL (pseudo)VPN**
- **Tunneling based on TCP or UDP**

Why Not IPsec VPN?

- IPsec too difficult and/or too expensive to use securely
 - Too many options to be configured and administered
- Operates in kernel space
 - Failures potentially catastrophic
 - Installation difficult and risky
 - Concerns fade with maturity

Why SSL VPN

- **Lower complexity**
 - **Installation**
 - **Configuration**
 - **Management**
- **Non-interference with kernel**
- **Most widely used**
- 
- **Higher, more robust security**

Compared to IPsec VPN

- No problem with NAT traversal
 - No authentication of IP header
 - ESP (encapsulation security payload) IPsec to be used
- Packets dropped at a higher level
 - Critical with DOS attacks

Compared to PPTP

- **Initially proprietary (Microsoft)**
- **Initially weak security**
 - **Fixed later**
- **Poor interoperability with non-Microsoft platforms**
- **GRE (generic routing encapsulation) tunneling**
 - **Possibly blocked by routers**

SSL (pseudo)VPN

- IPsec VPNs connect networks
 - Or hosts to networks
- SSL VPNs connect
 - Users to services
 - Application clients to application servers

Why SSL (pseudo)VPN

- **No client code is to be installed**
 - **Usable anywhere (kiosk)**
- **Applications available through web browser**
 - **Deploying HTTPS**
- **Not a general security solution**
 - **Specific solutions suitable to selected applications**

In Summary

SSL VPNs have a good chance of working on any network scenario

→ TCP or UDP tunneling enable


→ NAT traversal

→ Firewall traversal

→ Router traversal

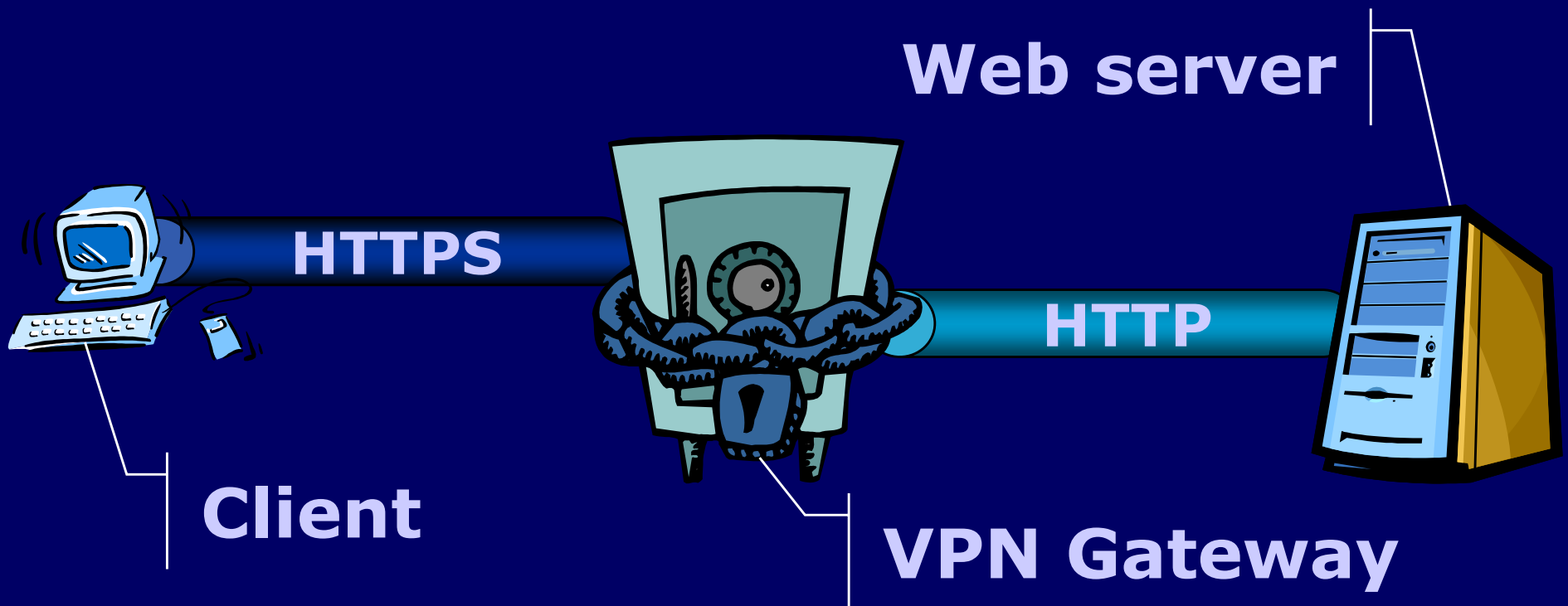
**→ SSL (pseudo)VPN enable
universal client (web browser)**

