



OS/390 Firewall Technology

The hidden Security Treasure

Vanguard Enterprise Security Expo '99


June 6-11, 1999 Session 28

Paul de Graaff
 IBM International Technical Support Organisation
 Poughkeepsie, New York


(914) 433-1389
 graaff@us.ibm.com




IBM Technical Support



Disclaimer




The information contained in this document is distributed on an "as is" basis without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed programs may be used. Functionally equivalent programs may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.


It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.




© Copyright IBM Corporation, 1999

IBM Technical Support



Trademarks




The following are trademarks of International Business Machines Corporation:

CICS	DFSMS	HiperBatch
DB2	Open Edition	PSF
IBM	OS/390	System/390
IMS	MVS/ESA	VTAM
	RACF	


The following are trademarks or registered trademarks of other companies or institutions:

Open Software Foundation	Open Software Foundation, Inc.
OSF	
DCE	
Distributed Computing Environment	
NetWare	Novell
NT	Microsoft Corporation
ACF2, Topsecret	Computer Associates Inc.




© Copyright IBM Corporation, 1999


IBM Technical Support



Agenda



- Network Security SNA and TCP/IP
- What is a Firewall ?
- OS/390 Key Firewall Technology explained
- Sample customer scenarios
- OS/390 Firewall Technology Delivery
- Denial Of Service ?



© Copyright IBM Corporation, 1999

IBM Technical Support

@ Agenda

e-business

☛ Network Security SNA and TCP/IP

- What is a Firewall ?
- OS/390 Key Firewall Technology explained
- Sample customer scenarios
- OS/390 Firewall Technology Delivery
- Denial Of Service ?

IBM

© Copyright IBM Corporation, 1999

IBM Technical Support



Network Security in the SNA days

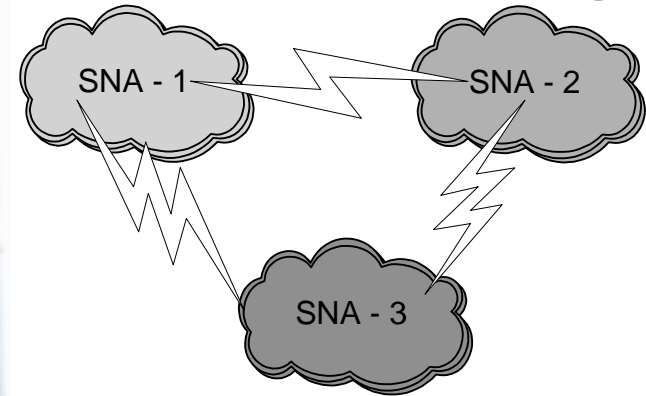
e-business



IBM

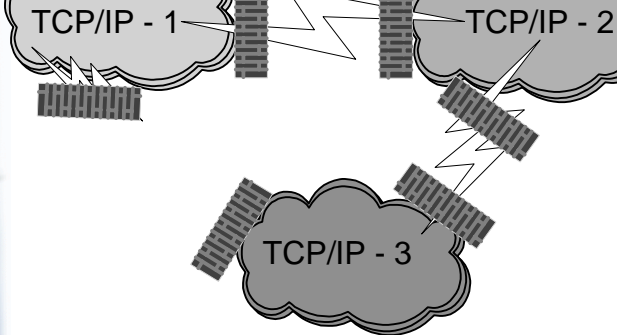
© Copyright IBM Corporation, 1999

IBM Technical Support



Network Security in the TCP/IP days

e-business



IBM

© Copyright IBM Corporation, 1999

IBM Technical Support



Agenda

e-business

- Network Security SNA and TCP/IP
- ☛ What is a Firewall ?
- OS/390 Key Firewall Technology explained
- Sample customer scenarios
- OS/390 Firewall Technology Delivery
- Denial Of Service ?

IBM

© Copyright IBM Corporation, 1999

IBM Technical Support



What is a Firewall ?

© Copyright IBM Corporation, 1999

IBM Technical Support

A Router Firewall

© Copyright IBM Corporation, 1999

IBM Technical Support

An Application Gateway Firewall

© Copyright IBM Corporation, 1999

IBM Technical Support

Agenda

- Network Security SNA and TCP/IP
- What is a Firewall ?
- OS/390 Key Firewall Technology explained
- Sample customer scenarios
- OS/390 Firewall Technology Delivery
- Denial Of Service ?

