



E-Certify

Network

Security

Assessment

Prepared For
E-Commerce Inc.

August 20, 1999

Table of Contents



Chapter 1	Executive Summary	
	Systems Analyzed	1 - 1
	Findings	1 - 2
	Mitigating Risk	1 - 3
Chapter 2	Internet Security	
	Internet Architecture Overview	2 - 2
	PIX Firewall	2 - 2
	PIX Overview	2 - 3
	PIX Physical Security	2 - 3
	PIX Operating System Security	2 - 3
	Telnet Access Allowed for All Hosts — ●●●	2 - 4
	PIX Configuration Security	2 - 4
	CheckPoint FireWall-1	2 - 4
	FireWall-1 Overview	2 - 5
	FireWall-1 Physical Security	2 - 6
	FireWall-1 Operating System Security	2 - 6
	ToolTalk Enabled — ●●●	2 - 6
	Sendmail Enabled — ●●●	2 - 6
	Administrators Use Telnet to Access Server — ●●●	2 - 6
	Insecure File Permissions — ●●	2 - 7
	Excessive Services Enabled — ●	2 - 7
	Remote Root Logins Allowed — ●	2 - 7
	Log Files Not Reviewed/Archived/Rotated — ●	2 - 7
	FireWall-1 Configuration Security	2 - 7
	IP Spoofing not Configured — ●●●	2 - 7
	Weak Policy Properties — ●●●	2 - 8
	Weak Security Policy — ●●●	2 - 10

Log Files not Reviewed/Archived/Rotated — 🚫🚫🚫	2 - 11
Internet Routers	2 - 11
Internet Router Overview	2 - 12
Internet Router Physical Security	2 - 12
Internet Router Configuration	2 - 12
Telnet Enabled: rt-bk — 🚫🚫🚫	2 - 13
IP Spoofing not Configured: rt-pr, rt-bk — 🚫🚫🚫	2 - 13
Excessive Services Enabled: rt-bk — 🚫🚫	2 - 14
DMZ Servers	2 - 14
DMZ Overview	2 - 15
Maple Physical Security	2 - 15
Maple Operating System Security	2 - 16
Old Operating System Version — 🚫🚫🚫	2 - 16
Tootalk Enabled — 🚫🚫🚫	2 - 16
SNMP Enabled — 🚫🚫🚫	2 - 17
Sendmail Enabled — 🚫🚫🚫	2 - 17
No Additional Security Software Installed — 🚫🚫🚫	2 - 18
Administrators Use Telnet to Access Server — 🚫🚫🚫	2 - 18
Excessive DNS Information — 🚫	2 - 19
Excessive Services Enabled — 🚫	2 - 19
Remote Root Logins Allowed — 🚫	2 - 20
Log Files not Reviewed/Archived/Rotated — 🚫	2 - 21
Maple User Accounts Security	2 - 21
Weak Passwords — 🚫🚫🚫	2 - 21
No Password Policy — 🚫🚫	2 - 21

Chapter 3 Extranet Security

Extranet Architecture Overview.	3 - 2
Extranet Servers	3 - 3
Extranet Server Overview	3 - 3
Palm Physical Security	3 - 4
Palm Operating System Security	3 - 4
Old Version of the Operating System — 🚫🚫🚫	3 - 5
No Additional Security Software Installed — 🚫🚫🚫	3 - 5
Excessive Services Enabled — 🚫🚫🚫	3 - 5
Sendmail Enabled — 🚫🚫🚫	3 - 6
Insecure File Permissions — 🚫🚫🚫	3 - 6
Insecure Setuid Programs Installed — 🚫🚫🚫	3 - 6
Administrators Use Telnet to Access Server — 🚫🚫🚫	3 - 6
Log Files Not Being Reviewed/Archived/Rotated — 🚫	3 - 7

Remote Root Logins Allowed — 🚩	3 - 7
Palm User Account Security	3 - 7
Weak Passwords — 🚩🚩🚩	3 - 7
No Password Policy — 🚩🚩🚩	3 - 7
Unnecessary User Accounts — 🚩🚩	3 - 7
Too Many People With Administrator Access — 🚩🚩	3 - 8
Palm Application Security	3 - 8
Application Directly Accessing Internal Server — 🚩🚩🚩	3 - 8
Database Login and Password Stored in Clear Text — 🚩🚩🚩	3 - 9
Database Login has too Many Privileges — 🚩🚩🚩	3 - 9
Insecure Session ID's — 🚩🚩🚩	3 - 9
Session Timeout Too Long — 🚩🚩	3 - 9
Database Password Same As Administrator Password — 🚩🚩	3 - 10
Database Stores Unencrypted Sensitive Information — 🚩🚩	3 - 10
Server Co-located with an Internet HTTP Server — 🚩🚩	3 - 10
Insufficient Application Logging — 🚩	3 - 10
No Formal Policy For Granting/Rejecting Application Access — 🚩	3 - 10
Palm Netscape Service	3 - 10
Insecure CGI Programs Installed — 🚩🚩🚩	3 - 11
Setuid CGI Programs Installed — 🚩🚩🚩	3 - 11
Old Software Versions — 🚩🚩🚩	3 - 11
Open Administration Port — 🚩🚩🚩	3 - 12
Weak SSL encryption Allowed — 🚩🚩	3 - 12
Weak Administrator Password — 🚩🚩	3 - 12
Too Many People with Administrator Access — 🚩🚩	3 - 12
Administration Server Always Running — 🚩🚩	3 - 12
Insufficient Monitoring Of Server Availability — 🚩🚩	3 - 12
Log files not Being Reviewed/Archived/Rotated — 🚩🚩	3 - 13
Partner Network Security	3 - 13
Partner Network Overview	3 - 14
Partner Network Physical Security	3 - 14
Partner Network Connected inside the PIX Firewall — 🚩🚩🚩	3 - 15
Partner Network Connected to Remote Office Router — 🚩🚩🚩	3 - 15
Partner Network Dial-in Access Security	3 - 15

Chapter 4

Intranet Security

WAN.	4 - 1
-------------	--------------

LAN	4 - 2
NT Servers	4 - 2
NT Server Overview	4 - 3
NT Physical Security	4 - 4
Unrestricted Physical Access to Server: cardinal — ●●●●	4 - 4
Server's Case is not Secured: all servers — ●●●●	4 - 4
Floppy Drive Available for Boot: all servers — ●●●●	4 - 4
Power Switch not Covered: all servers — ●●●●	4 - 4
No Power-on BIOS-Protect Passwords: all servers — ●●●●	4 - 4
NT File System Security	4 - 5
FAT File System Being Used: cardinal — ●●●●	4 - 5
User Data on the System Partition: cardinal, cedar — ●●●●	4 - 5
NTFS Permissions not Properly Applied: all servers — ●●●●	4 - 5
Administrative Shares Enabled: redwood — ●●●	4 - 5
User Permissions not Set Properly: cardinal — ●●●	4 - 5
Files Still Present in %systemroot%\repair: all servers — ●●●	4 - 6
NT Operating System Security	4 - 6
Current Service Packs and Hot Fixes not Installed — ●●●●	4 - 7
Passwords Cracked from SAM: all servers — ●●●●	4 - 7
Remote Access to Registry Enabled: all servers — ●●●●	4 - 8
Trust Relationships not Secure — ●●●●	4 - 9
Caching of Logon Credentials Enabled: all servers — ●●●	4 - 9
Anonymous Network Access Enabled: all servers — ●●●	4 - 9
Unneeded Network Services Running: cedar — ●●●	4 - 9
Services Bound to External Network Cards: pine — ●●●	4 - 10
Unneeded Protocols Installed in the System: cedar — ●●●	4 - 10
Last Logged on User Name Displayed: all servers — ●●	4 - 10
Computer Visible from Browser: redwood, pine, acorn — ●●	4 - 10
System Page File not Cleared at Shutdown: all servers — ●●	4 - 10
No Port Restrictions: all servers — ●●	4 - 10
Logs Set to Default: all servers — ●●	4 - 10
Guest Access to Event Logs: all servers — ●●	4 - 10
No Legal Warning displayed at Logon: all servers — ●●	4 - 11
No Auditing Enabled: all servers — ●●	4 - 11
NT User Account Security	4 - 11
No Account Restrictions — ●●●●	4 - 11
Passwords Never Expire — ●●●●	4 - 12
Account Lockout not Set — ●●●●	4 - 12
Lockout Duration not Set — ●●●	4 - 12
Minimum Password Length not Set — ●●●	4 - 13
Administrator Name Still Active — ●●●	4 - 13
NT Dial-in Access Security	4 - 13
Modems not Properly Documented — ●●●●	4 - 13
No RAS Auditing — ●●●	4 - 14

RAS Access Granted to Unnecessary User Accounts — 🚫🚫	4 - 15
Restrictive Hours not Set for Remote Users — 🚫🚫	4 - 15
Weak Remote User Passwords — 🚫🚫	4 - 15
Microsoft Encrypted Authentication not Required — 🚫🚫	4 - 15
Microsoft Windows NT 128 bit not Installed — 🚫🚫	4 - 15
128 Bit Service Pack not Installed— 🚫🚫	4 - 15
RAS Dial Back not Enabled — 🚫	4 - 16
PPTP Not in Use — 🚫	4 - 16
Third Party Authentication not in Use — 🚫	4 - 16
Novell Netware Server4 - 16
Novell Server Overview	4 - 17
Novell Physical Security	4 - 17
Unrestricted Physical Access to Server — 🚫🚫🚫	4 - 17
Server's Case is Not Secured — 🚫🚫🚫	4 - 18
Floppy Drive Available for Boot — 🚫🚫🚫	4 - 18
Power Switch not Covered — 🚫🚫🚫	4 - 18
No Power-on BIOS-Protect Passwords — 🚫🚫🚫	4 - 18
Novell File System Security	4 - 18
Root Access of Volume Granted to Users — 🚫🚫🚫	4 - 18
All Users Have Access to Public Directory — 🚫🚫🚫	4 - 19
Data being Stored on SYS Volume — 🚫🚫	4 - 19
Print Queues in Use on SYS Volume — 🚫🚫	4 - 19
Inherited Rights Filters not Set Properly — 🚫	4 - 19
Novell Operating System Security	4 - 19
NDS not Patched — 🚫🚫🚫	4 - 20
NetWare OS not Patched — 🚫🚫🚫	4 - 20
Year 2000 Patches not Applied — 🚫🚫🚫	4 - 20
Secure.ncf not in Use — 🚫🚫🚫	4 - 20
NWADMIN not Protected — 🚫🚫🚫	4 - 20
RCONSOLE Encryption not in Use — 🚫🚫	4 - 20
RCONSOLE not Protected — 🚫🚫	4 - 20
NLM's can be Loaded Remotely — 🚫🚫	4 - 20
Inappropriate Rights Set on NDS Objects — 🚫	4 - 21
Multiple NDS Trees Present — 🚫	4 - 21
Novell User Accounts Security	4 - 21
Cracked 70% of Passwords — 🚫🚫🚫	4 - 21
No Lockout Set — 🚫🚫	4 - 21
No Password Length Restriction — 🚫🚫	4 - 21
Users Have Rights at Root of Tree — 🚫🚫	4 - 22
No Password History— 🚫	4 - 22
Unix Production Servers4 - 22
Unix Server Overview	4 - 23
Unix Physical Security	4 - 23

Unix File System Security	4 - 24
Unix Operating System Security.	4 - 24
Unrestricted NFS Exports: juniper — ●●●	4 - 24
Vulnerable X-Window Configuration: cypress — ●●●	4 - 24
Tooltalk Enabled: juniper, cypress — ●●●	4 - 24
Trust Relationship Configured: cypress — ●●●	4 - 25
SNMP Enabled: juniper: cypress — ●●●	4 - 25
Calendar Service Enabled: juniper, cypress — ●●●	4 - 25
Sendmail Enabled: juniper — ●●●	4 - 25
Excessive Services Enabled: juniper, cypress — ●	4 - 25
Unix User Account Security	4 - 25

Executive Summary

E-Certify is pleased to provide this Network Vulnerability Analysis to the E-Commerce MIS staff. During the past three weeks, the E-Certify team assessed and analyzed E-Commerce's network systems and discovered a large number of vulnerabilities. This chapter summarizes our vulnerability findings. Chapters 2 - 4 provide technical details and recommendations to fix these vulnerabilities.