SSL VPN Flavors

- Web proxying
 - Application translation
 - Port forwarding
 - SSL'ed protocols
 - Application proxying
 - Network extension
 - Site-to-site connectivity
- 
- Pseudo VPN**

Proxying

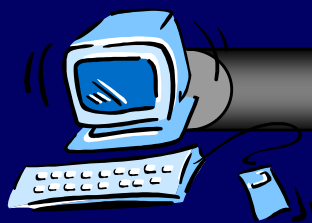
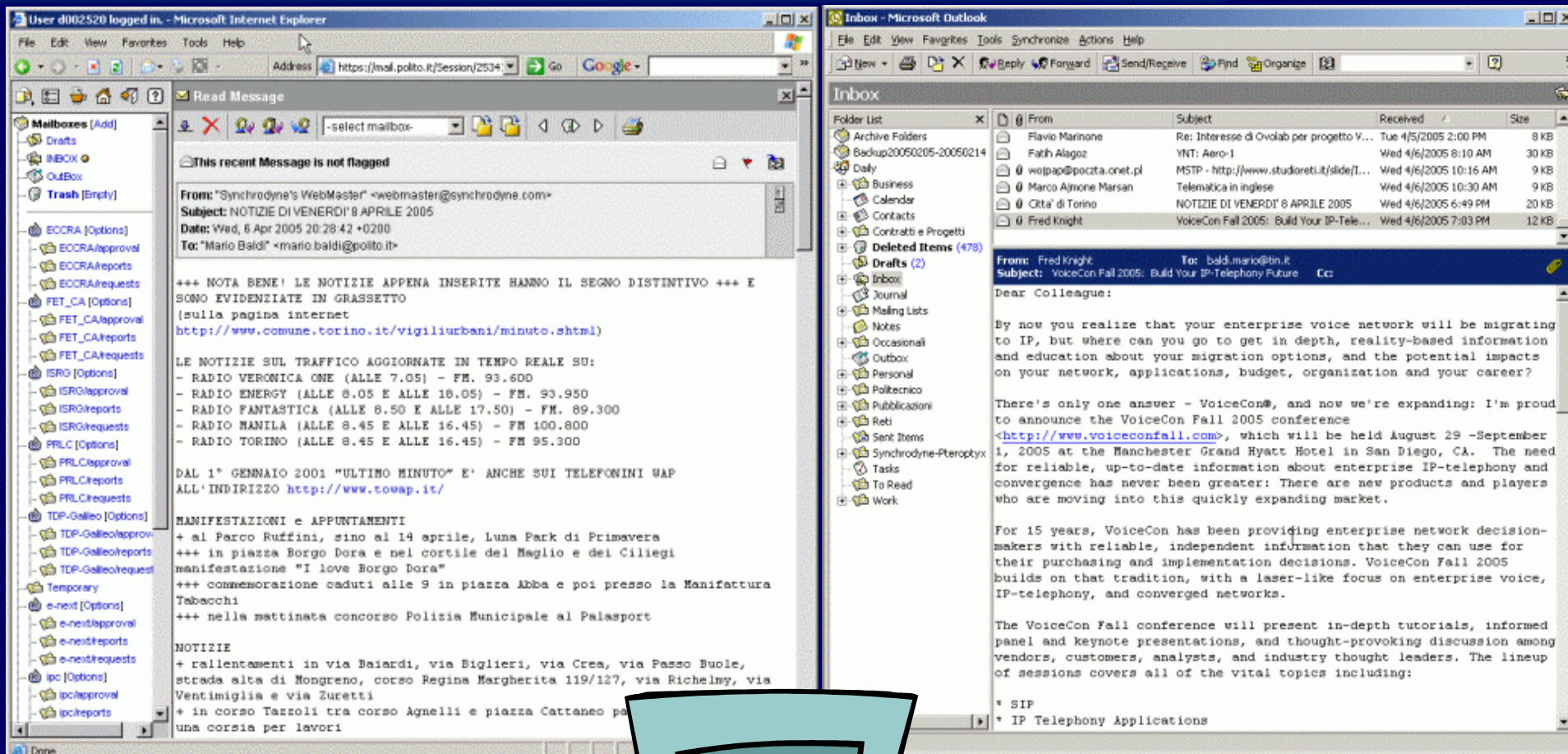
- VPN Gateway downloads web pages through HTTP
- Ship them through HTTPS