© Copyright IBM Corporation, 1999

IBM Technical Support



OS/390 Key Firewall Technologies



e-business

Access Control

- IP Packet Filter
- FTP (Application Gateway) Proxy
- SOCKS (Circuit Gateway) Server
- Network Address Translation (NAT)
- Virtual Private Networks (VPN)
- Real Audio Support

Management

- Logs and Reports
- Monitor and Detect
- Administration GUI



© Copyright IBM Corporation, 1999

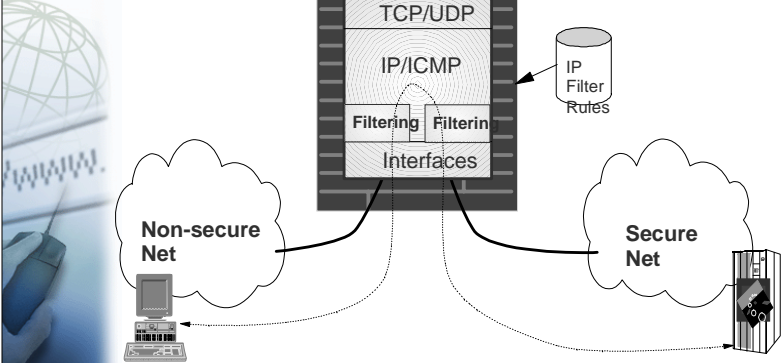
IBM Technical Support



IP Filters



e-business



© Copyright IBM Corporation, 1999

IBM Technical Support

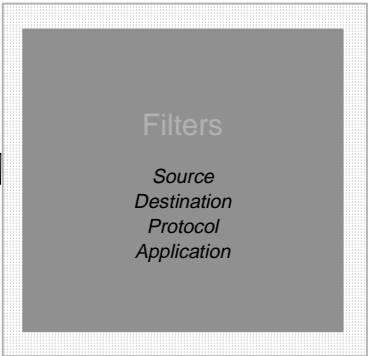


IP Filters ...