This chapter covers these topics:

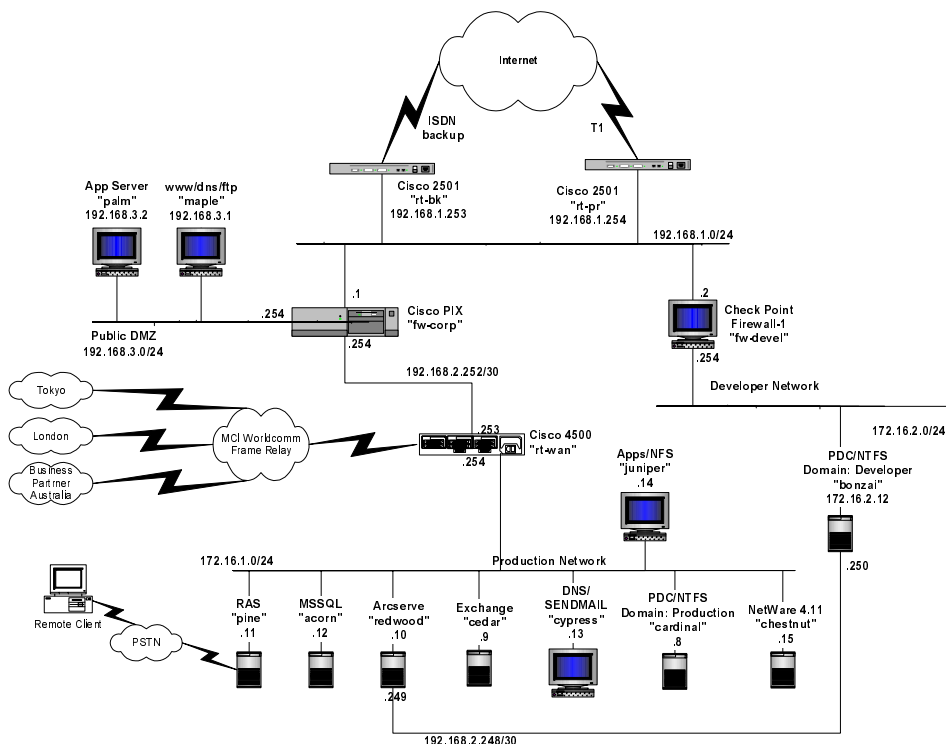
- Systems Analyzed
- Findings
- Mitigating Risk

Systems Analyzed

Based on requirements listed in the Statement of Work, E-Certify focused the analysis on the following E-Commerce information systems:

- Wide Area Network Architecture
- Extranet Access Systems and Architecture
- Remote Access Systems and Architecture
- Local Area Network Architecture
- Firewall Systems and Architecture
- Unix, NT, and Novell Servers

The following Server diagram illustrates the architecture and components assessed in this report.



Findings

The following bullets summarize our findings:

- 🚨🚨🚨 or “High Risk” - E-Certify discovered **69** high vulnerabilities that will allow an intruder to immediately gain privileged access—sysadmin or root—to the system. For example, the intruder could send a sequence of instructions to a computer and the computer responds with a command prompt.
- 🚨🚨 or “Medium Risk” - E-Certify discovered **41** medium security vulnerabilities that will allow an intruder immediate access to the system, though in an unprivileged state. This access, however, allows the intruder the opportunity to continue attempts to gain root access. For example, a configuration error could allow an intruder to capture the password file.

- 🚫 or “Low Risk” - E-Certify discovered **26** nominal security vulnerabilities that provide information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DOS) attack. Note that while a DOS attack is considered low from a threat potential, this attack’s frequency is very high. DOS attacks against mission-critical nodes are not included in this rating, and any attack of this nature should be considered “High.”

***Note:** All of the above examples use a metaphor of compromising servers. Our assessment, however, covers more than servers; it includes network configurations, firewall configurations, and so forth.*

In sum, E-Commerce critical assets are at risk of being compromised from the Internet and also from partner networks. Further, it is possible for an Internet hacker to penetrate into partner networks through E-Commerce’s firewall. And if this event occurred, and if the business partner’s critical assets were compromised, E-Commerce would be vulnerable to a lawsuit, the type of which has been successfully prosecuted.

Mitigating Risk

The vulnerabilities discovered by the E-Certify team expose critical E-Commerce systems and information assets to unauthorized use, theft, and tampering. The following chapters provide recommendations to manage or eliminate our identified vulnerabilities. We highly recommend that the E-Commerce MIS staff review, approve, and implement our recommendations to ensure an effective security posture in the near future.

Additionally, maintaining an effective security posture involves creating security awareness among employees; providing the MIS staff with the necessary training and tools to detect and correct problems; and creating, maintaining, and enforcing Security Policies and Procedures. Without this follow-up, in a year your network will again be vulnerable to attack.

We also recommend that E-Commerce consider hiring a full-time security officer. This person would be responsible for all aspects regarding network and computer security. For example, this person would be responsible for verifying that our recommendations are implemented as appropriate, responsible for implementing and enforcing security policies and procedures, responsible for implementing and enforcing configuration control, and responsible for all firewall rulebase implementations and changes.

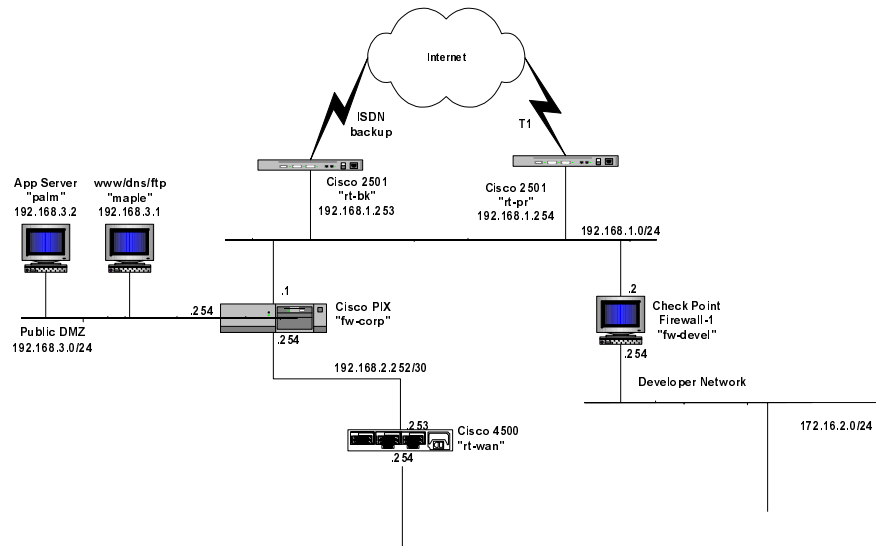
This chapter assesses the security posture of E-Commerce's Internet connection and components— firewalls, Internet routers, and DMZ servers. Having a secure Internet connection is the most important part of your enterprise security since most external attacks are initiated from this connection. By having a secure Internet connection, E-Commerce will significantly reduce exposure to a successful, external attack.

This chapter covers these topics:

- Internet Architecture Overview
- PIX Firewall
- CheckPoint FireWall-1
- Internet Routers
- DMZ Servers

Internet Architecture Overview

The following diagram illustrates E-Commerce's Internet architecture.



E-Commerce's Internet architecture is composed of PIX and CheckPoint Firewall-1 firewalls that protect the production and development networks respectively. The purpose of the PIX firewall is to protect the production network while providing partner access to an E-Commerce application in the Demilitarized Zone (DMZ).

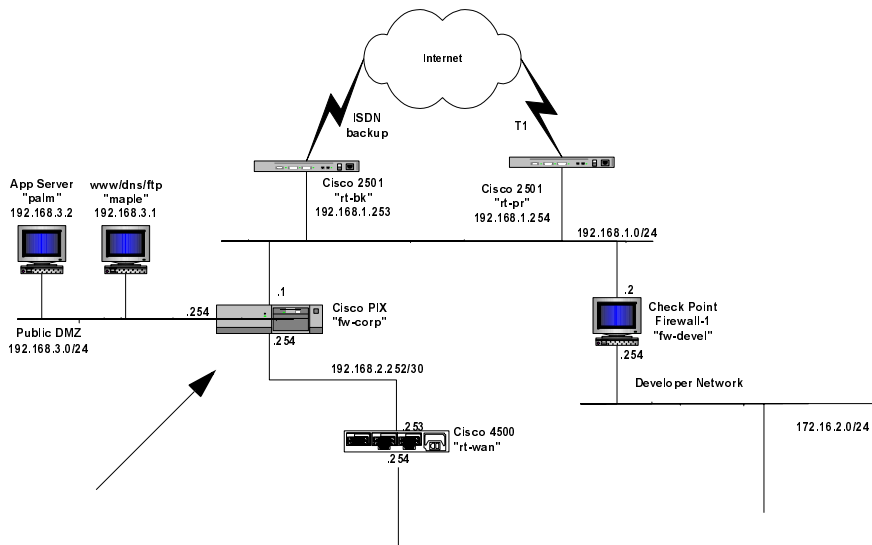
PIX Firewall

This section covers these topics:

- PIX Overview
- PIX Physical Security
- PIX Operating System Security
- PIX Configuration Security

PIX Overview

The following diagram shows the location of the PIX firewall.



The PIX firewall is connected to the internet routers and protects the Public DMZ, the partner network (Australia), the remote offices (Tokyo and London), and the Production Network. The following table details the security policy of the PIX firewall protecting the production network.

Table Deleted.

PIX Physical Security

Section Deleted.

PIX Operating System Security

We found one vulnerability relating to the PIX OS.

Telnet Access Allowed for All Hosts — ☹️☹️

Any host can telnet to the PIX firewall and attempt to login. A user could gain access by brute force against the telnet password.

Recommendation

Restrict telnet access to specific hosts if remote access is required. If remote access is not required then disable telnet access completely.

PIX Configuration Security

Section Deleted.

