SSL VPN

Virtual Private Networks based on Secure Socket Layer

Mario Baldi

Politecnico di Torino

(Technical Univesity of Turin)

http://staff.polito.it/mario.baldi

SSL VPN: What is that?

SSL as the central mechanism on which to base secure access

- ➔ Site-to-site VPN
- ➔ Remote access VPN 远程接入VPN
- ➔ Secure service access 安全服务接入
  - ➔ Loose interpretation of VPN
    - ➔ SSL (pseudo)VPN
- ➔ Tunneling based on TCP or UDP

管道是基于TCP或者UDP

Why Not IPsec VPN?

IPsec太复杂并且过于昂贵

- 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 低复杂度
  - Installation
  - Configuration
  - Management

跟核心区域没有交互

- Non-interference with kernel
- Most widely used 广泛使用
- Higher, more robust security

更高的安全鲁棒性

Compared to IPsec VPN

- No problem with NAT traversal
  - No authentication of IP header
  - ESP (encapsulation securty payload) IPsec to be used
- Packets dropped at a higher level L4判断是否丢弃数据包
  - Critical with DOS attacks 对DoS攻击很敏感

Compared to PPTP

微软专用

- Initially proprietary (Microsoft)
- Initially weak security
  - Fixed later

脆弱的安全性

- Poor interoperability with non-Microsoft platforms

兼容性差

- GRE (generic routing encapsulation) tunneling
  - Possibly blocked by routers

使用的是GRE管道，很有可能会被路由器屏蔽

SSL (pseudo)VPN

IPsec直接连接网络，对整个主机，或子网开VPN

- IPsec VPNs connect networks
  - Or hosts to networks
- SSL VPNs connect

SSL只对，应用或者用户开VPN

  - Users to services
  - Application clients to application servers

Why SSL (pseudo)VPN

- No client code is to be installed
  - Usable anywhere (kyosk)
- Applications available through web browser
  - Deploying HTTPS
- Not a general security solution

不是一个普遍的安全解决方案（取决于应用的类型）

  - 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 内网穿透
  - Firewall traversal 防火墙穿透
  - Router traversal 路由器穿透
- SSL (pseudo)VPN enable universal client (web browser)

SSL VPN Flavors

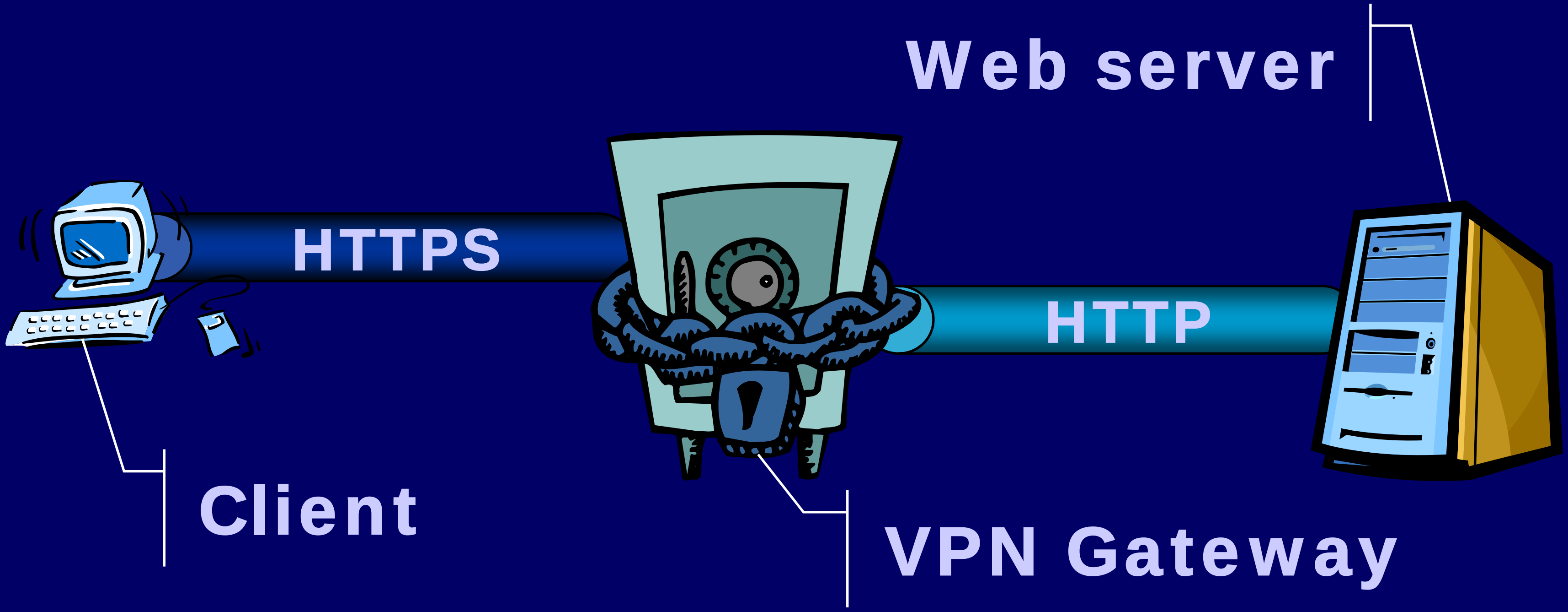
- Web proxying 代理
- Application translation
- Port forwarding
- SSL’ed protocols
- Application proxying
- Network extension
  - Site-to-site connectivity