e-business

Internal



External



© Copyright IBM Corporation, 1999

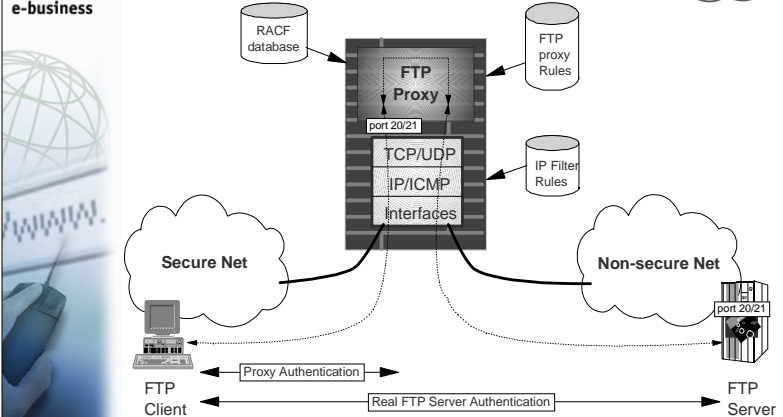
IBM Technical Support



FTP Proxy Server

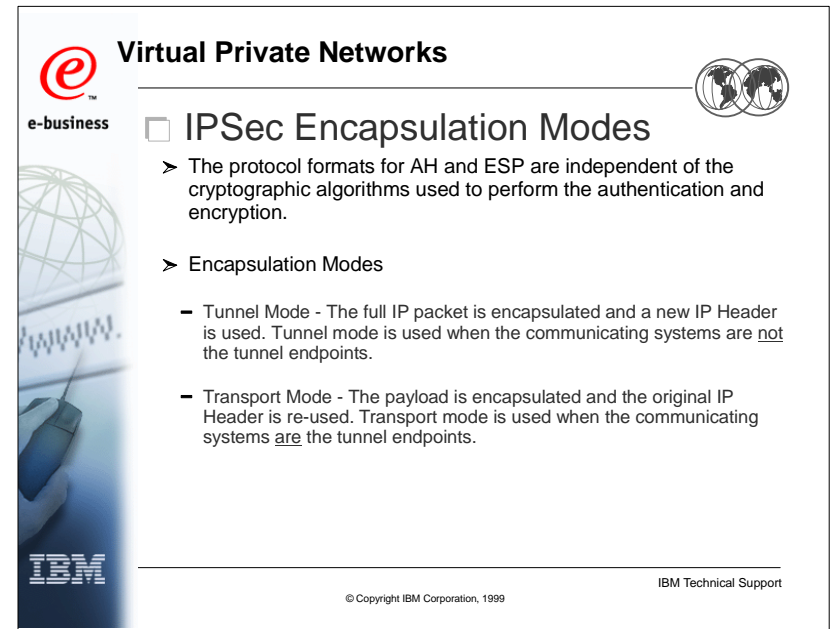
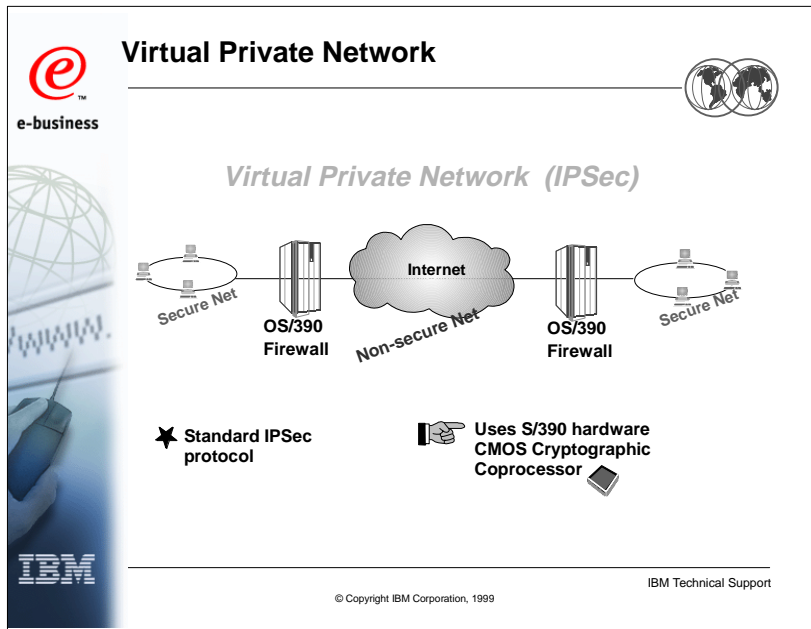
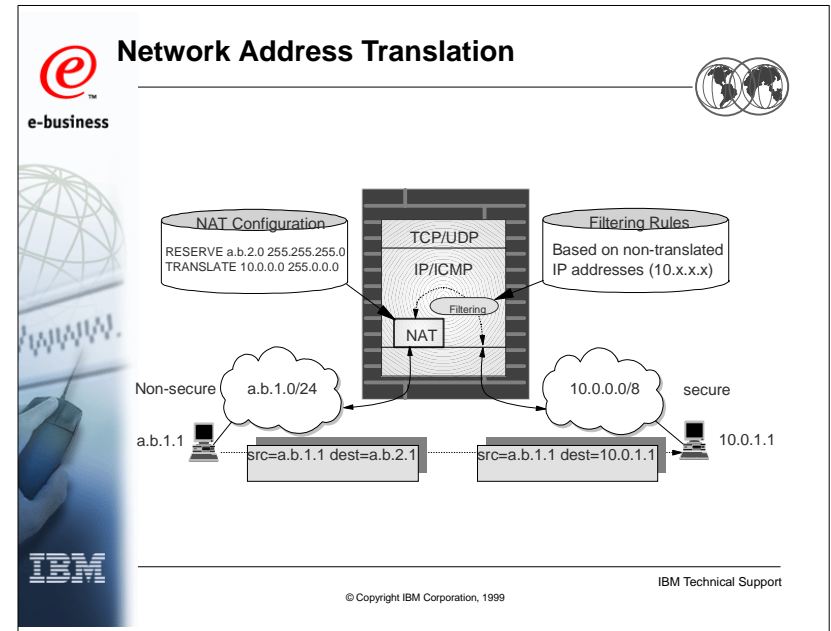
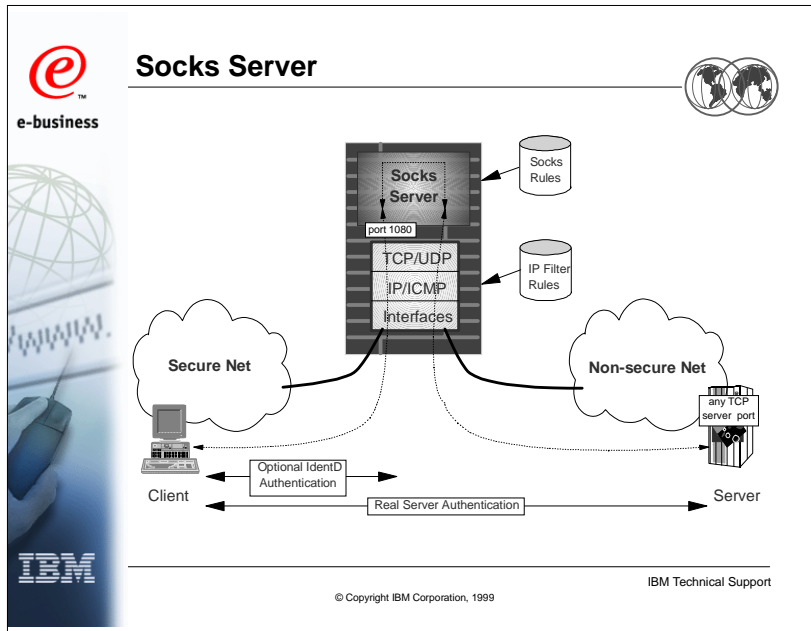