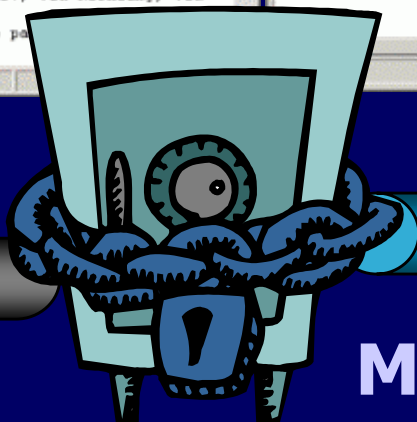
Application Translation

- Native protocol between VPN server and application server
 - E.g., FTP, STMP, POP
- Application user interface as a web page
- HTTP(S) between VPN server and client
- Not suitable for all applications
 - Look&feel might be lost

Application Translation

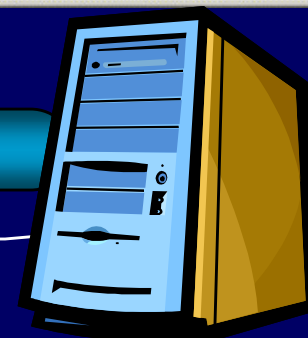


HTTPS



POP3

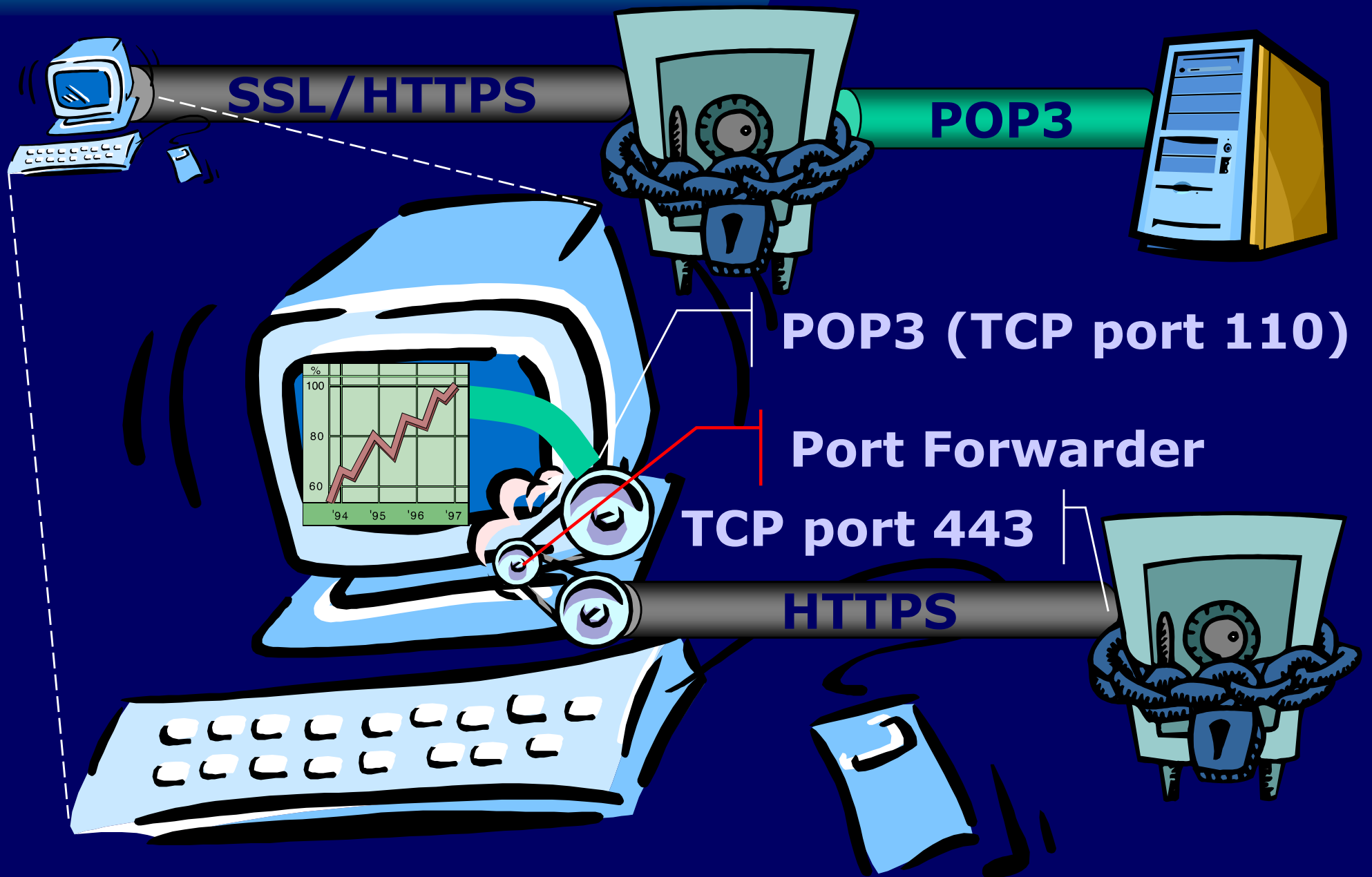
Mail server



Port Forwarding

- **Port forwarder on client**
 - **Additional software**
 - **Platform dependent**
 - **Unless Java or ActiveX**
- **Application points to localhost**
 - **To port X**
 - **Usual application port**
 - **E.g., TCP port 110 (POP3)**