Pseudo VPN

Proxying

代理

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

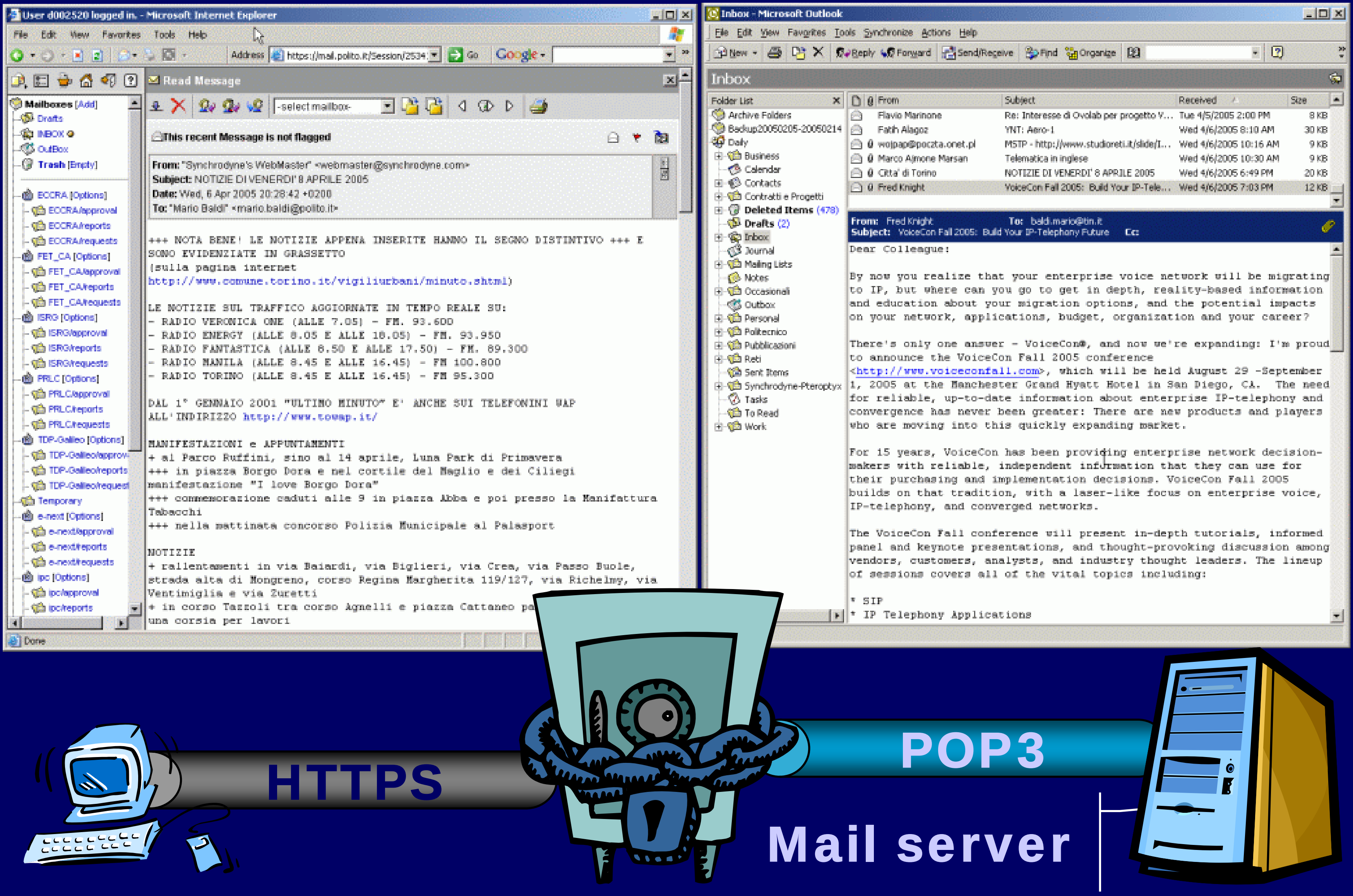


Application Translation

- 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

应用转换：应用工作像一个浏览器

Application Translation



From: "Synchrodyne's WebMaster" <webmaster@synchrodyne.com>
Subject: NOTIZIE DI VENERDI' 8 APRILE 2005
Date: Wed, 6 Apr 2005 20:28:42 +0200
To: "Mario Baldi" <mario.baldi@polito.it>

```
+++ NOTA BENE! LE NOTIZIE APPENA INSERITE HANNO IL SEGNO DISTINTIVO +++ E
SONO EVIDENZIATE IN GRASSETTO
(sulla pagina internet
http://www.comune.torino.it/vigiliurbani/minuto.shtml)

LE NOTIZIE SUL TRAFFICO AGGIORNATE IN TEMPO REALE SU:
- RADIO VERONICA ONE (ALLE 7.05) - FM. 93.600
- RADIO ENERGY (ALLE 8.05 E ALLE 18.05) - FM. 93.950
- RADIO FANTASTICA (ALLE 8.50 E ALLE 17.50) - FM. 89.300
- RADIO MANILA (ALLE 8.45 E ALLE 16.45) - FM 100.800
- RADIO TORINO (ALLE 8.45 E ALLE 16.45) - FM 95.300

DAL 1° GENNAIO 2001 "ULTIMO MINUTO" E' ANCHE SUI TELEFONINI WAP
ALL'INDIRIZZO http://www.towap.it/

MANIFESTAZIONI e APPUNTAMENTI
+ al Parco Ruffini, sino al 14 aprile, Luna Park di Primavera
+++ in piazza Borgo Dora e nel cortile del Maglio e dei Ciliegi
manifestazione "I love Borgo Dora"
+++ commemorazione caduti alle 9 in piazza Abba e poi presso la Manifattura
Tabacchi
+++ nella mattinata concorso Polizia Municipale al Palasport

NOTIZIE
+ rallentamenti in via Baiardi, via Biglieri, via Crea, via Passo Buole,
strada alta di Mongreno, corso Regina Margherita 119/127, via Richelmy, via
Ventimiglia e via Zuretti
+ in corso Tazzoli tra corso Agnelli e piazza Cattaneo pa
una corsia per lavori
```