e-business



© Copyright IBM Corporation, 1999

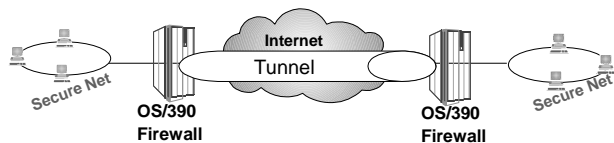
IBM Technical Support



Virtual Private Network ; Tunnel Mode



Virtual Private Network (IPSec)

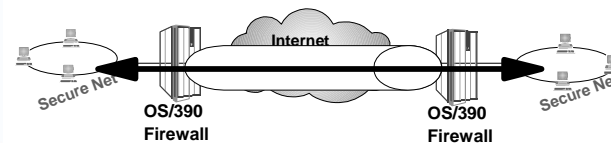


Tunnel mode designed to provide secure communications between two firewalls

Virtual Private Network ; Transport Mode

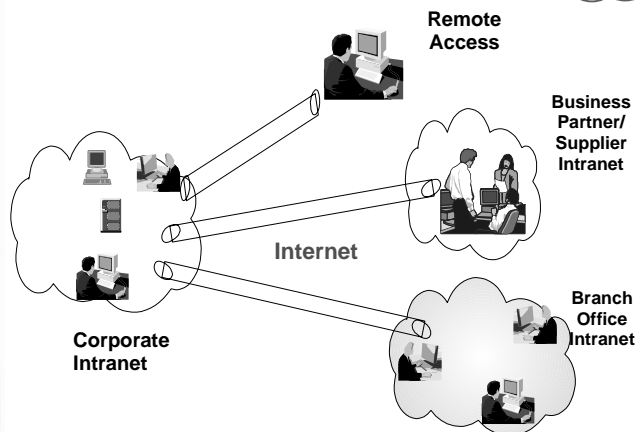


Virtual Private Network (IPSec)



Transport mode designed to provide secure communications between two communication systems

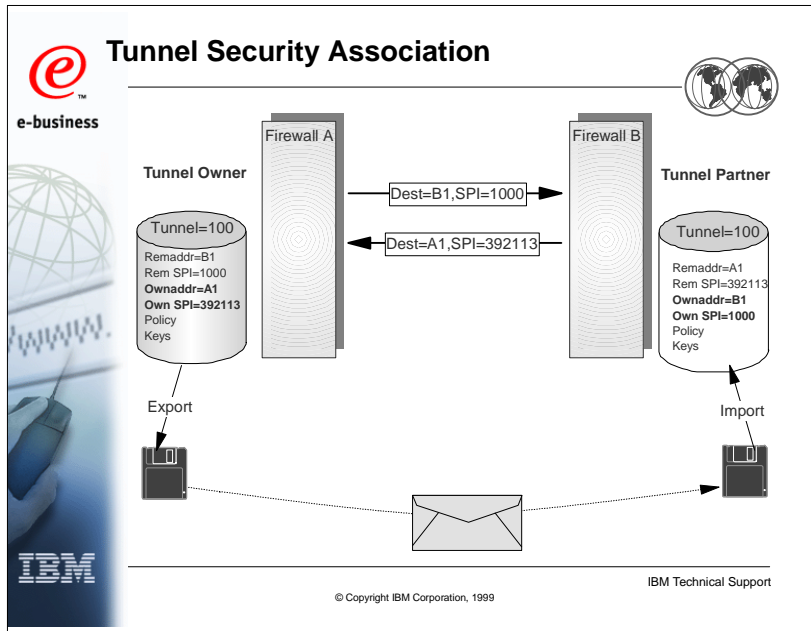
Customer's use of VPN's



VPN support on OS/390



- Support for so called manual tunnels only !
- Support for dynamic tunnels announced for V2R8 Sept.99
- Support for tunnel and transport mode !
- IPsec support for the latest Internet drafts to provide better interoperability.



