

Securing a Windows 2000 Server

Virginia Tech NT Users Group

By Adel Alfahad

Introduction

- Securing a WIN2000 Server using Native Tools “configuring firewall”
- Demonstrating IPSec, VPN and IP filters
- Background and interest of the audience
 - IPSec details or brief

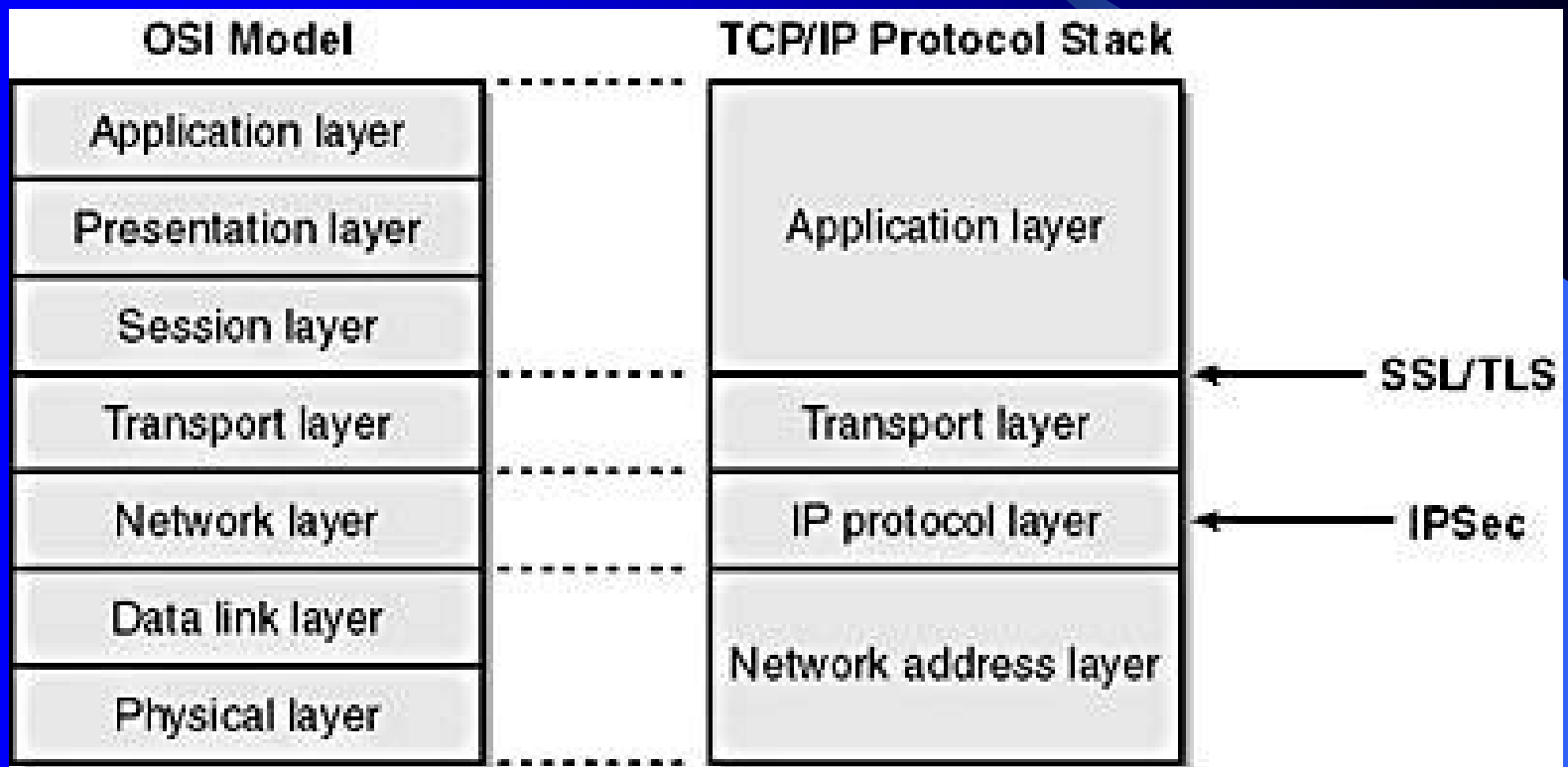
Agenda

- Topics covered
 - IPSec or IP secure, 15 minutes
 - VPN, 15 minutes
 - IP filters, 25 minutes