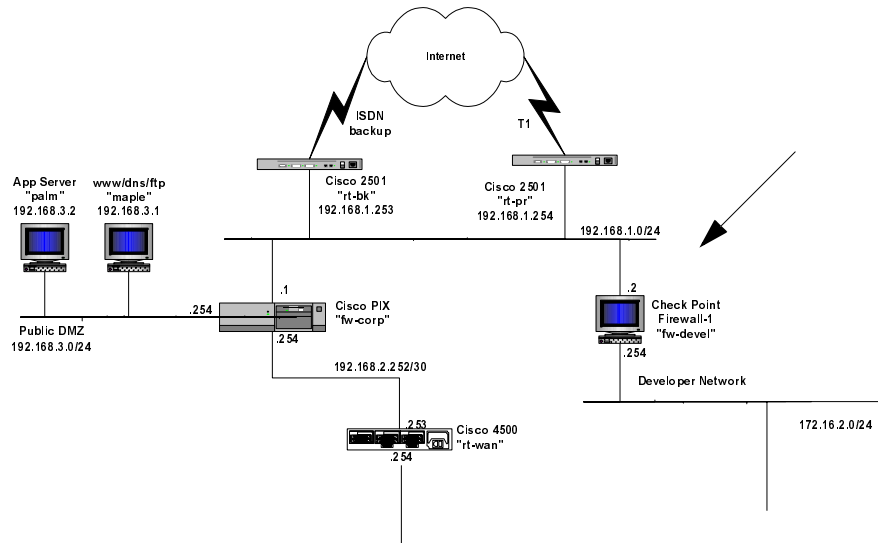
CheckPoint FireWall-1

This section covers these topics:

- FireWall-1 Overview
- FireWall-1 Physical Security
- FireWall-1 Operating System Security
- FireWall-1 Configuration Security

FireWall-1 Overview

The following diagram shows the location of the CheckPoint firewall.



The CheckPoint FireWall-1 is on a Sun Sparc system running a Solaris 2.7 operating system. The purpose of the CheckPoint firewall is to protect the development network from the Internet and provide restricted access from the production network to the development servers. The following table details the security configuration of the CheckPoint firewall protecting the development network.








Rule	Source	Destination	Service	Action
1	192.168.1.254 192.168.1.253	192.168.1.2	syslog	Accept
2	172.16.1.50 192.168.1.2	192.168.1.2 172.16.1.50	snmp, snmp-trap	Accept
3	192.168.1.100 172.16.2.101 172.16.2.100	192.168.1.2	telnet	Accept
4	172.16.2.101 172.16.2.100	192.168.3.1 192.168.3.2	telnet, ftp, http, http-admin	Accept
5	172.16.2.0/24	Any	ftp, telnet, http, https, dns	Accept
6	Any	Any	NBT	Drop
7	Any	Any	Any	Reject

FireWall-1 Physical Security

Section deleted.

FireWall-1 Operating System Security

This section covers these vulnerabilities:

- ToolTalk Enabled — 
- Sendmail Enabled — 
- Administrators Use Telnet to Access Server — 
- Insecure File Permissions — 
- Excessive Services Enabled — 
- Remote Root Logins Allowed — 
- Log Files Not Reviewed/Archived/Rotated — 

ToolTalk Enabled —

Text Deleted.

Sendmail Enabled —

Text Deleted.

Administrators Use Telnet to Access Server —

Text Deleted

Insecure File Permissions — 🚩🚩

Text Deleted.

Excessive Services Enabled — 🚩

Text Deleted.

Remote Root Logins Allowed — 🚩

Text Deleted.

Log Files Not Reviewed/Archived/Rotated — 🚩

Text Deleted.

FireWall-1 Configuration Security

The section covers these vulnerabilities:

- IP Spoofing not Configured — 🚩🚩🚩
- Weak Policy Properties — 🚩🚩🚩
- Weak Security Policy — 🚩🚩🚩
- Log Files not Reviewed/Archived/Rotated — 🚩🚩🚩

IP Spoofing not Configured — 🚩🚩🚩

IP spoofing has not been configured on the Firewall, allowing an easy way for hackers to send malicious data through the firewall by changing their source address to an E-Commerce IP address.

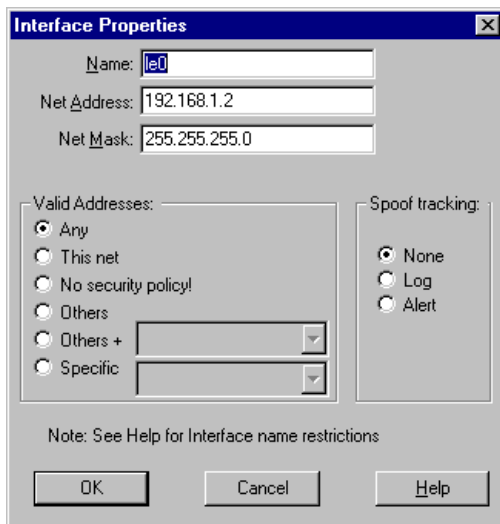
Recommendation

Enable IP Spoofing and Spoof tracking on all interfaces of the firewall. The table below reveals a typical configuration:

Interface	Valid Addresses	Spoof Tracking
le0 Internet	Others	Log
qfe1 Development Network	This network	Log

To access the IP-spoofing configuration for CheckPoint FireWall-1, Launch the Security Policy, Select Manage -> Network Objects, Highlight the firewall object, Select Edit, Select the Interfaces tab, Select the desired interface by name, Select Edit.

The below window depicts the configuration of ip-spoofing for the Internet interface of the firewall.

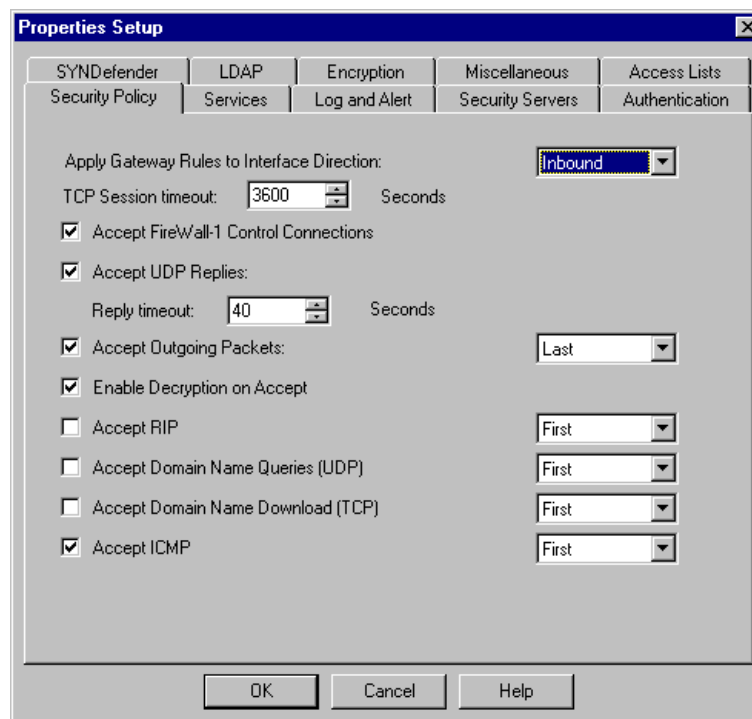


The IP Spoofing properties are not enabled on the interfaces of the CheckPoint firewall. Configuring IP Spoofing ensures that all packets inbound from the Internet that have a source address of E-Commerce’s internal network will be dropped at the firewall.

Weak Policy Properties — ☹️☹️☹️

The Default property settings for Firewall-1 have not been changed. These properties settings create openings through the firewall that create unnecessary vulnerabilities.

The next graphic reveals the configuration of the security policy properties for the CheckPoint firewall.



While reviewing the security policy of the CheckPoint firewall, we discovered settings that compromised E-Commerce's security posture.

The "Accept FireWall-1 Control Connections" allows the following ports from any system to the firewall allowing remote management: FW1 (256/tcp), FW1_clntauth (259/tcp), FW1_log (257/tcp), FW1_mgmt (258/tcp), FW1_snmp (260/udp), ISAKMP (500/udp), RDP (259/udp), SNMP (161/udp). An external intruder can exploit this vulnerability to determine the type and version of the firewall protecting the development network. Additionally, an intruder can query the system via SNMP to determine system information such as architecture, operating system version, network configuration, running processes, and Firewall-1 statistics.

Finally, The "Accept ICMP" allows an external intruder to quickly identify systems that are externally accessible.

Recommendation

The "Accept FireWall-1 Control Connections" property should be disabled and an explicit rule should be added to the security policy allowing authorized stations to administer the firewall remotely. The following rule shows an example:



The “Accept ICMP” property should be disabled and explicit rules should be created as required. Here’s an example:



Weak Security Policy — ☹☹☹

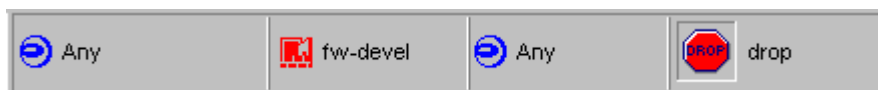
The next graphic reveals the configuration of the security policy for the CheckPoint firewall

No.	Source	Destination	Service	Action
1	rt-pr rt-bk	fw-devel	syslog	accept
2	hpov fw-devel	hpov	snmp snmp-trap	accept
3	Admin-production Admin-development	fw-devel	telnet	accept
4	bob-wk joe-wk	maple palm	telnet ftp http http-admin	accept
5	net-development	Any	ftp telnet http https dns	accept
6	Any	Any	NBT	drop
7	Any	Any	Any	reject

The security policy implemented on “fw-devel”, while restrictive, allows internal systems access to the firewall. Access to the firewall is allowed by rules one through three; access is restricted to authorized systems for a specific services. The intention of rule five is to allow systems on the development network access to the Internet. In addition to Internet access the internal systems are allowed access to the firewall for the specified services.

Recommendation

The following rule should be added to the security policy between rules three and four to implement the intended access to the firewall. The following rule is the stealth rule:



Log Files not Reviewed/Archived/Rotated — 🚫🚫🚫

Text Deleted.

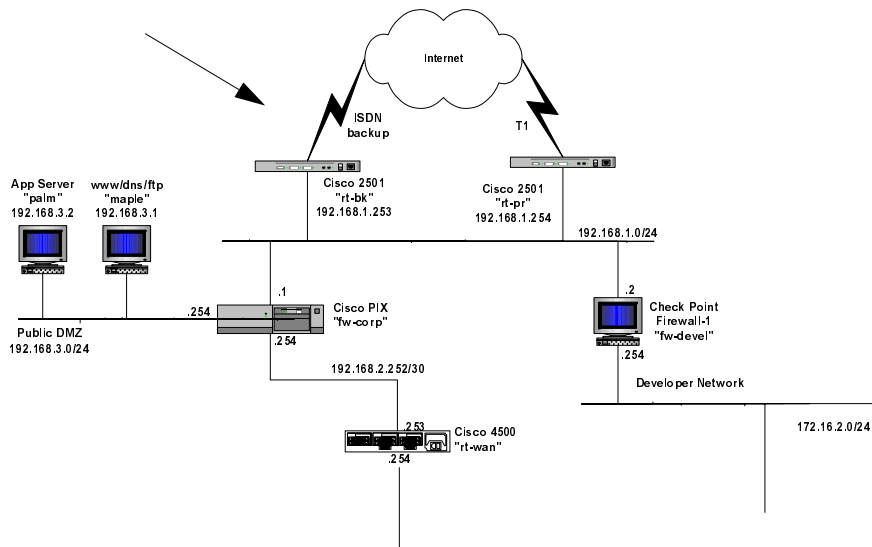
Internet Routers

This section covers these topics:

- Internet Router Overview
- Internet Router Physical Security
- Internet Router Configuration

Internet Router Overview

The Internet routers are connected to the PIX firewall as shown in the following diagram.



Internet Router Physical Security

Section deleted.

