SECURE
COMPUTING

Shared e-Business Servers
Using the 3Com Embedded Firewall

12 December 2001

Dr. Tom Haigh. CTO
haigh@securecomputing.com

SECURE
COMPUTING

Preliminaries

- Overview
  - Why use Shared Severs
  - The 3Com Embedded Firewall
  - Building Shared Servers
- Objectives of this Presentation
  - Present the solution
  - Present EFW
  - Stimulate thought on other applications

SECURE COMPUTING

E-Business Networks

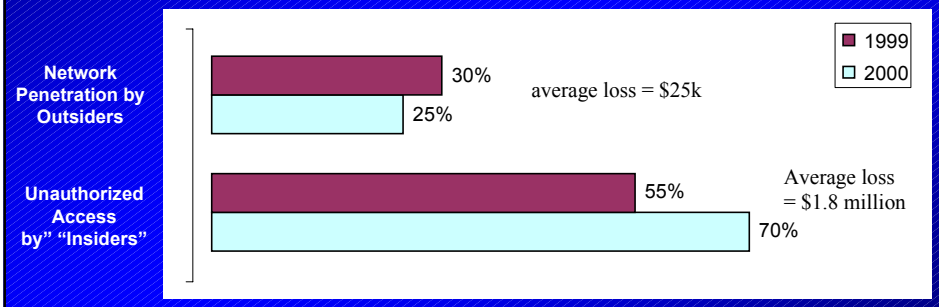
- Are changing the security paradigm
- Authorized outsiders now access internal networks
  - Must give partners timely access to the data & services they need
  - Not give them any other access
- Outsiders are becoming virtual "insiders"

SECURE COMPUTING

Insider Attacks Are Expensive

Computer Crime and Security Survey 2000

- Joint CSI/FBI survey of 643 US organizations
  - 93% with WWW sites
  - 43% provide electronic commerce services



Percentage of Companies Surveyed

SECURE COMPUTING

An "Insider" Attack

- Establish a beachhead
  - Use known attack, and
  - Legitimate access to a host on the network
- Expand the beachhead
  - Create backdoor for easy return
  - Import tools, like a sniffer
  - Erase the audit records
- Monitor traffic for passwords and names/addresses of interesting hosts
- Utilize weak authentication and access controls to jump to other hosts or networks that trust the one you cracked
- Launch the real attack

SECURE COMPUTING

The Need for a New Access Control Solution

- Perimeter firewalls cannot control "insider" threats
- Operating system security is notoriously weak/complex
- Application layer access control relies on the host OS
- Need something inside the network that is independent of the host OS

SECURE COMPUTING

Embedded Firewall

SECURE COMPUTING

DARPA

3com

SCC software
- Modified NIC firmware
- Centralized policy management

3Com COTS 3CR990 NIC
- IPSec 3DES encryption
- ARM 9 processor

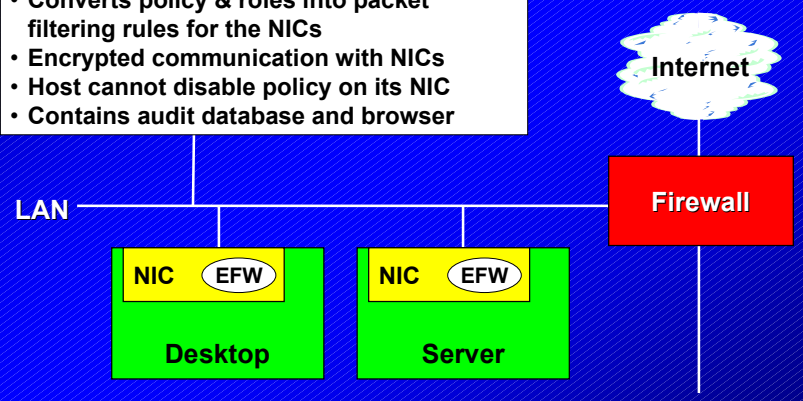
- New approach to network security
- Addresses needs of complex, partner networks

SECURE COMPUTING

EFW Architecture

Mgmt Station (GUI)

Policy Server
- Converts policy & roles into packet filtering rules for the NICs
- Encrypted communication with NICs
- Host cannot disable policy on its NIC
- Contains audit database and browser



Secure Computing Confidential

SECURE COMPUTING

EFW Client Functions

- Only accepts configuration data from encrypted channel with the Policy Server
- Filters on:
  - Source/Destination IP addresses & Port Ranges
  - IP protocols & subnet masks
  - Direction (transmit/receive)
  - TCP initiation vs. accept
- Controls for:
  - Non-IP traffic
  - Fragmented packets
  - Packet sniffing
  - IP spoofing
- Actions:
  - Allow packet, Allow & Audit packets
  - Deny (drop) packet, Deny & Audit packets