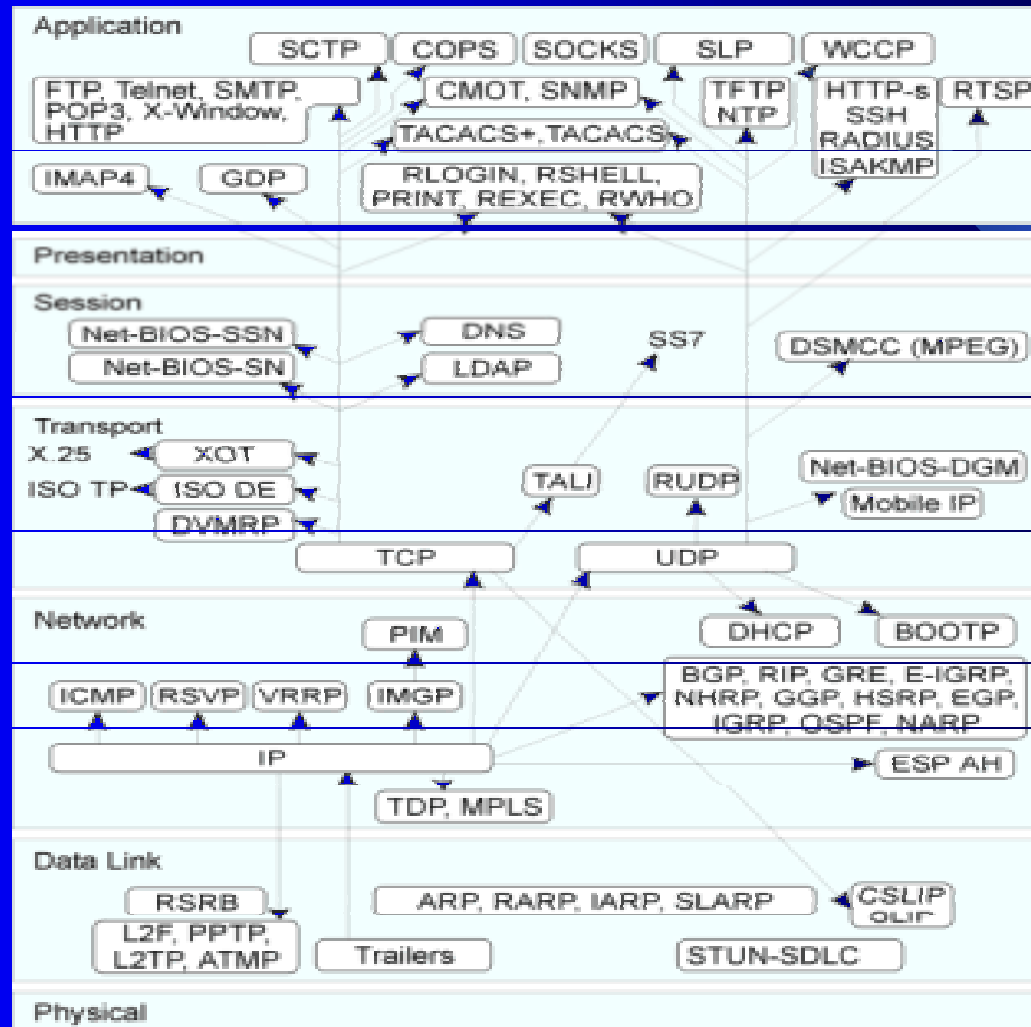
Overview

- Protecting WIN2000 server using Network Layer of the OSI model
 - common firewall like zonealarm uses the Application Layer of the OSI model
- All Tools needed together for complete protection
 - IPSec, VPN for remote users and IP filters

OSI Model & TCP/IP Stack



Detailed TCP/IP stack



IPSec or Secure IP

- Introduction

- Guarantees all data is authenticated and encrypted
- Provides data security at the network layer
 - most encrypting tools works at the application level (SSH, PGP)
 - does not secure data if application can be cracked
- Securing at network layer is more secure
 - difficult to crack
 - independent of applications
 - transparent to the user
 - transparent to routers
 - Does not require a special router configuration