Internet Router Configuration

This section covers these vulnerabilities:

- Telnet Enabled: rt-bk — 🚫🚫🚫
- IP Spoofing not Configured: rt-pr, rt-bk — 🚫🚫🚫
- Excessive Services Enabled: rt-bk — 🚫🚫

Telnet Enabled: rt-bk — ●●●

The Internet backup router does not restrict telnet access of the router to authorized systems only. An external intruder at most has the potential of gaining administrative control of the router and at least the ability to identify this system as a Cisco router. Administrative control can be obtained by attempting to guess the administrative passwords. This guessing is considered a brute force attack and success is determined by the strength of the passwords.

Recommendation

Restrict telnet access by applying an Access List (ACL) to the administrative vtys. Below is an example ACL:

```
ip access-list 12 permit 192.16.1.100 0.0.0.0
```

Apply the access-list to the vtys by adding the following line after the vty definitions.

```
ip access-class 12 in
```

IP Spoofing not Configured: rt-pr, rt-bk — ●●●

The Internet routers do not implement ACLs preventing an external intruder from successfully spoofing E-Commerce's Internet addresses. Configuring ACLs that prevent IP Spoofing would ensure that all packets inbound from the Internet that have a source address within E-Commerce's Internet range would be dropped by the routers.

Recommendation

Enable IP Spoofing by applying ACLs on the serial interfaces connecting to the Internet Service Provider (ISP). Below is an example ACL:

```
ip access-list 101 deny ip 192.168.1.0 0.0.0.255 any
ip access-list 101 deny ip 192.168.2.0 0.0.0.255 any
ip access-list 101 deny ip 192.168.3.0 0.0.0.255 any
ip access-list 101 allow ip 0.0.0.0 0.0.0.0 any
```

Apply the access-list to the external interface:

```
ip access-group 101 in
```

Excessive Services Enabled: rt-bk — 🌟🌟

Cisco routers enable the finger, tcp-small and udp-small services unless they are explicitly disabled. These services when enabled allow an external intruder to identify this system as a Cisco router.

Recommendation

Disable these services by adding the following lines to the Cisco configuration.

```
no service finger
no service tcp-small-servers
no service udp-small-servers
```

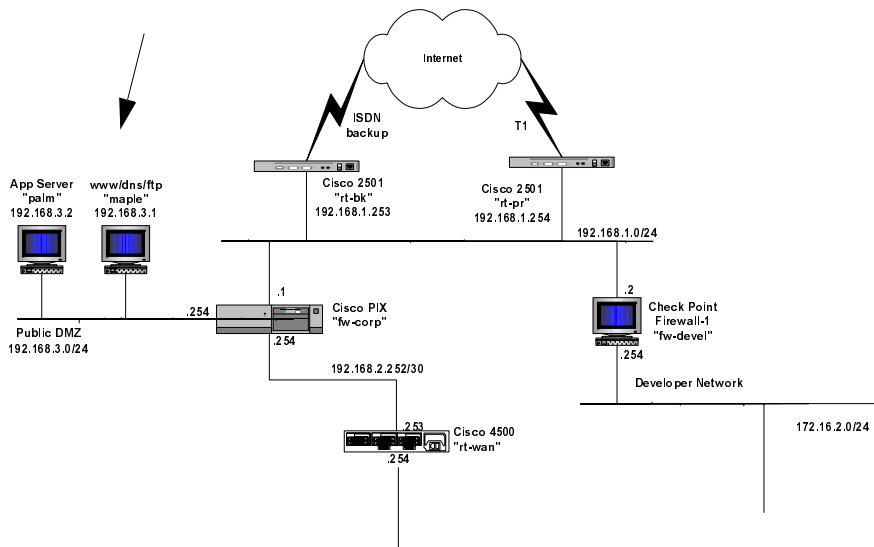
DMZ Servers

This section covers these topics:

- Maple Physical Security
- Maple Operating System Security
- Maple User Accounts Security

DMZ Overview

The DMZ servers are connected to the PIX firewall as shown in the following diagram.



The primary function of this network is to support E-Commerce business partners and provide the basic services needed to work securely over the Internet. The following table details the systems located in the DMZ and their function.

System	IP Address	Function
Maple	192.168.3.1	Company Web Server Company FTP Server Public DNS
Palm	192.168.3.2	E-Commerce Application Server

Note: The assessment for the server Palm is in the Extranet Chapter 3.

Maple Physical Security

Section deleted.

Maple Operating System Security

This section covers these vulnerabilities:

- Old Operating System Version — 🚩🚩🚩
- Tooltalk Enabled — 🚩🚩🚩
- SNMP Enabled — 🚩🚩🚩
- No Additional Security Software Installed — 🚩🚩🚩
- Sendmail Enabled — 🚩🚩🚩
- Administrators Use Telnet to Access Server — 🚩🚩🚩
- Excessive DNS Information — 🚩
- Excessive Services Enabled — 🚩
- Remote Root Logins Allowed — 🚩
- Log Files not Reviewed/Archived/Rotated — 🚩

Old Operating System Version — 🚩🚩🚩

Maple is running Solaris 2.6 with no additional patches installed. This version is out of date and has several known vulnerabilities that could compromise the system.

Recommendation

Upgrade the operating system to the latest version of Solaris (currently Solaris 7) with the latest recommended/security patches (see <http://sunsolve.sun.com>).

Tooltalk Enabled — 🚩🚩🚩

Solaris servers enable the tooltalk service unless explicitly disabled. This service when enabled could allow an intruder to gain administrative access of the server.

Recommendation

All systems located within the Internet perimeter should only have authorized services enabled. The following procedure will disable the tooltalk service.

Comment the line ending with `rpc.ttdbserverd` in the `/etc/inetd.conf` file with a pound sign `#`.

Determine the process id of the `inetd` daemon

```
# ps -ef | grep inetd
root    148      1  0 15:14:58 ?          0:00 /usr/sbin/inetd -s
root    387     380  0 15:33:29 pts/1      0:00 grep inetd
```

Restart the `inetd` daemon

```
# kill -HUP 148
```

SNMP Enabled — ☹️☹️☹️

The SNMP service is enabled during a default install of later versions of Solaris. Access to view or modify SNMP information is protected by a public and private community string. The SNMP service has a hidden community string that could allow an intruder to modify system configuration and gain system information.

Recommendation

Perform the following procedure as root to disable the SNMP service.

Stop the current SNMP daemons

```
/etc/rc3.d/S77dmi stop
/etc/rc3.d/S76snmpx stop
```

Disable the startup files

```
mv /etc/rc3.d/S77dmi /etc/rc3.d/_s77dmi
mv /etc/rc3.d/S76snmpx /etc/rc3.d/_s76snmpx
```

If SNMP services are required this vulnerability has been remedied in version 7 of the operating system and the current version of Solaris Enterprise Agents (currently SEA 1.0.3).

Sendmail Enabled — ☹️☹️☹️

The Sendmail daemon is enabled as a mailhost for a default install of Solaris. This daemon has a notorious history of allowing intruders to gain administrative access to servers.

Recommendation

Review the business requirements for configuring this server as a mailhost. The following procedure reconfigures the start up files to disable accepting remote mail and ensures delivery of local mail.

Modify the line beginning with `/usr/lib/sendmail` in the `/etc/rc2.d/S88sendmail` file.

```
/usr/lib/sendmail -bd -q15m &
```

to be

```
/usr/lib/sendmail -q5m &
```

Restart sendmail

```
/etc/rc2.d/S88sendmail stop  
/etc/rc2.d/S88sendmail start
```

No Additional Security Software Installed — ☹☹☹

Palm does not have additional security software to protect it against attacks. This means that the firewall is the only layer of protection. All Internet-accessible servers should be protected by a multi-layered security approach.

Recommendation

Here is a list of types of software that will improve the security posture of a server. We also give specific examples of open source or commercial off-the-shelf products that fall into each category. These are only examples - there are many other products that perform an equivalent function.

Install and configure the following types of software on Palm:

- Network based access control and logging, such as TCP Wrappers.
- Host based intrusion detection, such as Axent ESM.
- File integrity auditing tools, such as TripWire.

Administrators Use Telnet to Access Server — ☹☹☹

Text Deleted

Excessive DNS Information —

The following section reveals the information available to the Internet.

ecomm.com.	SOA	ns1.ecomm.com, admin.ecomm.com
ecomm.com.	NS	ns1.ecomm.com
ecomm.com.	MX	10 mail.ecomm.com
ecomm.com.	A	192.168.3.1
rt-pr	A	192.168.1.254
rt-bk	A	192.168.1.253
maple	A	192.168.3.1
palm	A	192.168.3.2
maple-sun	CN	maple
palm-sun	CN	palm
fw-corp	A	192.168.1.1
pix1	CN	fw-corp
fw-devel	A	192.168.1.2
fw1	CN	fw-devel

During our assessment, we discovered that E-Commerce's external Domain Name Service (DNS) profile contained a wealth of perimeter information. An intruder would use this information to focus penetration efforts to critical systems and help reduce the number of vulnerabilities examined to those that would be the most successful.

Recommendation

Review the business requirements for the information available through DNS and reduce the number of systems advertised.

Excessive Services Enabled —

A default installation of Solaris will enable a number of services that allow an intruder can gain administrative access, deny authorized individual's access resources, or gain system information.

Recommendation

Review the business requirements for all the services available and explicitly disable any service that is not required. Disable the services that follow unless explicitly required.

Services invoked from the `inetd` daemon: To disable these services follow the `tooltalk` recommendation procedure.

<code>ftpd</code>	<code>rlogind</code>	<code>uucpd</code>
<code>telnetd</code>	<code>rexecd</code>	<code>fingerd</code>
<code>tnamed</code>	<code>comsat</code>	<code>time</code>
<code>rshd</code>	<code>talkd</code>	<code>echo</code>
<code>discard</code>	<code>sprayd</code>	<code>kerbd</code>
<code>daytime</code>	<code>walld</code>	<code>lpd</code>
<code>chargen</code>	<code>rstatd</code>	<code>gssd</code>
<code>sadmin</code>	<code>kcms_server</code>	<code>dtspcd</code>
<code>rquotad</code>	<code>fs.auto</code>	<code>cmsd</code>
<code>rusers</code>	<code>cachefs</code>	

Services invoked on system startup: To disable these services follow the `SNMP` recommendation procedure.

`/etc/rc2.d`

<code>S47aspp</code>	<code>S75savecore</code>	<code>S85power</code>
<code>S70uucp</code>	<code>S76nsd</code>	<code>S89bdconfig</code>
<code>S72autoinstall</code>	<code>S80PRESERVE</code>	<code>S93cacheos.finish</code>
<code>S73cachefs.daemon</code>	<code>S80lp</code>	<code>S99audit</code>
<code>S73nfs.client</code>	<code>S80spc</code>	<code>S99tsquantum</code>
<code>S74autofs</code>		

`/etc/rc3.d`

`S15nfs.server`

***Remote Root Logins Allowed* — **

Text Deleted.

Log Files not Reviewed/Archived/Rotated — 🚩

Text Deleted.

Maple User Accounts Security

This section covers these vulnerabilities:

- **Weak Passwords** — 🚩🚩🚩
- **No Password Policy** — 🚩🚩

Weak Passwords — 🚩🚩🚩

Text Deleted.

No Password Policy — 🚩🚩

Text Deleted.