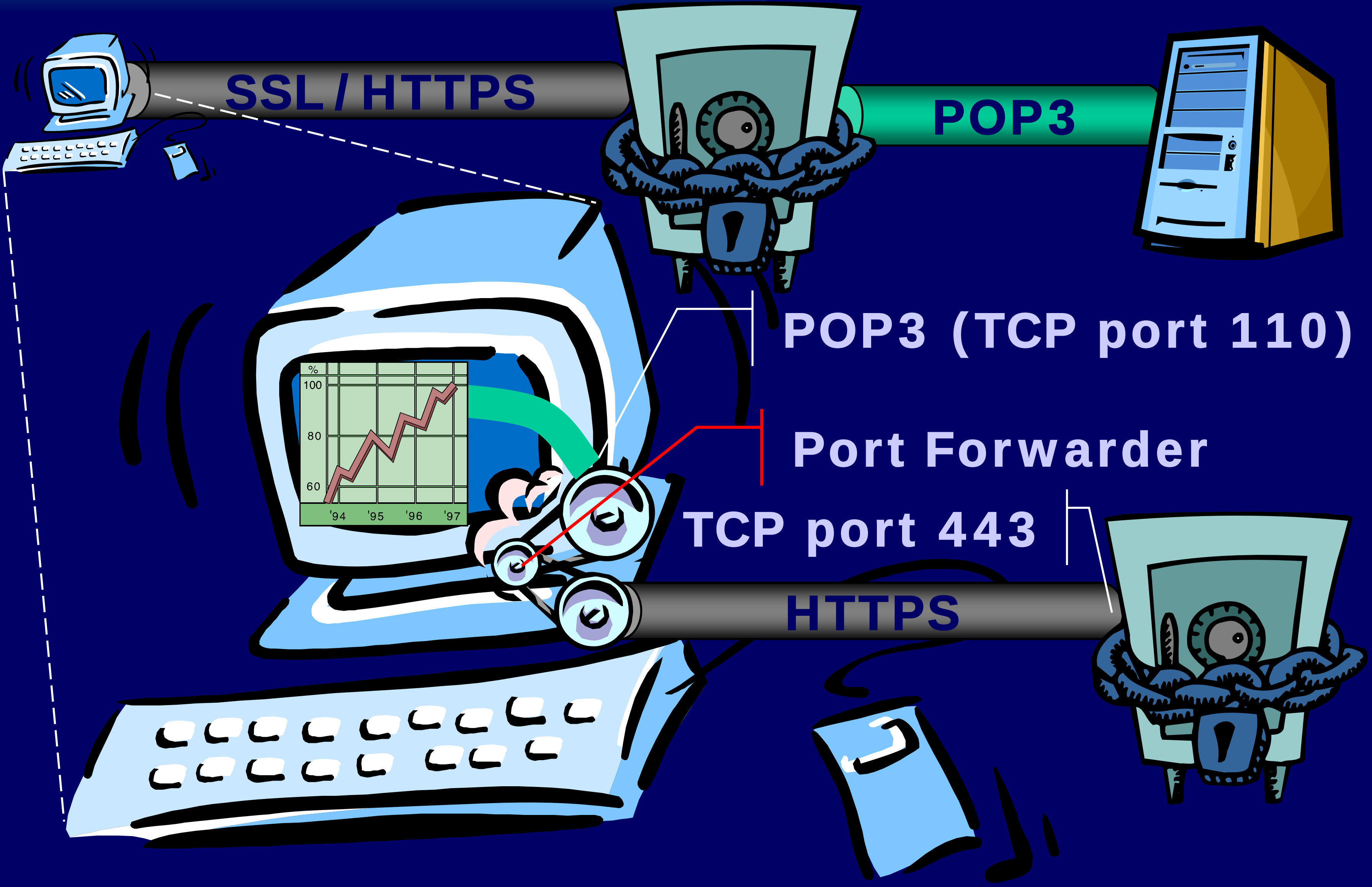
From	Subject	Received	Size
Flavio Marinone	Re: Interesse di Ovolab per progetto V...	Tue 4/5/2005 2:00 PM	8 KB
Fatih Alagoz	YNT: Aero-1	Wed 4/6/2005 8:10 AM	30 KB
wojpap@poczta.onet.pl	MSTP - http://www.studioreti.it/slide/I...	Wed 4/6/2005 10:16 AM	9 KB
Marco Ajmone Marsan	Telematica in inglese	Wed 4/6/2005 10:30 AM	9 KB
Citta' di Torino	NOTIZIE DI VENERDI' 8 APRILE 2005	Wed 4/6/2005 6:49 PM	20 KB
Fred Knight	VoiceCon Fall 2005: Build Your IP-Tele...	Wed 4/6/2005 7:03 PM	12 KB

From: Fred Knight **To:** baldi.mario@tin.it
Subject: VoiceCon Fall 2005: Build Your IP-Telephony Future **Cc:**