- ## e-business Firewall Management
- Logs and Reporting
 - Monitor and Detect
 - Administration GUI
- © Copyright IBM Corporation, 1999
- IBM Technical Support

- ## e-business Logging & Reporting
- Enhanced SYSLOG Daemon
 - Logs Firewall events in a condensed format to either :
 - > HFS log files
 - > SMF records (TYPE 109)
 - No standard Reporting Utility currently available !
 - We will supply a REXX procedure to prepare the records for loading into a Relational Database (DB2) as part of the redbook
- © Copyright IBM Corporation, 1999
- IBM Technical Support

- ## e-business Monitor and Detect
- Logging can be directed to the system log
 - System log can be scanned by Netview and Alerts can then be generated based upon thresholds set by customer !
 - This does not come out of the box !
 - Customer has to do that himself !
- © Copyright IBM Corporation, 1999
- IBM Technical Support

e-business Administration & Configuration

- Through the UNIX System Services command line interface
- Since Version 2 Release 7 a JAVA GUI
- System comes with predefined rule-set !

IBM Technical Support

© Copyright IBM Corporation, 1999

e-business Configuration Server

- Runs on OS/390
- Controlled by fwkern
- GUI <--> Config Server <--> DB APIs

IBM Technical Support

© Copyright IBM Corporation, 1999

e-business JAVA GUI

```

Command: Query Firewall Stack(s) Status
Command Viewer Results:
stack = CS390IP
status = Up
type = TCP/IP
level = N/A
active filters = No
filter logging = No
active NAT = No
Nat logging = No

stack = CS390IPB
status = Up
type = Firewall
level = 270
active filters = No
filter logging = No
active NAT = No
Nat logging = No
  