SECURE COMPUTING

EFW Policy Server

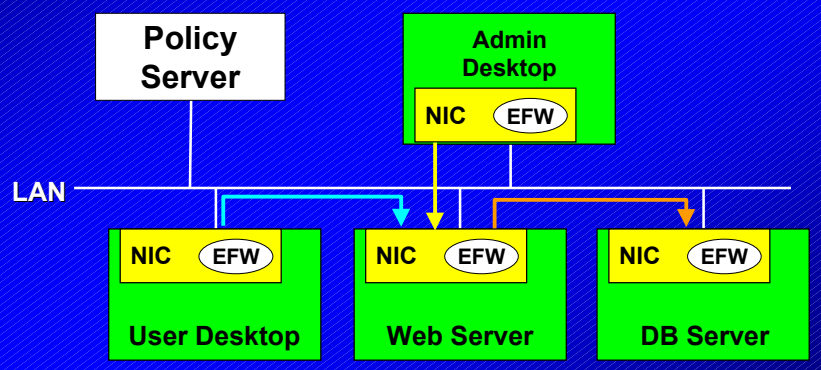
- Provides the policy and audit GUI
  - Filter mode. Enforces the packet filter rules
  - Test mode. Flags packets that matched the packet filter rule, but allows them to pass
- Uses a SQL database for storing policy and audit data
- Runs on Windows 2000 and NT
- Linux port underway
- Up to 3-way replication for fault tolerance

SECURE COMPUTING

Example 1

Web Server NIC:

- Accepts only HTTP from User Desktop(s)
- Initiates only SQL to DB server
- Accepts only SSH/telnet from Admin Desktop

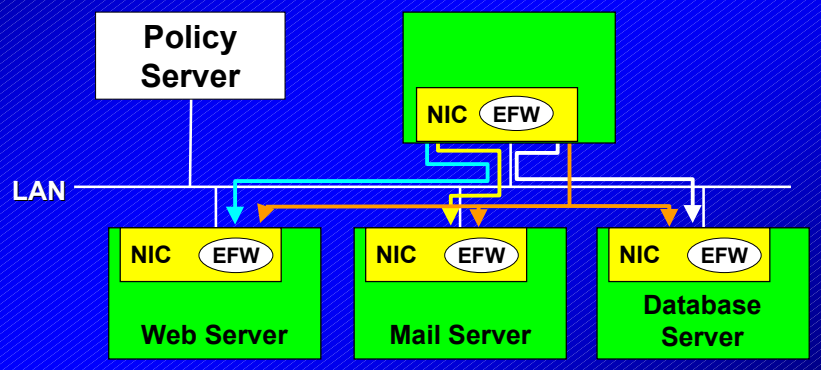


SECURE COMPUTING

Example 2

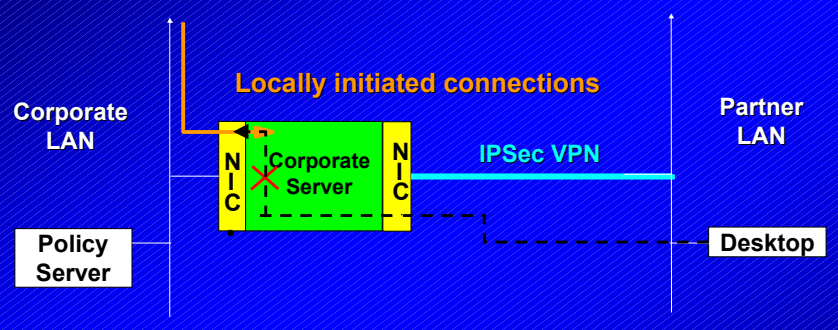
Admin Desktop NIC:

- Initiates SSH/telnet to all servers
- Initiates POP to Mail Server
- Initiates SQL to Database Server
- Initiates HTTP to Web Server
- Accepts nothing from anywhere else



SECURE COMPUTING

Example 3 – Shared Server



- Only allow IPSec connections on external NIC
- Do not allow shared server to initiate inbound connections to the corporate LAN