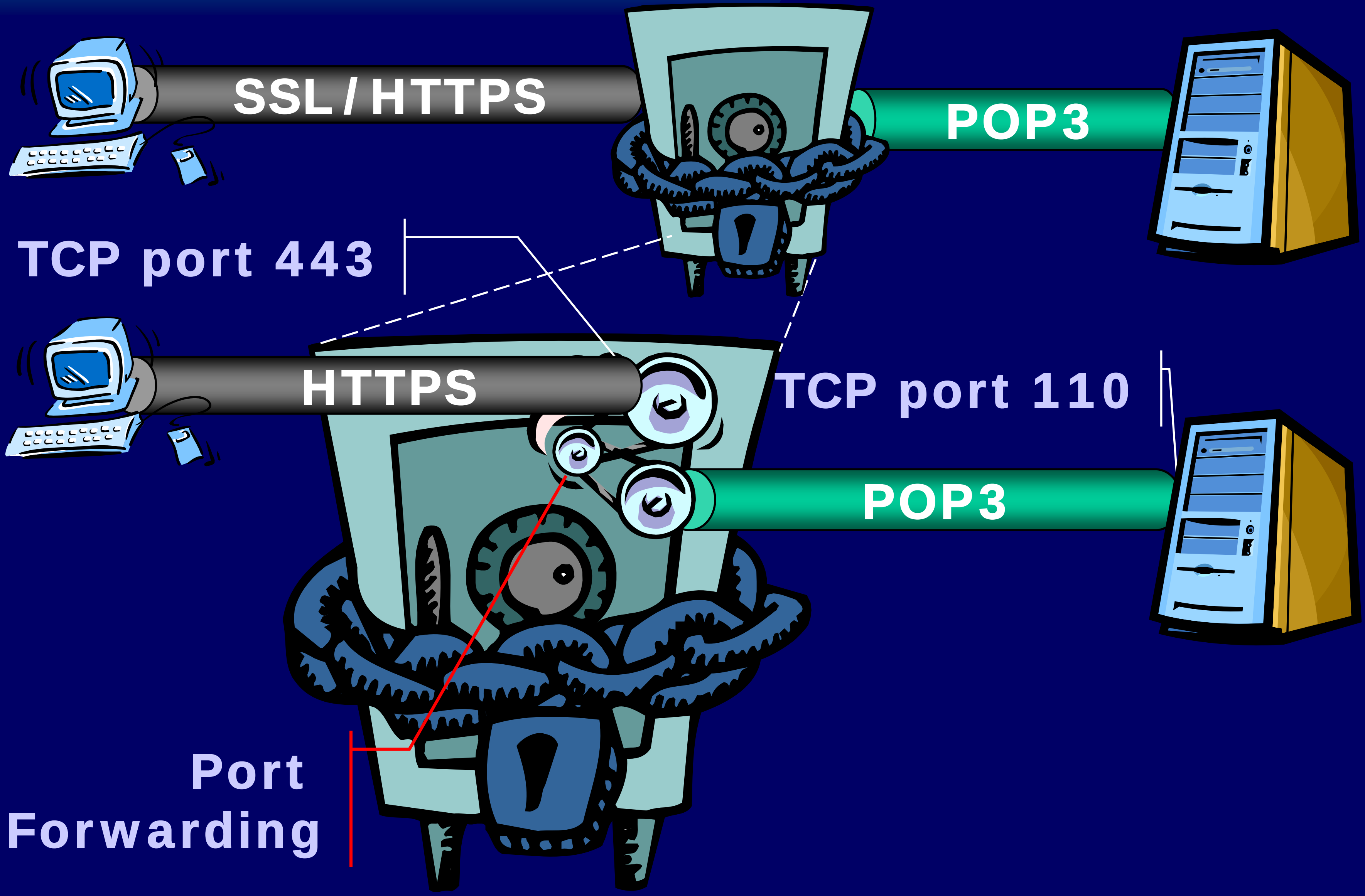
```
Dear Colleague:

By now you realize that your enterprise voice network will be migrating
to IP, but where can you go to get in depth, reality-based information
and education about your migration options, and the potential impacts
on your network, applications, budget, organization and your career?

There's only one answer - VoiceCon®, and now we're expanding: I'm proud
to announce the VoiceCon Fall 2005 conference
<http://www.voiceconfall.com>, which will be held August 29 -September
1, 2005 at the Manchester Grand Hyatt Hotel in San Diego, CA.  The need
for reliable, up-to-date information about enterprise IP-telephony and
convergence has never been greater: There are new products and players
who are moving into this quickly expanding market.

For 15 years, VoiceCon has been providing enterprise network decision-
makers with reliable, independent information that they can use for
their purchasing and implementation decisions. VoiceCon Fall 2005
builds on that tradition, with a laser-like focus on enterprise voice,
IP-telephony, and converged networks.

The VoiceCon Fall conference will present in-depth tutorials, informed
panel and keynote presentations, and thought-provoking discussion among
vendors, customers, analysts, and industry thought leaders. The lineup
of sessions covers all of the vital topics including:

* SIP
* IP Telephony Applications
```