Extranet Security

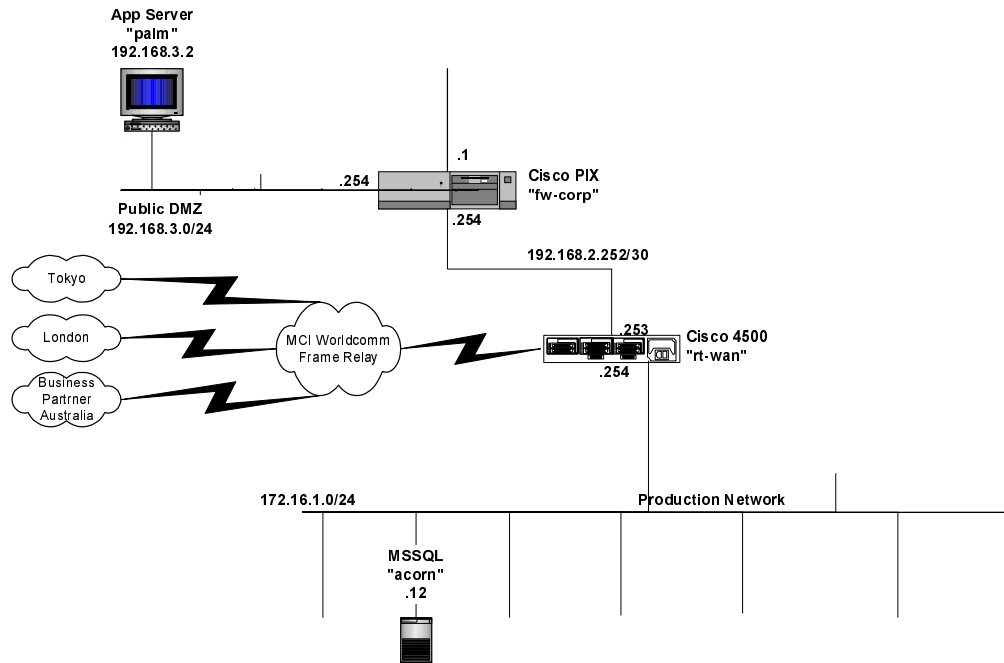
This chapter assesses the security posture of E-Commerce's extranet connections and components—servers, applications, and partner networks. We reviewed E-Commerce's extranet application and architecture and found several highly exposed vulnerabilities. These vulnerabilities can be easily fixed by updating operating systems and modifying configurations.

This chapter covers these topics:

- Extranet Server Overview
- Extranet Servers
- Palm Netscape Service
- Partner Network Security

Extranet Architecture Overview

The following diagram illustrates the E-Commerce's extranet architecture.



The extranet is composed of a Cisco 4500 series router connected to the business partner network. Connectivity is provided by a T1 connection from the Cisco 4500 into the MCI Worldcomm frame relay cloud.

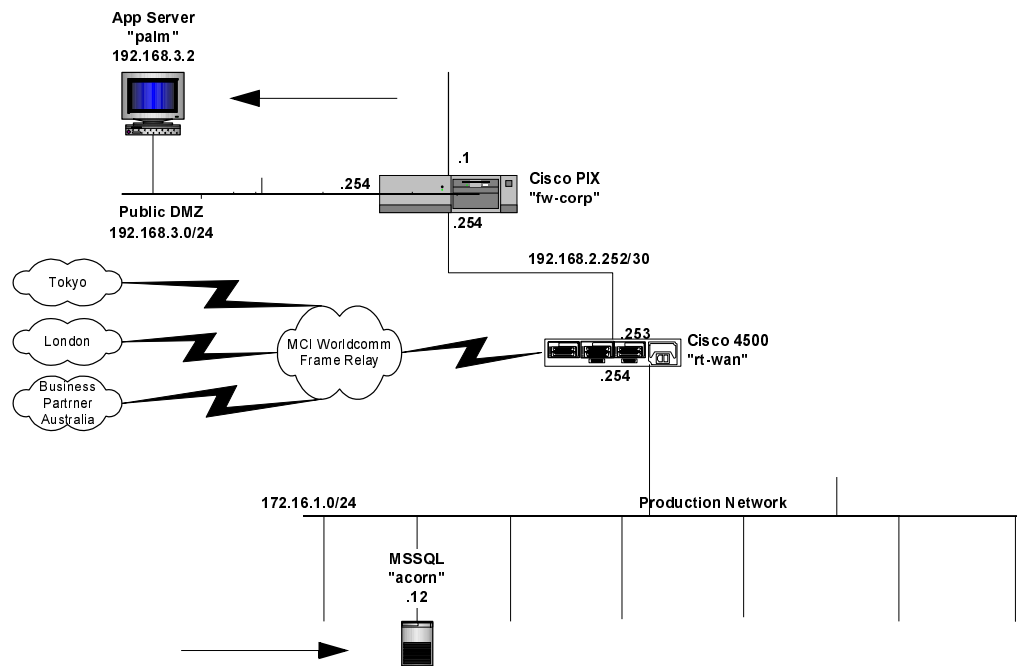
Extranet Servers

This section covers these topics:

- Extranet Server Overview
- Palm Physical Security
- Palm Operating System Security
- Palm User Account Security
- Palm Application Security

Extranet Server Overview

The following diagram reveals the location of the extranet servers.



The server Palm is a Sun Sparc architecture machine running the Solaris 2.6 operating system. It is logically located in the Public DMZ network off of the fw-corp firewall. The primary function of the server is to run an extranet application that allows particular external customers read/write access to some proprietary information housed on Acorn, the internal database server.

System	IP Address	Function
Acorn	172.16.1.12	Database Server
Palm	192.168.3.2	E-Commerce Application Server

Note: *Acorn is assessed in the Intranet Chapter 4.*

Palm Physical Security

Section Deleted.

Palm Operating System Security

This section covers these vulnerabilities:

- Old Version of the Operating System — 🚩🚩🚩
- No Additional Security Software Installed — 🚩🚩🚩
- Excessive Services Enabled — 🚩🚩🚩
- Sendmail Enabled — 🚩🚩🚩
- Insecure File Permissions — 🚩🚩🚩
- Insecure Setuid Programs Installed — 🚩🚩🚩
- Administrators Use Telnet to Access Server — 🚩🚩🚩
- Log Files Not Being Reviewed/Archived/Rotated — 🚩
- Remote Root Logins Allowed — 🚩

Old Version of the Operating System — ☹️☹️☹️

Palm is running Solaris 2.6 with no additional patches installed. This version is out of date and has several known vulnerabilities that could compromise the system.

Recommendation

Upgrade the operating system to the latest version of Solaris (currently Solaris 7) with the latest security patches (see <http://sunsolve.sun.com>). Keep informed of the latest security vulnerabilities and operating system patches by monitoring security-related web sites and mailing lists.

No Additional Security Software Installed — ☹️☹️☹️

Palm does not have additional security software to protect it against attacks. This means that the firewall is the only layer of protection. All Internet-accessible servers should be protected by a multi-layered security approach.

Recommendation

Here is a list of types of software that will improve the security posture of a server. We also give specific examples of open source or commercial off-the-shelf products that fall into each category. These are only examples - there are many other products that perform an equivalent function.

Install and configure the following types of software on Palm:

- Network based access control and logging, such as TCP Wrappers.
- Host based intrusion detection, such as Axent ESM.
- File integrity auditing tools, such as TripWire.

Excessive Services Enabled — ☹️☹️☹️

Palm is running the default configuration in `/etc/inetd.conf`. This file determines what network services are run on the system. Many of the services run by default have known vulnerabilities that could lead to a system compromise.

Recommendation

Edit /etc/inetd.conf to comment out all unnecessary services, such as:

```
comsat          rquotad        telnet
exec           rstatd         tftp
ftp            rusersd        uucp
name           sprayd         walld
netstat        systat         ypsupdated
rexd
```

To disable services:

1. vi /etc/inetd.conf
2. Insert '##' at the beginning of a line to comment out that service.
3. Save the changes and exit.
4. kill -HUP `cat /var/run/inetd.pid`

Sendmail Enabled —

Text Deleted

Insecure File Permissions —

Text Deleted

Insecure Setuid Programs Installed —

Text Deleted

Administrators Use Telnet to Access Server —

Text Deleted

Log Files Not Being Reviewed/Archived/Rotated — ●*

Text Deleted

Remote Root Logins Allowed — ●*

Text Deleted

Palm User Account Security

This section covers these vulnerabilities:

- **Weak Passwords** — ●*●*●*
- **No Password Policy** — ●*●*●*
- **Unnecessary User Accounts** — ●*●*
- **Too Many People With Administrator Access** — ●*●*

Weak Passwords — ●*●*●*

Text Deleted

No Password Policy — ●*●*●*

Text Deleted

Unnecessary User Accounts — ●*●*

Text Deleted

Too Many People With Administrator Access — 🚫🚫

Text Deleted

Palm Application Security

This section covers these vulnerabilities:

- Application Directly Accessing Internal Server — 🚫🚫🚫
- Database Login and Password Stored in Clear Text — 🚫🚫🚫
- Database Login has too Many Privileges — 🚫🚫🚫
- Insecure Session ID's — 🚫🚫🚫
- Session Timeout Too Long — 🚫🚫
- Database Password Same As Administrator Password — 🚫🚫
- Database Stores Unencrypted Sensitive Information — 🚫🚫
- Server Co-located with an Internet HTTP Server — 🚫🚫
- Insufficient Application Logging — 🚫
- No Formal Policy For Granting/Rejecting Application Access — 🚫

Application Directly Accessing Internal Server — 🚫🚫🚫

The database server acorn is located on the internal company network. Palm, which is in the public DMZ, communicates directly with acorn. A machine in the public DMZ, which is always at a higher risk of compromise, should never communicate directly with an internal network server.

Recommendation

Modify the system architecture in one of two ways:

1. Move the database server acorn into a private DMZ off of the fw-corp firewall. Communication will look like the following:

Public DMZ ↔ Private DMZ

Or

2. Employ a proxy server in a private DMZ off of the fw-corp firewall. This proxy server will talk directly with palm, and relay requests into the internal network server acorn. Communication will look like the following:

Public DMZ ↔ Private DMZ ↔ Internal network

Database Login and Password Stored in Clear Text — ☹☹☹

The database login and password is stored in an include file located under the document root of the web server. This means that if someone knows the name of the file, they can retrieve the file remotely from anywhere on the Internet.

Recommendation

Move all include files out of the document root area. Audit all files under the document root to ensure they belong there.

Database Login has too Many Privileges — ☹☹☹

The database login used by the extranet application has more privileges than necessary. It can also create and drop tables.

Recommendation

Use a database login that has the minimum privileges necessary to do the job.

Insecure Session ID's — ☹☹☹

Text Deleted

Session Timeout Too Long — ☹☹

Text Deleted

Database Password Same As Administrator Password — ☹☹☹

Text Deleted

Database Stores Unencrypted Sensitive Information — ☹☹☹

Text Deleted

Server Co-located with an Internet HTTP Server — ☹☹☹

Insufficient Application Logging — ☹

Text Deleted

No Formal Policy For Granting/Rejecting Application Access — ☹

Text Deleted

Palm Netscape Service

This section covers these vulnerabilities:

- Insecure CGI Programs Installed — ☹☹☹☹☹
- Setuid CGI Programs Installed — ☹☹☹☹☹
- Old Software Versions — ☹☹☹☹☹
- Open Administration Port — ☹☹☹☹☹
- Weak SSL encryption Allowed — ☹☹☹☹☹
- Weak Administrator Password — ☹☹☹☹☹

- Too Many People with Administrator Access — 🚩🚩
- Administration Server Always Running — 🚩🚩
- Insufficient Monitoring Of Server Availability — 🚩🚩
- Log files not Being Reviewed/Archived/Rotated — 🚩🚩

Insecure CGI Programs Installed — 🚩🚩🚩

We found several insecure CGI programs installed on the system (mailer.cgi, testmail.cgi, forward.cgi). They allow any remote user to run an arbitrary program on the server as the same user as the web server process (nobody).