IPSec, Introduction

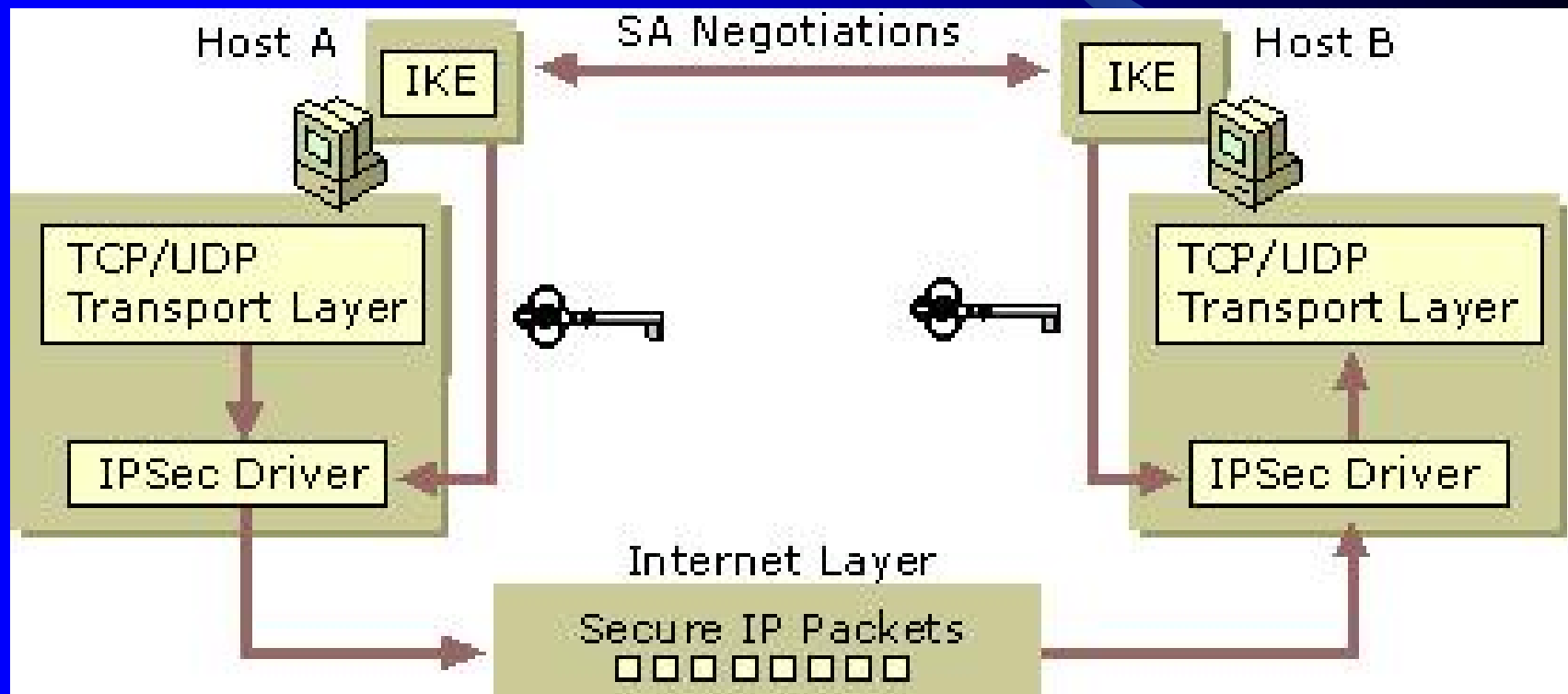
- IPSEC enhances security
 - mutually authenticates computers prior to data exchange
 - Establishes a direct security association between computers
 - Fully encrypts the entire data exchange
- IPSec is an excellent solution
 - Especially for VPN tunnels
 - if implementing IPSEC on entire network
 - Must plan extremely well
 - if a machine requires secure data transmission it will not communicate with machines that do not share the same level of security

