

Shared e-Business Servers Using the 3Com Embedded Firewall

12 December 2001

Dr. Tom Haigh, CTO
haigh@securecomputing.com

Preliminaries

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

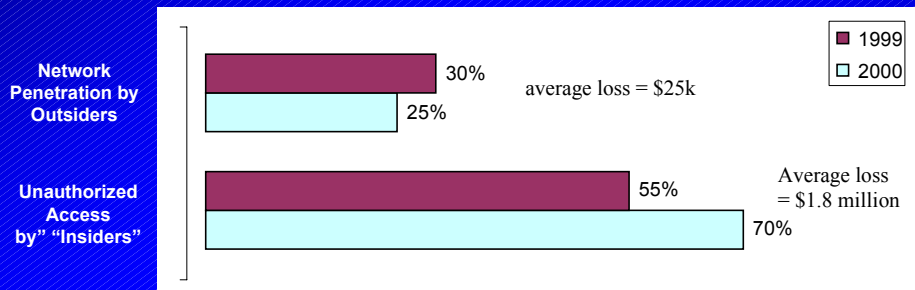
E-Business Networks

- 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”

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

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


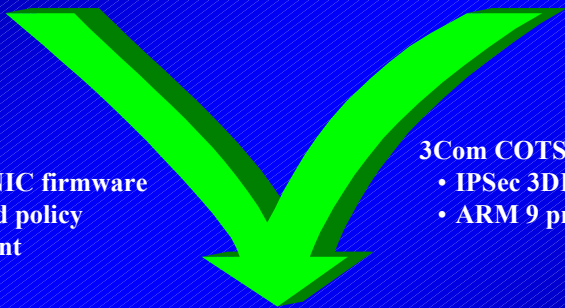
The Need for a New Access Control Solution

- 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

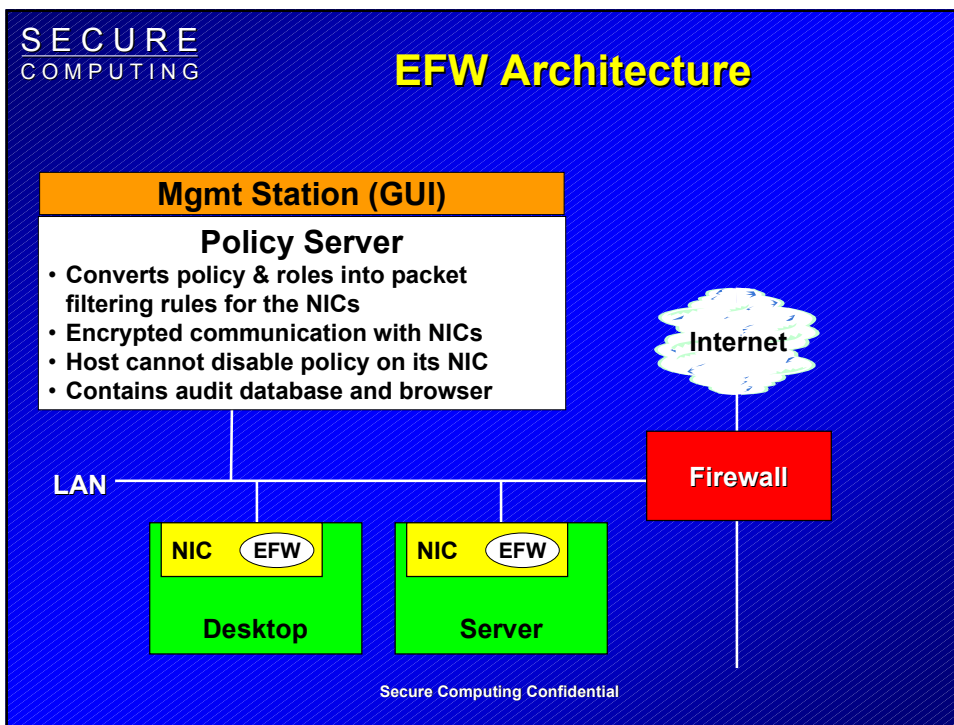
SCC software

- 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



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

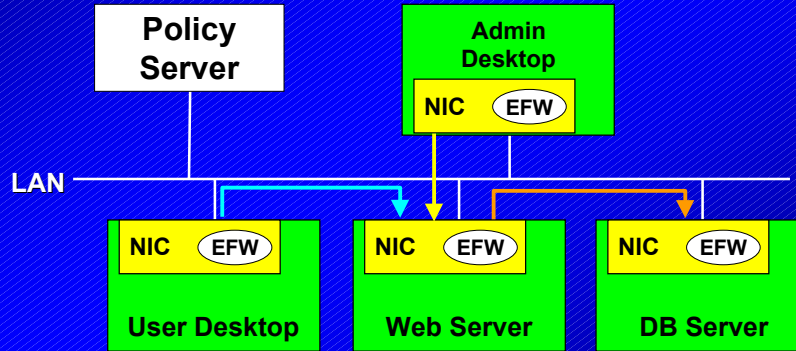
EFW Policy Server

- 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

Example 1

Web Server NIC:

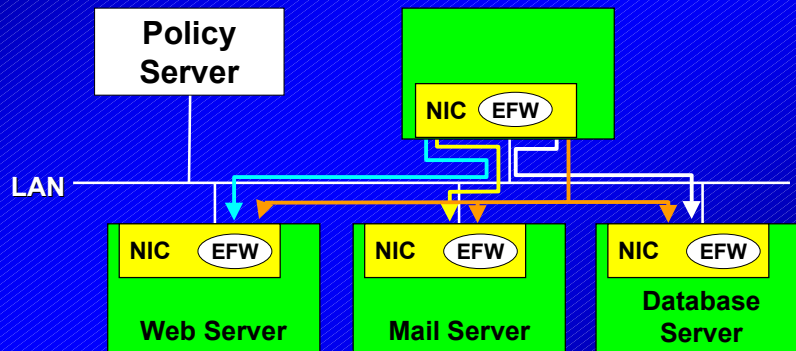
- Accepts only HTTP from User Desktop(s)
- Initiates only SQL to DB server
- Accepts only SSH/telnet from Admin Desktop



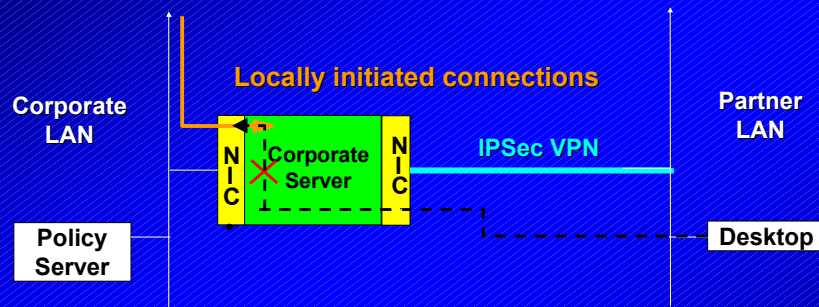
Example 2

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



Example 3 – Shared Server



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

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**

Configuring the External NIC

Policy: iPTB to partner

Fallback Mode: Drop all traffic

Usage:

- Policy normal operation
- Policy in bridge mode

Description: Provides a TB to our partner with no split tunneling.

#	Rule Name	Action	Action Name	Source IP Address	Source Port	Destination IP Address	Destination Port	IP Protocol	Outgoing Interface	Outgoing Action	Test
1	Block SMTP	Allow		Any IP	25	Any IP	25	tcp (5)	out		
2	Match an SMTP	Allow		Any IP	0	Any IP	0	tcp (5)	out		
3	Default Rule	Deny		Any IP	0	Any IP	0	any (0)	out		

Configuring the Internal NIC

Policy: Block incoming SMTP

Fallback Mode: Drop all traffic

Usage:

- Policy normal operation
- Policy in bridge mode

Description: Block incoming SMTP. Update the source of porting SMTP and SMTPS on the LAN.

#	Rule Name	Action	Action Name	Source IP Address	Source Port	Destination IP Address	Destination Port	IP Protocol	Outgoing Interface	Outgoing Action	Test
1	Block incoming SMTP	Deny		Any IP	0	Any IP	0	tcp (5)	out		
2	Deny SMTP To	Deny		SMTP Client IP	25	Any IP	25-255	tcp (5)	out		
3	Deny SMTP To	Deny		Any IP	25-255	SMTP Client IP	25	tcp (5)	out		
4	Deny SMTP To	Deny		SMTP Client IP	25	Any IP	25-255	tcp (5)	out		
5	Deny SMTP To	Deny		Any IP	25-255	SMTP Client IP	25	tcp (5)	out		
6	Default Rule	Deny		Any IP	0	Any IP	0	any (0)	out		

Conclusion

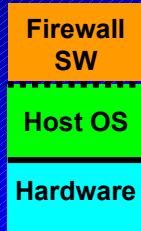
- **Organizations need better controlled sharing with partners**
- **Shared Server using 3Com EFW is the solution**
 - Robust, unbyassable security technology
 - Affordable and scalable
 - Provides timely access to most current data
 - Prevents partner from using legitimate access to mount an attack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

Questions?

Thanks!

EFW vs. Host Based FWs

Perimeter Firewall



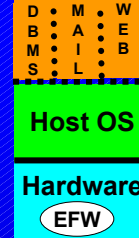
- No interference from other apps
- Interference by OS is possible
- Unbypassable entry point to network

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