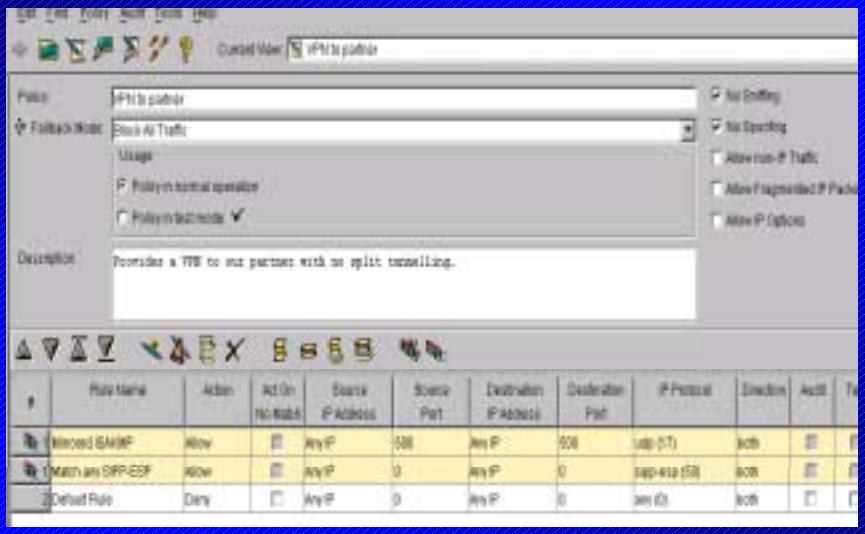
SECURE COMPUTING

Benefits of Shared Servers

- Employees and partners share same data
  - No synchronization or latency issues
  - Rapid update and response
- Tighter control of partner activities
  - Significantly reduced risk of attacks on internal network
  - DMZ in a box
- Tighter control of employee activities
- Less load on perimeter firewalls

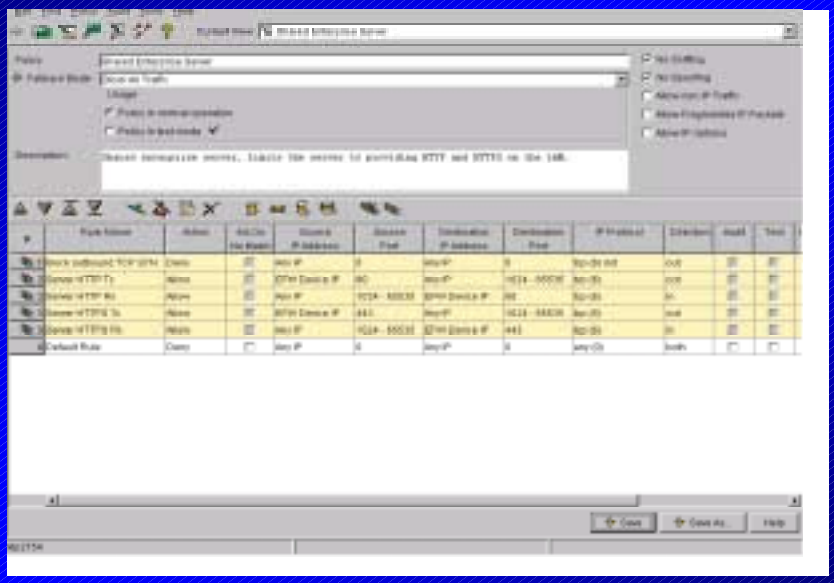
SECURE
COMPUTING

Configuring the External NIC



SECURE
COMPUTING

Configuring the Internal NIC



SECURE
COMPUTING

Conclusion

- Organizations need better controlled sharing with partners
- Shared Server using 3Com EFW is the solution
  - Robust, unbypassable security technology
  - Affordable and scalable
  - Provides timely access to most current data
  - Prevents partner from using legitimate access to mount an attack
  - Easy to distribute, configure, and manage

SECURE
COMPUTING

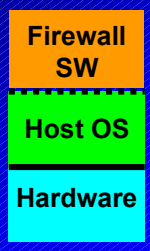
Questions?

Thanks!

SECURE COMPUTING

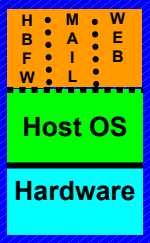
EFW vs. Host Based FWs

Perimeter Firewall



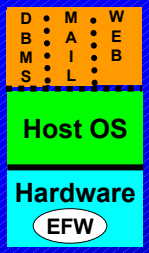
- No interference from other apps
- Interference by OS is possible
- Unbypassable entry point to network

Host-Based Firewall



- Interference from other apps or the OS can occur
- Apps can bypass FW

Embedded Firewall



- No interference from apps or OS
- Unbypassable entry point to host