```

IBM Technical Support

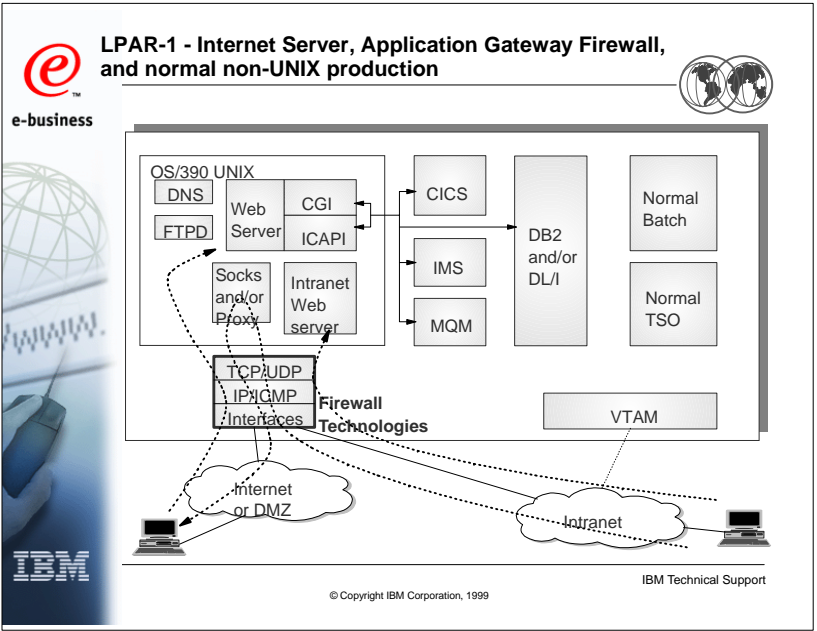
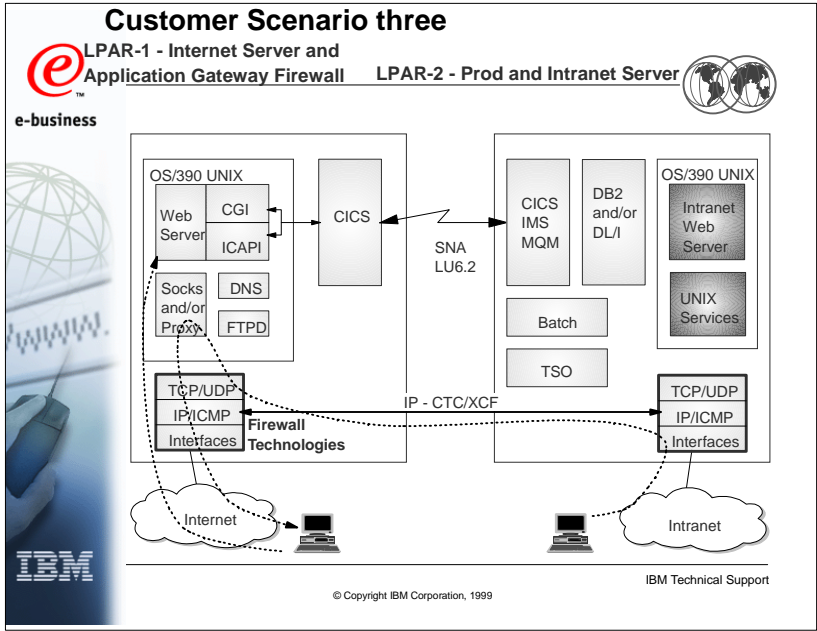
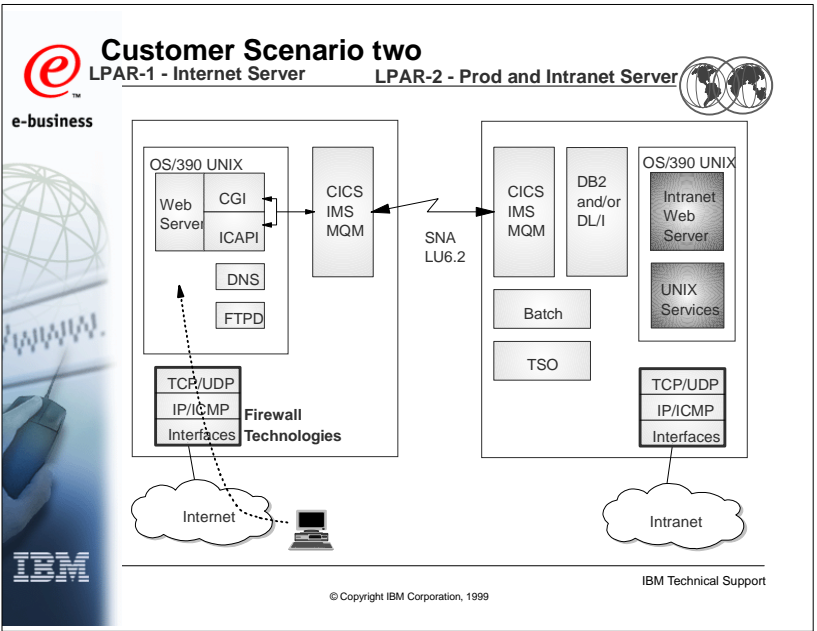
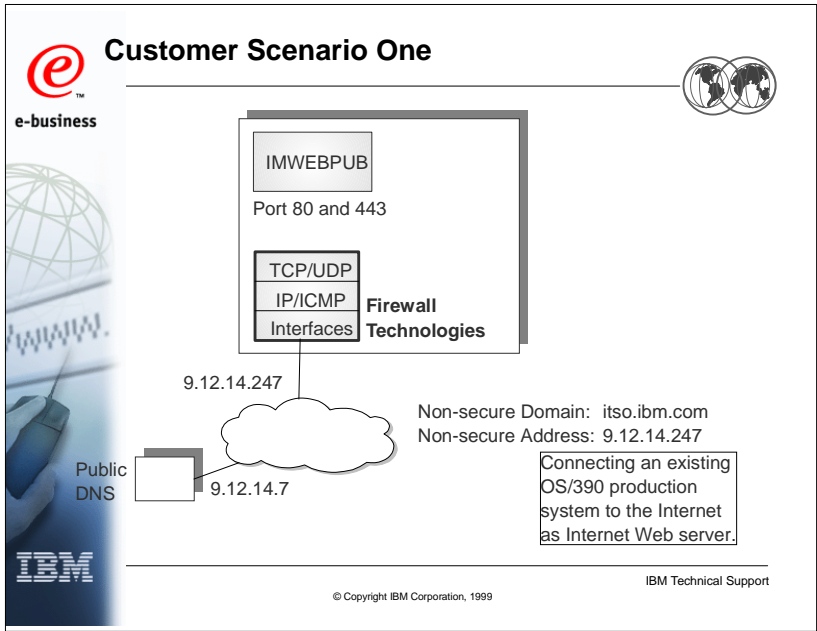
© Copyright IBM Corporation, 1999