Recommendation

After the Netscape Enterprise Server is installed, go back and remove all unnecessary CGI programs from the cgi-bin directory. Configure the web server to only execute CGI programs from the cgi-bin directory. Have all programmers read the document describing secure programming practices. Perform regular security reviews on all software developed in-house and installed on production systems.

Setuid CGI Programs Installed — 🚩🚩🚩

The CGI program chgpass.cgi is setuid to root. It allows users to remotely change their own password. This practice is extremely dangerous as any vulnerability in the program allows anyone on the Internet to execute an arbitrary command as root on the server.

Recommendation

The application password file does not need to be owned by root. Configure the application password file to be owned by another non-privileged user. Set the chgpass.cgi program to be setuid to that new user. Review chgpass.cgi for security vulnerabilities.

Old Software Versions — 🚩🚩🚩

Text Deleted

Open Administration Port — ●●●

Text Deleted

Weak SSL encryption Allowed — ●●

The Netscape Enterprise Server is configured to allow SSL connections of all types (40 bits, 128 bits) depending on the client browser capability. The 40-bit encryption strength is considered weak by current standards.

Recommendation

Configure Netscape to require strong encryption (128 bits) for client SSL connections. Any client browser that is not 128-bit capable will not be able to connect. The user will see a panel detailing the problem. Since all users of the extranet application are domestic to the US, this is a reasonable requirement. Provide links on a non-SSL page where users can download the domestic versions of recommended browsers.

Weak Administrator Password — ●●

Text Deleted

Too Many People with Administrator Access — ●●

Text Deleted

Administration Server Always Running — ●●

Text Deleted

Insufficient Monitoring Of Server Availability — ●●

Text Deleted

Log files not Being Reviewed/Archived/Rotated — 🚫🚫

Text Deleted.

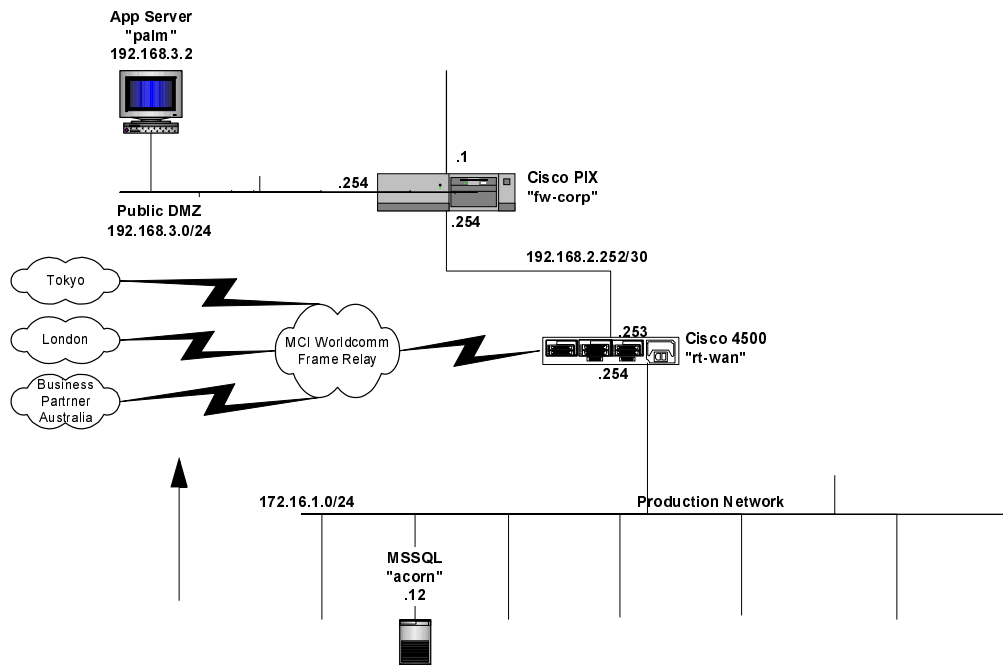
Partner Network Security

This section covers these topics:

- Partner Network Overview
- Partner Network Physical Security
- Partner Network Dial-in Access Security

Partner Network Overview

The following diagram reveals the location of the partner network.



The extranet is composed of a Cisco 4500 series router connected to the business partner network. Connectivity is provided by a T1 connection from the Cisco 4500 into the MCI Worldcomm frame relay cloud.

Partner Network Physical Security

This section covers these vulnerabilities:

- Partner Network Connected inside the PIX Firewall — ☹️☹️☹️
- Partner Network Connected to Remote Office Router — ☹️☹️☹️

Partner Network Connected inside the PIX Firewall — ☹️☹️☹️

This is a problem because the firewall cannot protect access to the Production network from the Partner network. The only device that can provide any type access control between the partner and production networks is the router which has very limited capabilities.

Recommendation

Connect the Partner network on a separate DMZ off the PIX firewall allowing it to thoroughly control access to the Production network.

Partner Network Connected to Remote Office Router — ☹️☹️☹️

The Partner network terminates on the same router as the remote locations, putting the Production/remote locations at risk. Misconfiguration of the router could open up security holes to the Production/remote networks from the partner network.

Recommendation

Use a separate router to provide connectivity to the partner network.

Partner Network Dial-in Access Security

Section Deleted.

This chapter assesses the security posture of E-Commerce's intranet connections and components—WAN, LAN, and critical servers. It is very important to have a well-defined and implemented internal security posture. All too often organizations place too much trust in their own network, yet internal network attacks are the most common.

This chapter covers these topics:

- WAN
- LAN
- NT Servers
- Novell Netware Server
- Unix Production Servers

WAN

Section deleted.

LAN

Section deleted.

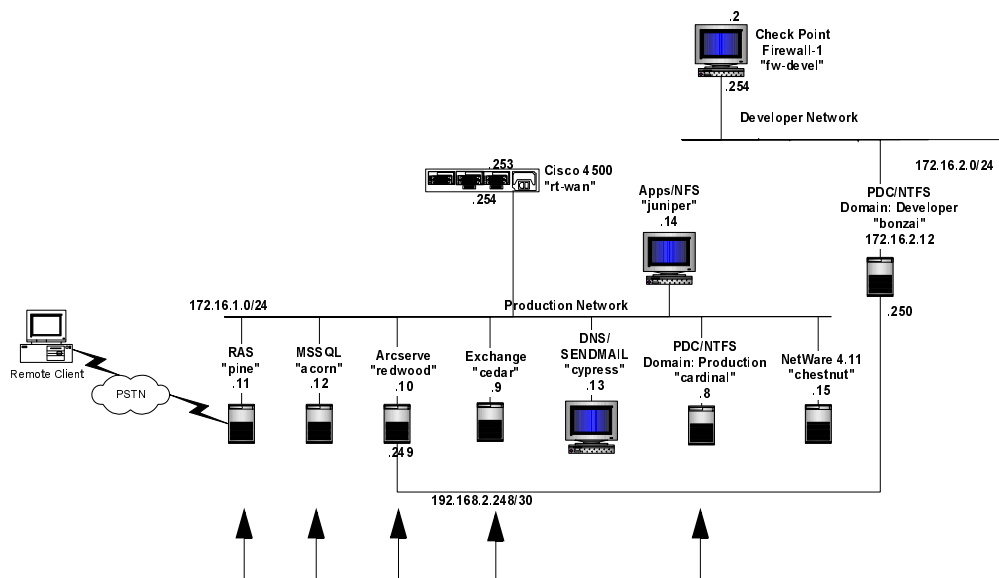
NT Servers

This section covers these topics:

- NT Server Overview
- NT Physical Security
- NT File System Security
- NT Operating System Security
- NT User Account Security
- NT Dial-in Access Security

NT Server Overview

E-Commerce is currently running five NT servers, indicated in the following diagram.



These servers offer different functionality for the internal E-Commerce network. None of E-Commerce's NT servers are accessed directly from the Internet. However, E-Commerce's servers are offering a lot of information to internal users that could be used to gain access to protected areas of the servers.

The following table summarizes the services offered by these servers.

Server	Services Offered
cardinal (Primary Domain Controller)	User Accounts, Print Services, Logon Scripts, and Data
cedar	MS Exchange E-Mail, SMTP and POP3 services, Calendaring and Scheduling
redwood	ArcServe Backup utilities IP Forwarding
acorn	MS SQL Server, Database Server. Holds Development information
pine	Remote Access

NT Physical Security

This section covers these vulnerabilities:

- Unrestricted Physical Access to Server: cardinal — ●●●●
- Server's Case is not Secured: all servers — ●●●
- Floppy Drive Available for Boot: all servers — ●●●
- Power Switch not Covered: all servers — ●●●
- No Power-on BIOS-Protect Passwords: all servers — ●●●

Unrestricted Physical Access to Server: cardinal — ●●●●

Text Deleted.

Server's Case is not Secured: all servers — ●●●

Text Deleted.

Floppy Drive Available for Boot: all servers — ●●●

Text Deleted.

Power Switch not Covered: all servers — ●●●

Text Deleted.

No Power-on BIOS-Protect Passwords: all servers — ●●●

Text Deleted.

NT File System Security

This section covers these vulnerabilities:

- FAT File System Being Used: cardinal — 🌲🌲🌲
- User Data on the System Partition: cardinal, cedar — 🌲🌲🌲
- NTFS Permissions not Properly Applied: all servers — 🌲🌲🌲
- Administrative Shares Enabled: redwood — 🌲🌲
- User Permissions not Set Properly: cardinal — 🌲🌲
- Files Still Present in %systemroot%\repair: all servers — 🌲🌲

FAT File System Being Used: cardinal — 🌲🌲🌲

Text Deleted.

User Data on the System Partition: cardinal, cedar — 🌲🌲🌲

Text Deleted.

NTFS Permissions not Properly Applied: all servers — 🌲🌲🌲

Text Deleted.

Administrative Shares Enabled: redwood — 🌲🌲

Text Deleted.

User Permissions not Set Properly: cardinal — 🌲🌲

Text Deleted.

Files Still Present in %systemroot%\repair: all servers — 🚩🚩

Text Deleted.

NT Operating System Security

This section covers these vulnerabilities:

- Current Service Packs and Hot Fixes not Installed — 🚩🚩🚩
- Passwords Cracked from SAM: all servers — 🚩🚩🚩
- Remote Access to Registry Enabled: all servers — 🚩🚩🚩
- Trust Relationships not Secure — 🚩🚩🚩
- Caching of Logon Credentials Enabled: all servers — 🚩🚩
- Anonymous Network Access Enabled: all servers — 🚩🚩
- Unneeded Network Services Running: cedar — 🚩🚩
- Services Bound to External Network Cards: pine — 🚩🚩
- Unneeded Protocols Installed in the System: cedar — 🚩🚩
- Last Logged on User Name Displayed: all servers — 🚩
- Computer Visible from Browser: redwood, pine, acorn — 🚩
- System Page File not Cleared at Shutdown: all servers — 🚩
- No Port Restrictions: all servers — 🚩
- Logs Set to Default: all servers — 🚩
- Guest Access to Event Logs: all servers — 🚩
- No Legal Warning displayed at Logon: all servers — 🚩
- No Auditing Enabled: all servers — 🚩

Current Service Packs and Hot Fixes not Installed — ☹☹☹

E-Commerce is not up to date on its Service Packs or Hot Fixes. E-commerce's PDC and Exchange server are using Service pack 3 with no Hot Fixes. Microsoft has released two Service Packs since SP3 and numerous hot fixes. There are several Security and Y2K related fixes that are critical for these Windows NT based servers to continue to function correctly. E-Commerce Inc. should upgrade as soon as possible to at least SP4 from Microsoft.