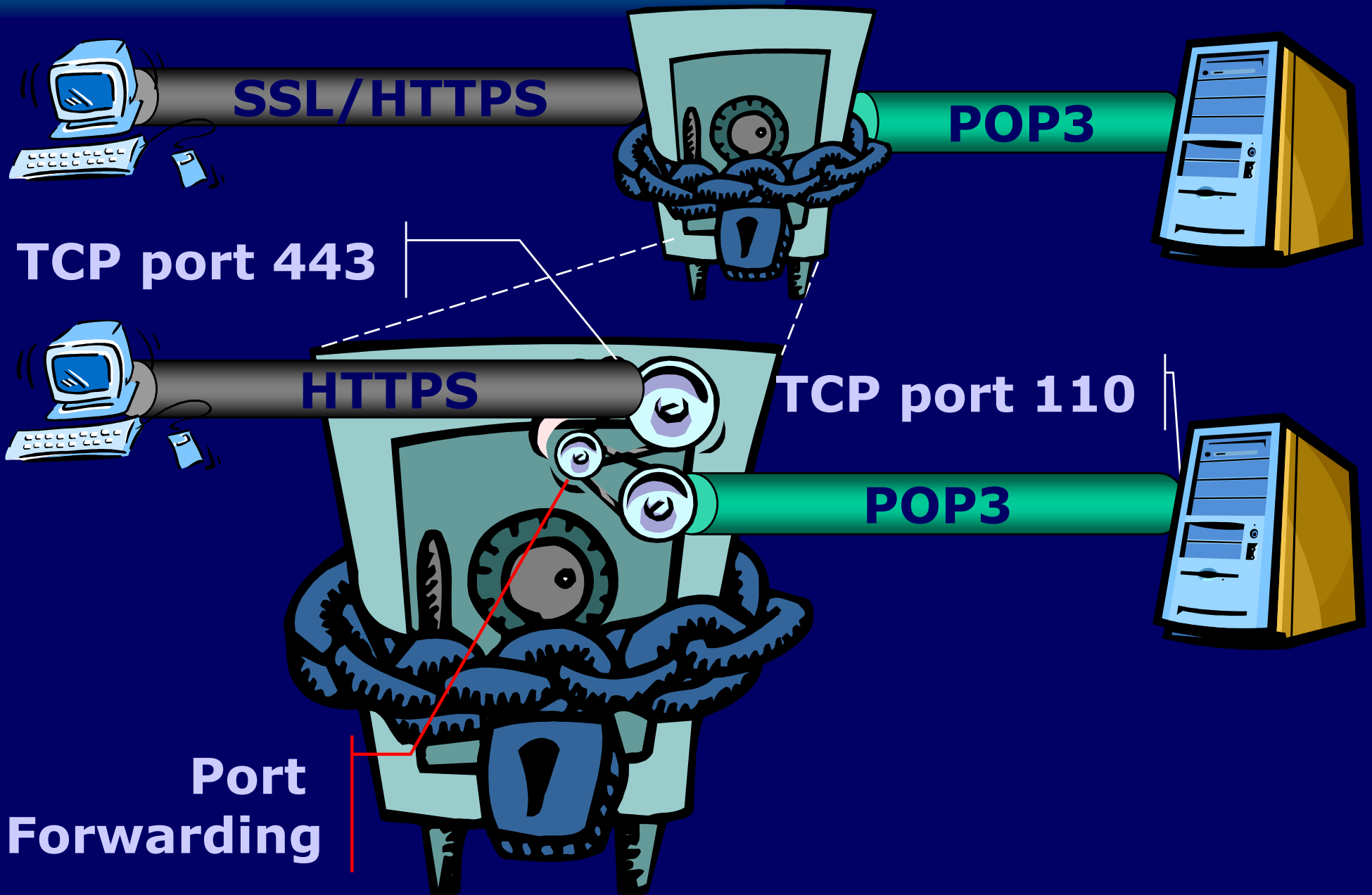
Port Forwarding



Port Forwarding

- Port forwarder sends data stream to SSL connection to VPN gateway
 - To port Y
 - Usually port 443 (HTTPS)
- VPN gateway forwards data stream to application server
 - To port X
 - E.g., TCP port 110 (POP3)

Port Forwarding

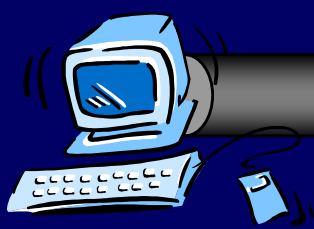


Port Forwarding

- Works only with fixed port protocols
- Problems with address and port in application layer protocol
 - SSL-VPN gateway must know application protocol to translate
 - Application layer gateway (ALG)