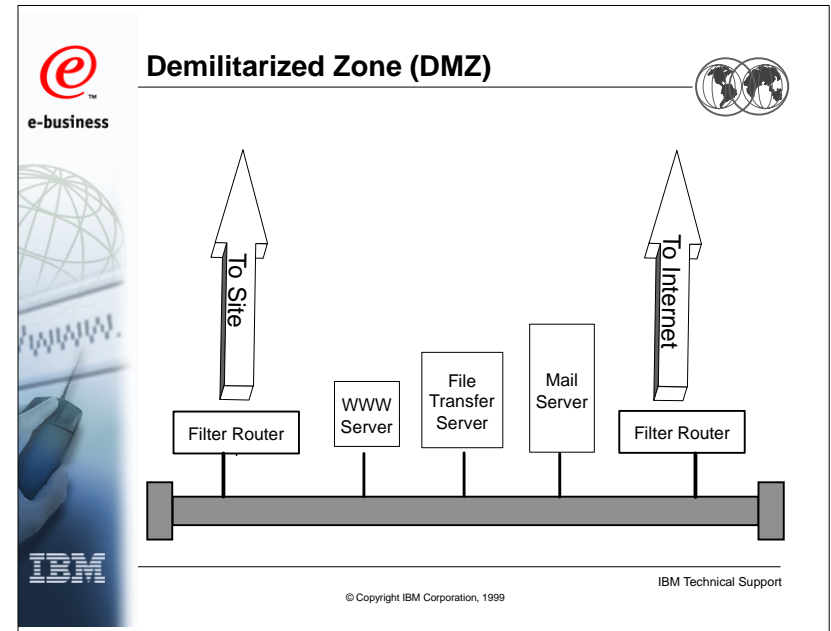
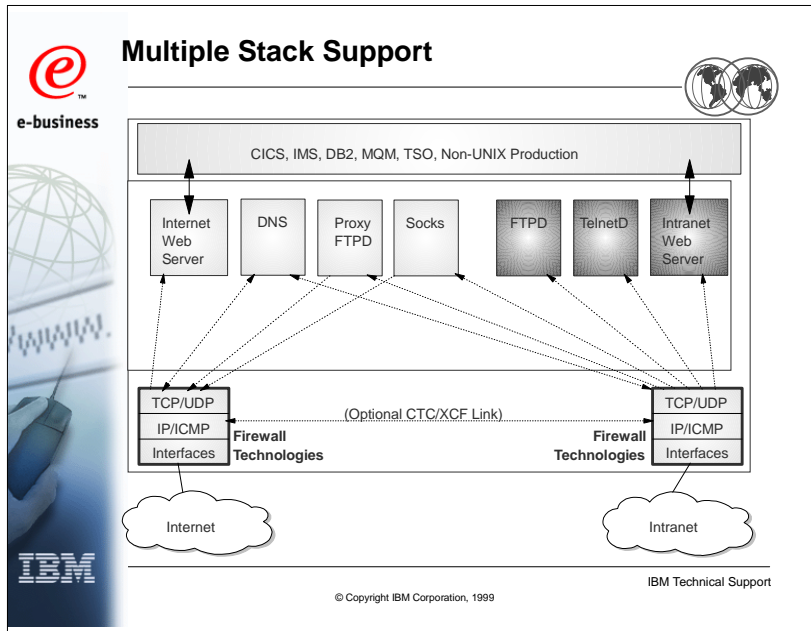
e-business Agenda

- Network Security SNA and TCP/IP
- What is a Firewall ?
- OS/390 Key Firewall Technology explained
- Sample customer scenarios
- OS/390 Firewall Technology Delivery
- Denial Of Service ?