Recommendation

All servers, especially mission critical servers, should be patched with the latest Service Packs and Hot Fixes available. Microsoft is currently offering Service Pack 5 and there are Hot Fixes out for that. To obtain the latest Service packs from Microsoft, visit Microsoft's Web Site. To obtain the latest Hot Fixes from Microsoft, connect to,

`ftp://ftp.micorosoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/`

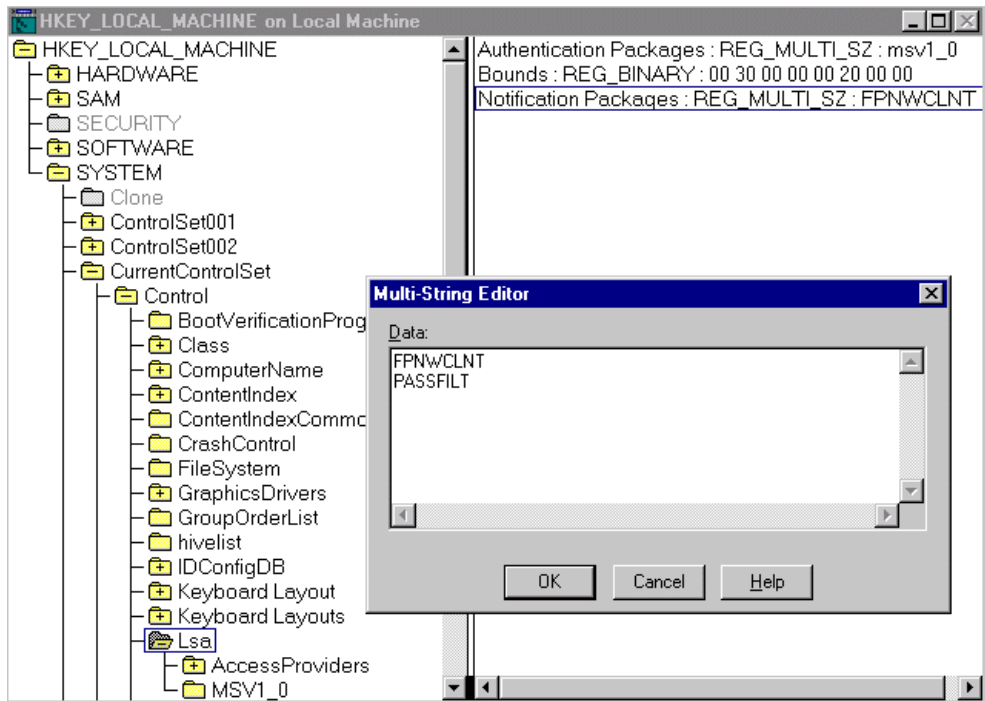
Passwords Cracked from SAM: all servers — ☹☹☹

While on site, E-Certify was able to crack 74% of all passwords from the SAM database including the Administrator password. These passwords were cracked in less than 5 minutes using L0pthCrack from Heavy Industries. E-Commerce Inc. should take extra precautions to enable strong passwords, especially on Administrator accounts. Even though E-Certify obtained the passwords from a copy of the SAM database, these passwords could be sniffed off E-Commerce's network by an Internal user.

Recommendation

Starting with Service Pack 3 from Microsoft, Administrators have the ability to require users to have stronger, or harder to crack passwords. This is enabled by using a .dll file that is included with Service Pack 3 from Microsoft (passfilt.dll). This .dll will enable System Administrators to require passwords that have a mixture of Upper and Lower case letters, a number or a symbol. To enable this .dll do the following:

1. Copy passfilt.dll to \Winnt\System32
2. From the Start Button, go to Run, the type regedt32.
3. Edit the Following registry key.
 - HKEY_Local_Machine\System\CurrentControlSet\Control\LSA
 - Add a "Reg_Multi_SZ" value titled "Notification Packages"
 - Add PASSFILT to the list, see figure below.



Remote Access to Registry Enabled: all servers — ☹️☹️☹️

Since having a password is only half of gaining access to a system, protecting the username is just as critical. By default, Windows NT offers usernames and other information to anyone who requests it. Certain parts of the registry are available for anonymous access.

Recommendation

E-Commerce Inc. should take immediate action to restrict anonymous access to the registry and even to disable remote access to the registry on its critical servers. E-Commerce Inc. must perform the following two registry edits on all critical servers.

Note: All registry modifications should be made using *regedt32.exe*.

Restrict Anonymous Network Access:

```
Hive/Key:HKEY_Local_Machine\System\CurrentControlSet\Control\LSA
Select Edit, Add Value.
Value Name=RestrictAnonymous
Data Type=REG_DWORD
Value=1
```

Disable Remote Access to Registry:

```
Hive/  
key=HKEY_Local_Machine\System\CurrentControlSet\Control\SecurePipe  
Servers\Winreg
```

Select the Winreg key and from the drop down menu “Security”, select the Permissions option. Only the Administrators group should have permissions there.

Trust Relationships not Secure — ☹️☹️☹️

Currently at E-Commerce Inc., there are two domains. The Production Domain and the Development Domain. E-Commerce Inc. is currently using two separate domains, which is set up as a two way trust set between the two domains.

Recommendation

E-Commerce Inc. should convert to the Single Master Domain model and implement a one way trust as follows.

```
Trusted Domain: Production Domain  
Trusting Domain: Development Domain
```

The Development Domain will trust all of the user accounts coming from the Production domain. As E-Commerce’s network grows so will the amount of Trust relationships. E-Commerce should take precautions to regulate the new Domains coming online and to make sure the trust relationships are configured correctly.

Caching of Logon Credentials Enabled: all servers — ☹️☹️

Text Deleted.

Anonymous Network Access Enabled: all servers — ☹️☹️

Text Deleted.

Unneeded Network Services Running: cedar — ☹️☹️

Text Deleted.

Services Bound to External Network Cards: pine — ●●●

Text Deleted.

Unneeded Protocols Installed in the System: cedar — ●●●

Text Deleted.

Last Logged on User Name Displayed: all servers — ●

Text Deleted.

Computer Visible from Browser: redwood, pine, acorn — ●

Text Deleted.

System Page File not Cleared at Shutdown: all servers — ●

Text Deleted.

No Port Restrictions: all servers — ●

Text Deleted.

Logs Set to Default: all servers — ●

Text Deleted.

Guest Access to Event Logs: all servers — ●

Text Deleted.

No Legal Warning displayed at Logon: all servers — 🚩

Text Deleted.

No Auditing Enabled: all servers — 🚩

Text Deleted.

NT User Account Security

The server cardinal is the primary domain controller and contains user accounts. This section covers user account vulnerabilities on cardinal:

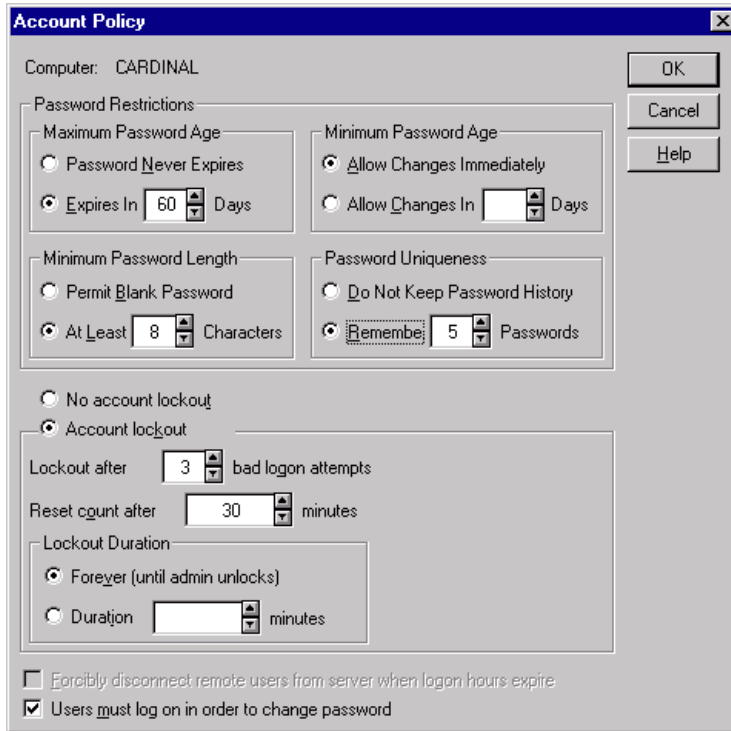
- No Account Restrictions — 🚩🚩🚩
- Passwords Never Expire — 🚩🚩🚩
- Account Lockout not Set — 🚩🚩🚩
- Lockout Duration not Set — 🚩🚩
- Minimum Password Length not Set — 🚩🚩
- Administrator Name Still Active — 🚩🚩

No Account Restrictions — 🚩🚩🚩

Since the Cardinal server is the Primary Domain Controller in the Windows NT domain, extra attention should be applied to the account policies. Currently, E-Commerce is not enforcing account restrictions.

Recommendation

All user accounts should be set to follow the same policies (Except Administrators). These policies are set through the “User Manager for Domains” located in the Administrative Tools group. The following graphic reveals recommended settings.



Passwords Never Expire — ❗❗❗

Text Deleted.

Account Lockout not Set — ❗❗❗

Text Deleted.

Lockout Duration not Set — ❗❗

Text Deleted.

Minimum Password Length not Set — ●●●

Text Deleted.

Administrator Name Still Active — ●●●

Text Deleted.

NT Dial-in Access Security

The server pine supports dial-in access. This section covers these remote access vulnerabilities on pine:

- Modems not Properly Documented — ●●●●
- No RAS Auditing — ●●●
- RAS Access Granted to Unnecessary User Accounts — ●●●
- Restrictive Hours not Set for Remote Users — ●●●
- Weak Remote User Passwords — ●●●
- Microsoft Encrypted Authentication not Required — ●●●
- Microsoft Windows NT 128 bit not Installed — ●●●
- 128 Bit Service Pack not Installed- — ●●●
- RAS Dial Back not Enabled — ●●
- PPTP Not in Use — ●●
- Third Party Authentication not in Use — ●●

Modems not Properly Documented — ●●●●

Text Deleted.

No RAS Auditing — ☹️☹️

Currently, E-Commerce Inc. is not auditing RAS connections.. Therefore, there is no way of tracking remote users accessing the system. E-Commerce would be unaware if a potential hacker was attempting to guess passwords or compromise the system.