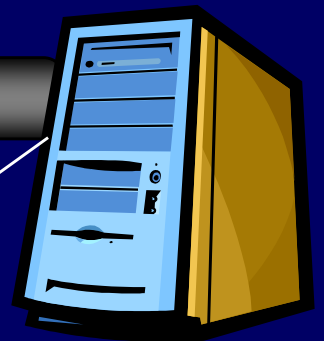
SSL'ed Protocols

- Secure application protocols
- Protocol-over-SSL
 - E.g., POP-over-SSL, IMAP-over-SSL, SMTP-over-SSL
- Client and server support required



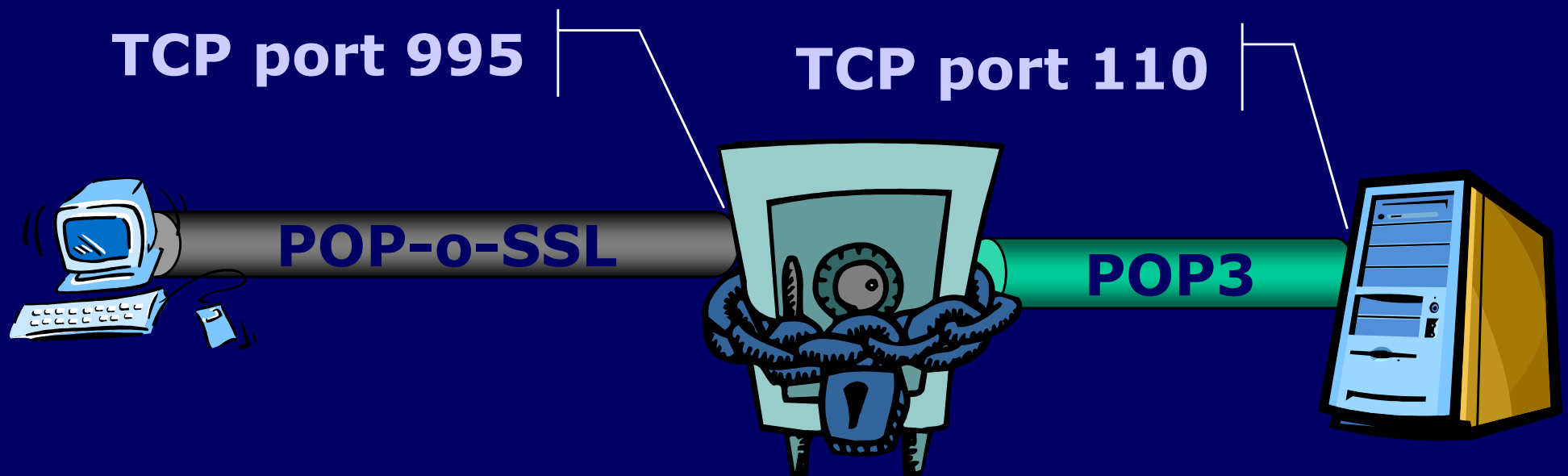
POP-over-SSL

TCP port 995

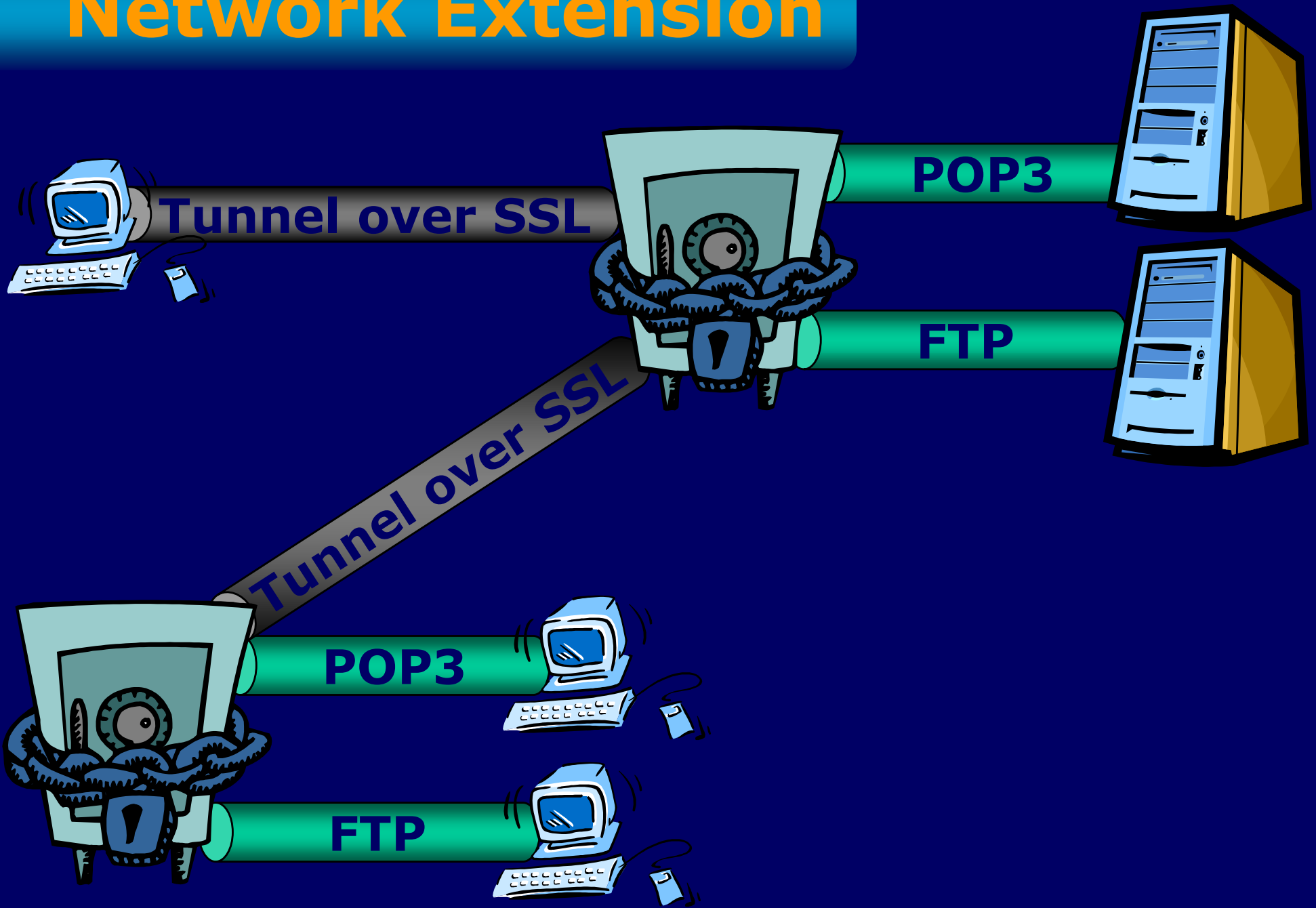


Application Proxying

- Compatibility with older servers
- Client points at SSL-VPN gateway



Network Extension



Products and Vendors

- **Open VPN (openvpn.net)**
- **AEP**
- **F5 Networks**
- **NetScreen Technologies**
- **Netilla**
- **Nokia**
- **Symantec**
- **Whale Communications**

Main Issues

- **Interoperability**
- **Product specific features**
- **Implementation weaknesses**
- **Availability of client on specific platforms**

Bibliography

- **S. Brumbaugh, "VPNs and Public Key Infrastructure," O'Reilly, Sep. 2004, http://www.onlamp.com/pub/a/security/2004/09/23/vpns_and_pki.html**
- **C. Hosner, "OpenVPN and the SSL VPN Revolution," SANS Institute, Aug. 2004, <http://www.sans.org/rr/whitepapers/vpns/1459.php>**
- **J. Snyder, "SSL VPN Gateways," NetworkWorldFusion, Dec. 2004, <http://www.nwfusion.com/reviews/2004/0112revmain.html>**