IPSec, Encryption & Authentication

- IPSEC provides a varying level of security
 - The Primary encryption methods
 - DATA Encryption standard (DES)
 - Triple DES (3DES)
 - 40-bit DES (International)
 - Transparent authentication methods
 - used when connections are initiated
 - Kerberos V5 authentication
 - Exchange of certificate authority
 - Uses digital signatures to exchange and authenticate
 - Exchange pre-configure private keys
 - Random text value which is input when IPSec is setup
 - done on both ends for connectivity

URL: [Step-by-Step Guide to Internet Protocol Security \(IPSec\)](#)

IPSec Figure



IPSec, continue

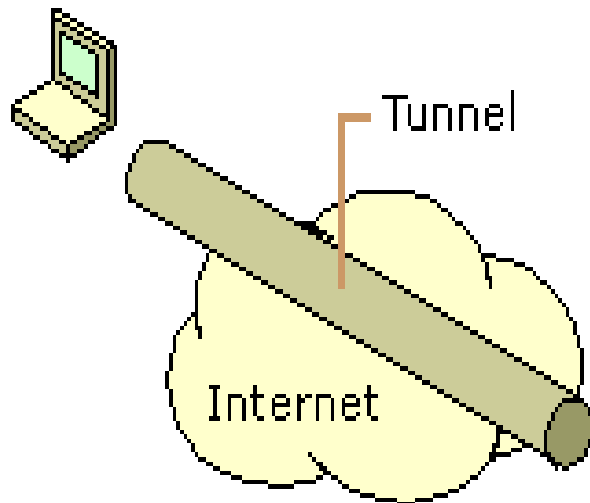
- IPSEC allows a variety of secure conversations
 - Two modes in IPSec in win2000
 - Transport mode
 - Implementation everywhere
 - Tunnel
 - Specify end points like VPN L2TP
 - Demonstrations
 - Local security policy
 - Group policy (requires DC)
 - Wizards for specific setting

VPNs

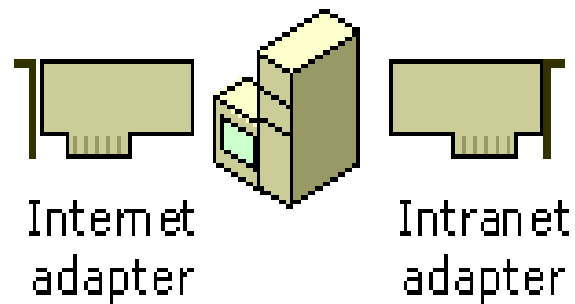
- Two Types
 - PPTP (point to point tunneling protocol)
 - L2TP (Layer two tunneling protocol)
- PPTP
 - Provides secure Tunnels between endpoints using network (GRE) and Transport (TCP) layers of the OSI Model
 - Emulate both Data link Layer and network Layer of OSI Model between the endpoints

PPTP figure

PPTP remote access client



Windows 2000 VPN server



Corporate intranet

VPN continues

- PPTP Demo

URL: [Server configuration](#)