IBM Technical Support

© Copyright IBM Corporation, 1999





- ## Agenda
- Network Security SNA and TCP/IP
 - What is a Firewall ?
 - OS/390 Key Firewall Technology explained
 - Sample customer scenarios
 - OS/390 Firewall Technology Delivery
 - Denial Of Service ?
- © Copyright IBM Corporation, 1999
- IBM Technical Support

- ## Software Requirements
- OS/390 Version 2 Release 4
 - OS/390 V2R4 eNetwork Communication Server IP, with the DNS w/WLM KIT SK2T-6136
 - OS/390 Security Server
 - OS/390 Firewall Technology Toolkit
 - OS/390 Version 2 Release 5
 - Firewall Technology integrated into :
 - OS/390 Security Server
 - OS/390 eNetwork Communication Server
- © Copyright IBM Corporation, 1999
- IBM Technical Support



OS/390 Firewall Technology Delivery



e-business

- OS/390 Security Server
 - Proxy server, Socks server
 - Enhanced Syslog daemon
 - Configuration Server (as of V2R7)
 - administration/configuration (no check in code to use this !!)
- OS/390 eNetwork Communication Server
 - IP filters
 - IPsec (tunnels, VPN)
 - Network Address Translation (N.A.T.)
- Customers using CA-ACF2/Topsecret will not have the Security Server functions !!



© Copyright IBM Corporation, 1999

IBM Technical Support



Agenda



e-business

- Network Security SNA and TCP/IP
- What is a Firewall ?
- OS/390 Key Firewall Technology explained
- Sample customer scenarios
- OS/390 Firewall Technology Delivery
- Denial Of Service ?



© Copyright IBM Corporation, 1999

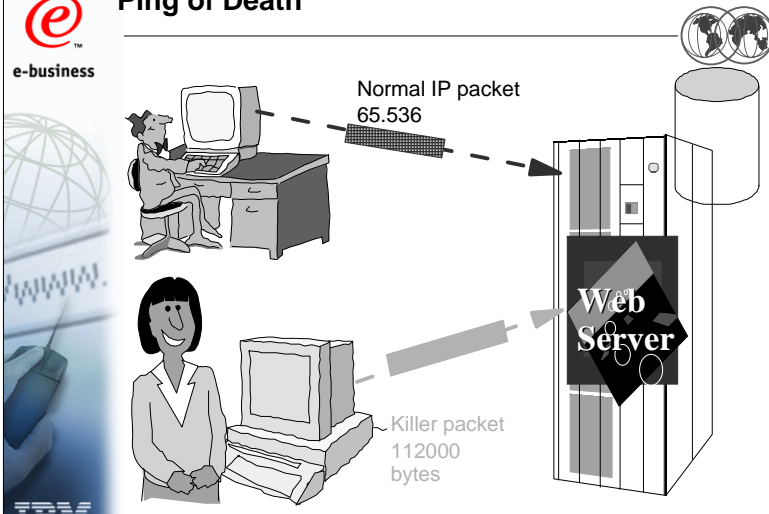
IBM Technical Support



Ping of Death



e-business



© Copyright IBM Corporation, 1999

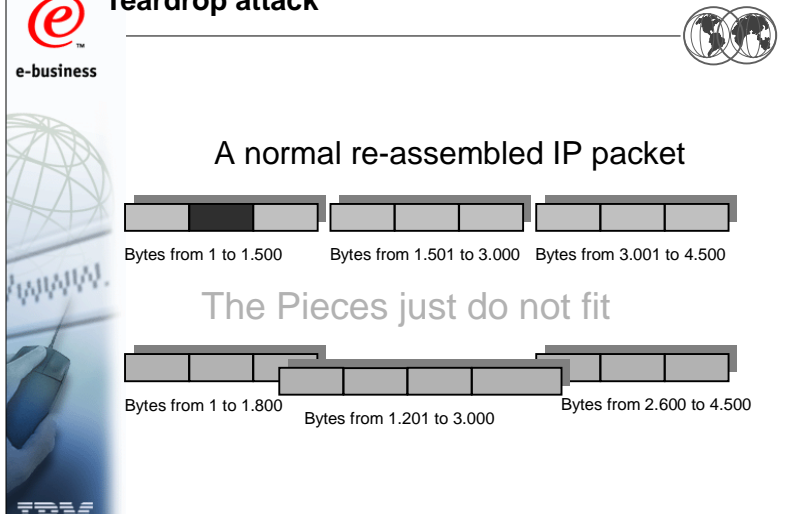
IBM Technical Support



Teardrop attack



e-business



© Copyright IBM Corporation, 1999

IBM Technical Support



e-business

Agenda



- Network Security SNA and TCP/IP
- What is a Firewall ?
- OS/390 Key Firewall Technology explained
- Sample customer scenarios
- OS/390 Firewall Technology Delivery
- Denial Of Service ?



IBM

© Copyright IBM Corporation, 1999

IBM Technical Support