Port Forwarding

端口映射：110到443



Port Forwarding



Port Forwarding

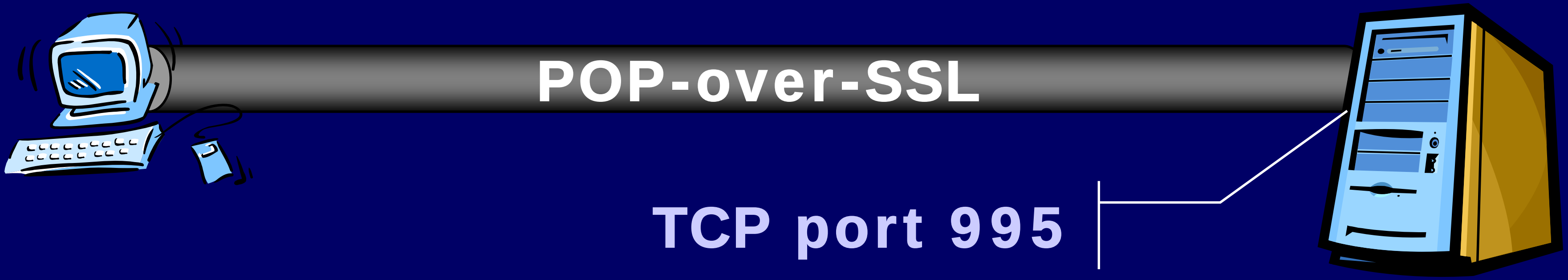
- Works only with fixed port protocols 只能用于固定的端口协议
- Problems with address and port in application layer protocol

  应用层协议中的地址和端口问题
  - SSL-VPN gateway must know application protocol to translate
  - Application layer gateway (ALG)