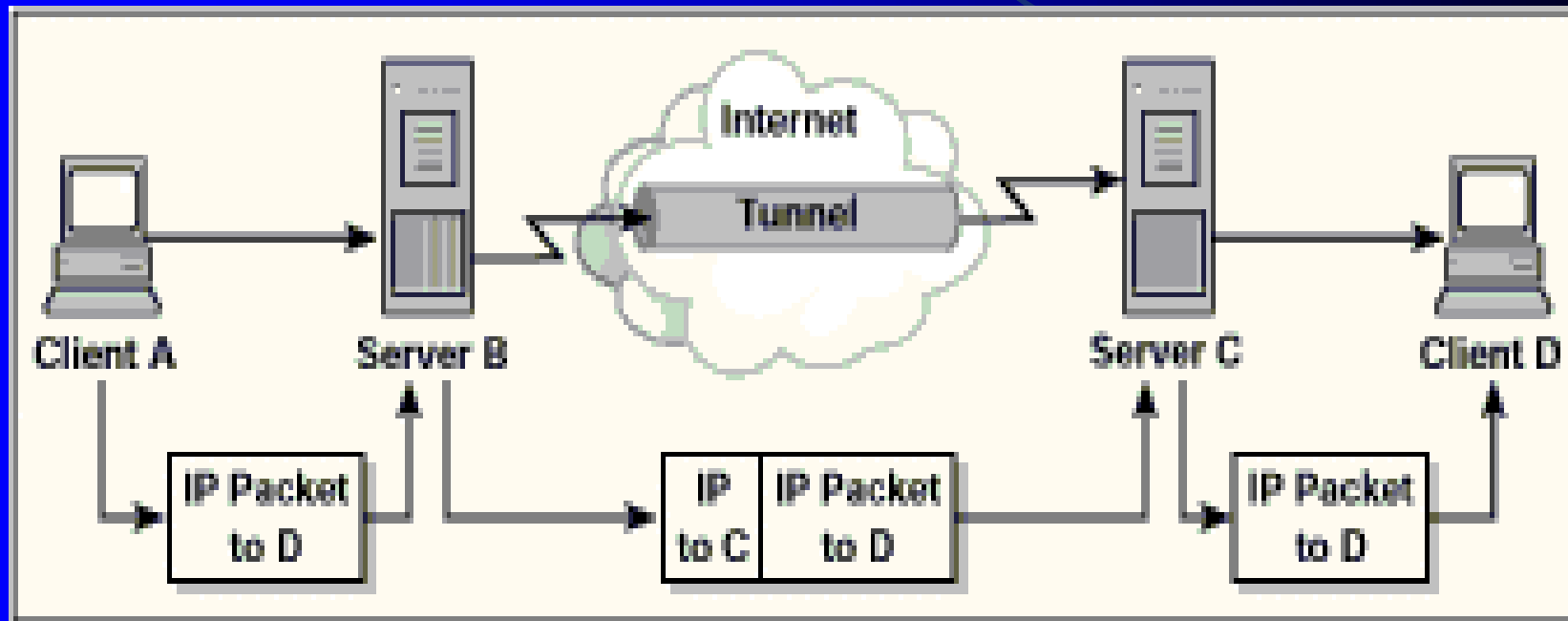
-Client configuration

- [L2TP](#)

-Adds IPSEC Mechanism to PPTP

-Demo is out of the lecture scope

L2TP Figure



IP filters

- IP filters works in the Network Layer of OSI model unlike Zonealarm (Applications Layer)
 - Less resources overhead (DLLs)
 - Harder to break
- Three Levels of IP filters in win2000
- The NT 4.0 legacy Packet filter
 - deny all but" basis
 - Show demo

IP filters, continue

- IPSEC IP filter implementation
 - Allows an interesting combination of filtering/tunneling

URL: [Step-by-Step Guide to Internet Protocol Security \(IPSec\)](#)

- Show Demo
 - Local Policy setting wizard
 - [IPSECPOL](#) Tool
 - Port scan (NMAP)

URL: [Q150543](#) default port in win2000

IP filters, continue

- IPSECPOL Tool demo

```
ipsecpol \\computername -w REG -p "Web" -o
```

```
ipsecpol \\computername -x -w REG -p "Web" -r  
"BlockAll" -n BLOCK -f 0+*
```

```
ipsecpol \\computername -x -w REG -p "Web" -r  
"OkHTTP" -n PASS -f 0:80+*::TCP
```

SourceAddr:SourcePort+DestinationAddr:DestinationPort:Protocol

IP filters, continue

- Routing and remote access feature (RRAS) also NETSH (URL: [Q242468](#))
 - define output/input filters per interface
 - enable fragmentation checking
 - The stack behaves extremely well under heavy TCP/UDP port scans. (dropping Raw/ARP/ICMP/IGMP packets)
- Show demo
 - netstat -an (shows listing ports)
 - Stealth mode scan (nmap -g 80)

Summary

- Learned techniques of securing win2000 server using the built in tools IPSec, IP filters (RRAS and IPSec filters) and VPNs (PPTP)

Where to Get More Information

- Other techniques
 - Content filtering using Squid for NT
- List books, articles, electronic sources
 - MS Press e-books
 - Designing Secure Web-Base Apps for W2k
 - URL: [TechNet Security](#)
 - The Rest of Internet
 - My Email: aalfahad@vt.edu