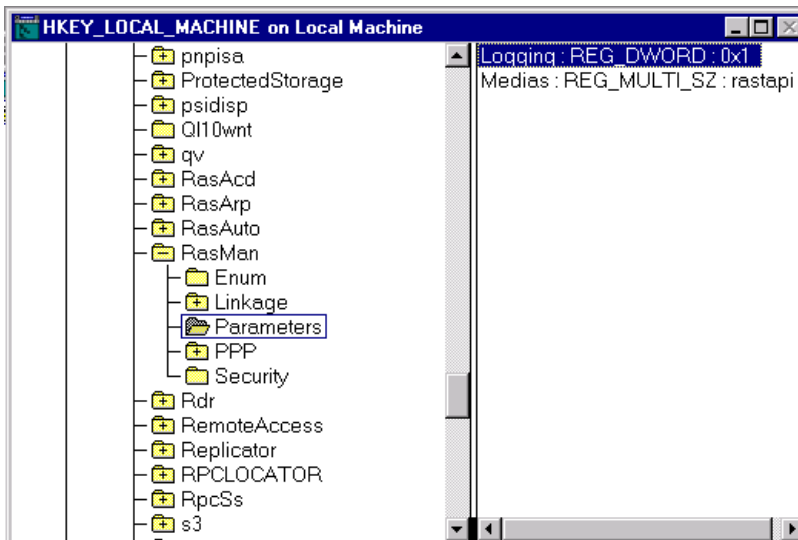
Recommendation

E-Commerce Inc. should enable RAS auditing immediately on the server pine.

Enable auditing for RAS

```
Hive/  
Key:HKEY_Local_Machine\System\CurrentControlSet\Services\RasMan\Parameters  
Value Name=Logging  
Data Type=REG_DWORD  
Value=1
```

The following graphic reveals the registry entry.



RAS Access Granted to Unnecessary User Accounts — ●●●

E-Commerce is not restricting what users have dial in access. While on site, E-Certify noticed several accounts that have dial in access and should not. One of these accounts is the guest account, which was probably used for testing but is now a serious security threat. Anyone can gain access to the internal network by using the guest account through remote access.

Recommendation

Disable the guest account immediately and revoke the dial in permissions to users who don't require it. This is done through the "User Manager for Domains".

Restrictive Hours not Set for Remote Users — ●●●

Text Deleted.

Weak Remote User Passwords — ●●●

Text Deleted.

Microsoft Encrypted Authentication not Required — ●●●

Text Deleted.

Microsoft Windows NT 128 bit not Installed — ●●●

Text Deleted.

128 Bit Service Pack not Installed- — ●●●

Text Deleted.

RAS Dial Back not Enabled — ●*

Text Deleted.

PPTP Not in Use — ●*

Text Deleted.

Third Party Authentication not in Use — ●*

Text Deleted.

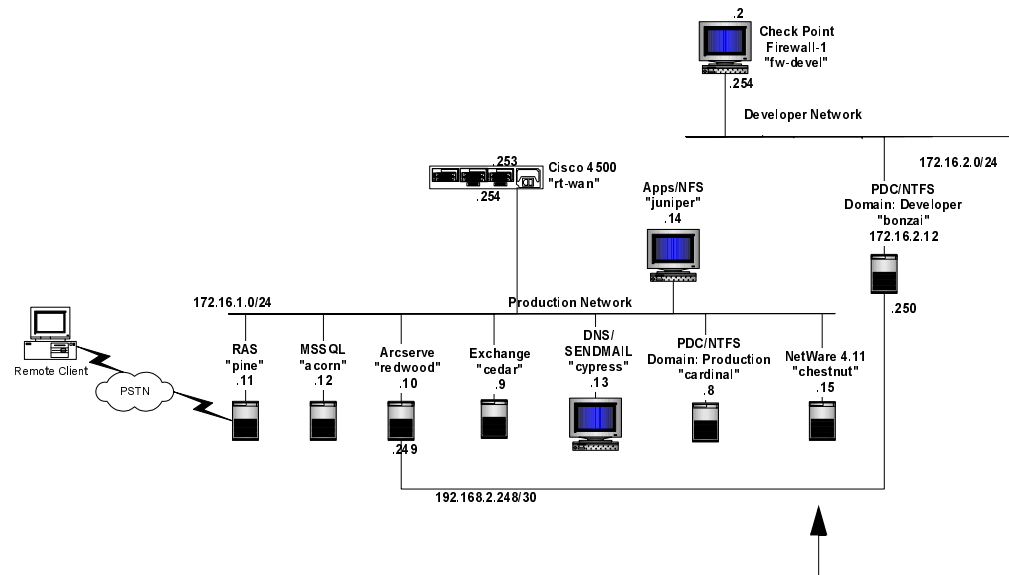
Novell Netware Server

This section covers these topics:

- Novell Server Overview
- Novell Physical Security
- Novell File System Security
- Novell Operating System Security
- Novell User Accounts Security

Novell Server Overview

The following diagram reveals the location of the Novell server chestnut.



Novell Physical Security

This section covers these vulnerabilities on chestnut:

- Unrestricted Physical Access to Server — 🚫🚫🚫
- Server's Case is Not Secured — 🚫🚫🚫
- Floppy Drive Available for Boot — 🚫🚫🚫
- Power Switch not Covered — 🚫🚫🚫
- No Power-on BIOS-Protect Passwords — 🚫🚫🚫

Unrestricted Physical Access to Server — 🚫🚫🚫

Text Deleted.

Server's Case is Not Secured — ●●●

Text Deleted.

Floppy Drive Available for Boot — ●●●

Text Deleted.

Power Switch not Covered — ●●●

Text Deleted.

No Power-on BIOS-Protect Passwords — ●●●

Text Deleted.

Novell File System Security

This section covers these vulnerabilities:

- ***Root Access of Volume Granted to Users — ●●●***
- ***All Users Have Access to Public Directory — ●●●***
- ***Data being Stored on SYS Volume — ●●***
- ***Print Queues in Use on SYS Volume — ●●***
- ***Inherited Rights Filters not Set Properly — ●***

Root Access of Volume Granted to Users — ●●●

Text Deleted.

All Users Have Access to Public Directory — ●●●

Text Deleted.

Data being Stored on SYS Volume — ●●

Text Deleted.

Print Queues in Use on SYS Volume — ●●

Text Deleted.

Inherited Rights Filters not Set Properly — ●

Text Deleted.

Novell Operating System Security

This section covers these vulnerabilities:

- NDS not Patched — ●●●
- NetWare OS not Patched — ●●●
- Year 2000 Patches not Applied — ●●●
- Secure.ncf not in Use — ●●●
- NWADMIN not Protected — ●●●
- RCONSOLE Encryption not in Use — ●●
- RCONSOLE not Protected — ●●
- NLM's can be Loaded Remotely — ●●
- Inappropriate Rights Set on NDS Objects — ●
- Multiple NDS Trees Present — ●

NDS not Patched — ●●●

Text Deleted.

NetWare OS not Patched — ●●●

Text Deleted.

Year 2000 Patches not Applied — ●●●

Text Deleted.

Secure.ncf not in Use — ●●●

Text Deleted.

NWADMIN not Protected — ●●●

Text Deleted.

RCONSOLE Encryption not in Use — ●●

Text Deleted.

RCONSOLE not Protected — ●●

Text Deleted.

NLM's can be Loaded Remotely — ●●

Text Deleted.

Inappropriate Rights Set on NDS Objects — 🚩

Text Deleted.

Multiple NDS Trees Present — 🚩

Text Deleted.

Novell User Accounts Security

This section covers these vulnerabilities:

- **Cracked 70% of Passwords — 🚩🚩🚩**
- **No Lockout Set — 🚩🚩**
- **No Password Length Restriction — 🚩🚩**
- **Users Have Rights at Root of Tree — 🚩🚩**
- **No Password History— 🚩**

Cracked 70% of Passwords — 🚩🚩🚩

Text Deleted.

No Lockout Set — 🚩🚩

Text Deleted.

No Password Length Restriction — 🚩🚩

Text Deleted.

Users Have Rights at Root of Tree — ●●

Text Deleted.

No Password History— ●

Text Deleted.

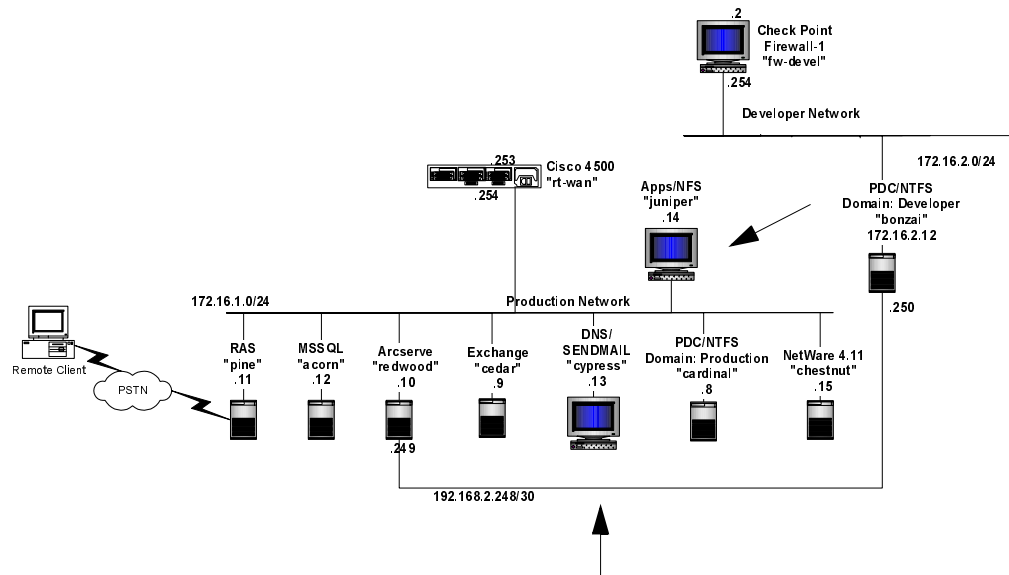
Unix Production Servers

This section covers these topics:

- Unix Server Overview
- Unix Physical Security
- Unix File System Security
- Unix Operating System Security
- Unix User Account Security

Unix Server Overview

The following diagram reveals the location of the two unix servers, juniper and cypress.



The following table summarizes the services offered by these servers.

Server	Services Offered
Juniper	User Accounts, Java Applications, and Data
Cypress	SMTP, POP3, and DNS

Unix Physical Security

Section deleted.

Unix File System Security

Section deleted.

Unix Operating System Security

This section covers these vulnerabilities:

- Unrestricted NFS Exports: juniper — 🚫🚫🚫
- Vulnerable X-Window Configuration: cypress — 🚫🚫🚫
- Tooltalk Enabled: juniper, cypress — 🚫🚫🚫
- Trust Relationship Configured: cypress — 🚫🚫🚫
- SNMP Enabled: juniper: cypress — 🚫🚫🚫
- Calendar Service Enabled: juniper, cypress — 🚫🚫🚫
- Sendmail Enabled: juniper — 🚫🚫🚫
- Excessive Services Enabled: juniper, cypress — 🚫

Unrestricted NFS Exports: juniper — 🚫🚫🚫

Text Deleted.

Vulnerable X-Window Configuration: cypress — 🚫🚫🚫

Text Deleted.

Tooltalk Enabled: juniper, cypress — 🚫🚫🚫

Text Deleted.

Trust Relationship Configured: cypress — ●●●

Text Deleted.

SNMP Enabled: juniper: cypress — ●●●

Text Deleted.

Calendar Service Enabled: juniper, cypress — ●●●

Text Deleted.

Sendmail Enabled: juniper — ●●●

Text Deleted.

Excessive Services Enabled: juniper, cypress — ●

Text Deleted.

Unix User Account Security

Section deleted.