SSL’ed Protocols

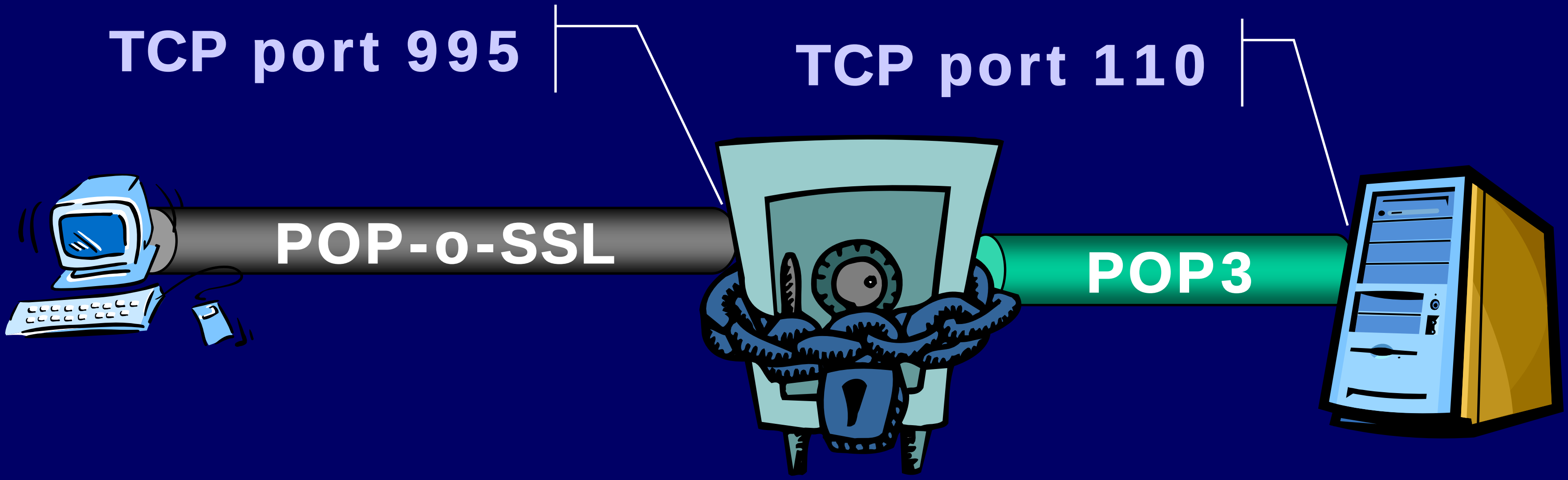
安全应用层协议

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

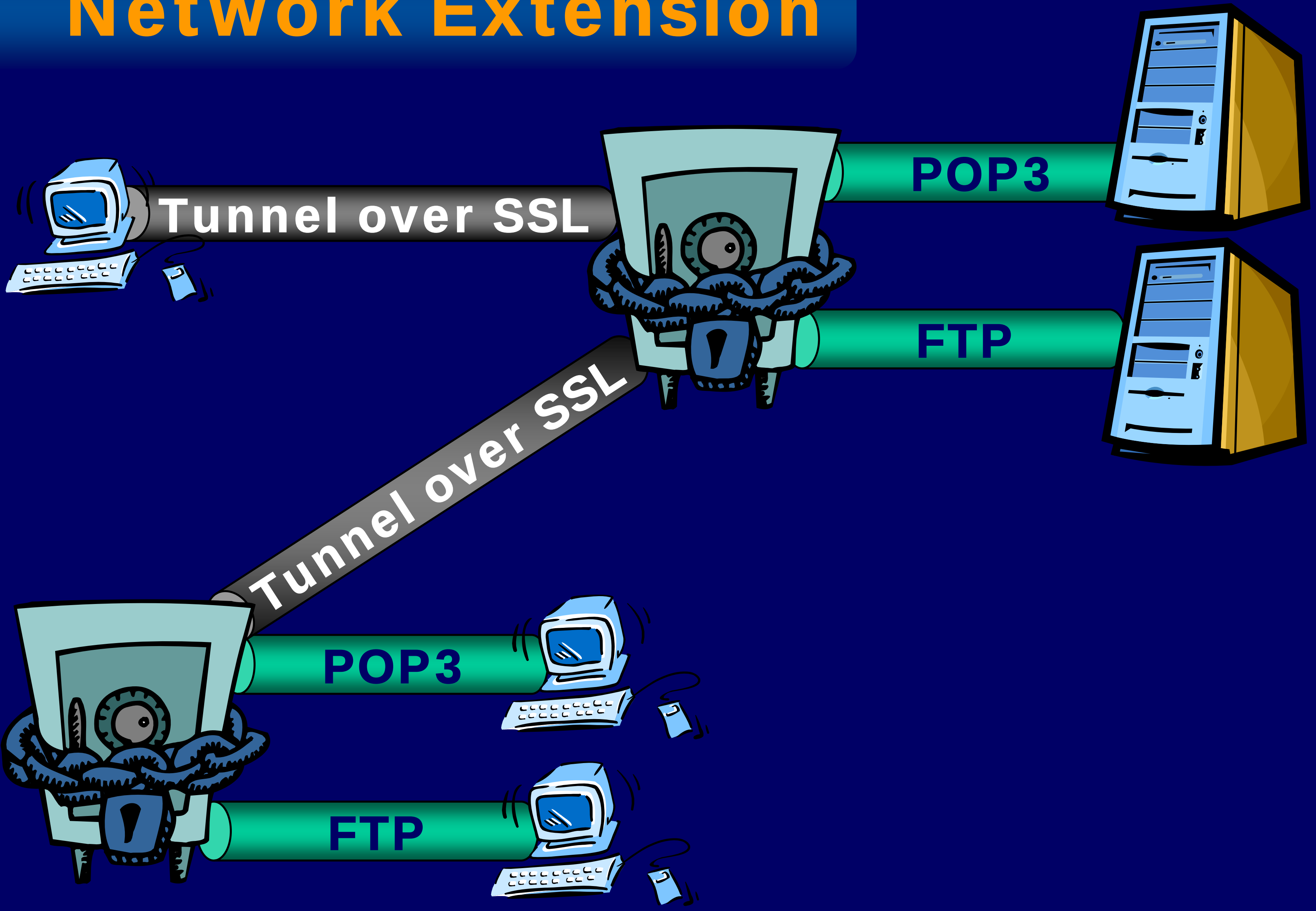


Application Proxying

- 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 互用性
- Product specific features 特定产品的功能
- Implementation weaknesses 实现的弱点
- Availability of client on specific platforms 特定平台上客户机的可用性