Global Information Assurance Certification Paper

Auditing a Business Partner Connection: An Auditor's Perspective.

By

Penny Khaw

GSNA Practical Assignment
Version 2.1 (amended July 5, 2002)
Option 1

Table of Contents

Table of Figures

Abstract

Business partner connectivity to corporate networks has become a large part of doing business in this day and age. Outsourcing of many business functions has resulted in the requirement for business partners to have access to corporate systems. This means that particular attention needs to be paid to the security of the connection between the business partner and the corporation.

The purpose of this paper is to provide a checklist for auditing a business partner that is connected to an organisation in the manner described in the paper. In addition to the checklist, the paper will also analyse the current configuration of the business partner connection, conduct a series of tests in accordance with the checklist and provide a report on the findings from the audit along with any recommendations.

Assignment 1 – Research in Audit, Measurement Practice, and Control

Identify the solution to be audited.

This audit will cover the connectivity of a business partner to PYP Computer Corporation (PCC). The business partner, LB and P Pty. Ltd. (LBaP), provides support for some of PCC's products to consumers. To facilitate the provision of this business function, they require access to PCC systems where product information, call-logging applications, parts and inventory, email and contact information reside. There is also a requirement to have access to PCC's internal email system to allow communication with the product divisions.

PCC manages the routers and network link that connects LBaP to PCC's infrastructure. PCC is responsible for setting up user accounts on their systems for access by LBaP's employees. LBaP is responsible for providing the PCs and implementing the mitigating actions, identified by the PCC business partner connectivity consultant, on these PCs.

An audit of LBaP's PC configuration, PCC's applications and systems being utilised by LBaP are out of scope. However, the mitigating actions LBaP were required to put in place to access PCC's network will be audited.

The LBaP PCs that access PCC systems are located on a segregated network separate from the LBaP corporate network. The segregated network is connected to one Ethernet interface on a Cisco 1605 router. Another Ethernet interface on the router is connected to a Cisco 2500 router to allow LBaP to control the access lists for traffic into their corporate network. The employees on the segregated network are then able to access their corporate resources as defined by the access lists. Finally, the router is connected to PCC's corporate network using an ISDN WAN link. The router at the other

end of the WAN link controls the access from the segregated network to the PCC systems. This configuration is depicted in the below diagram:

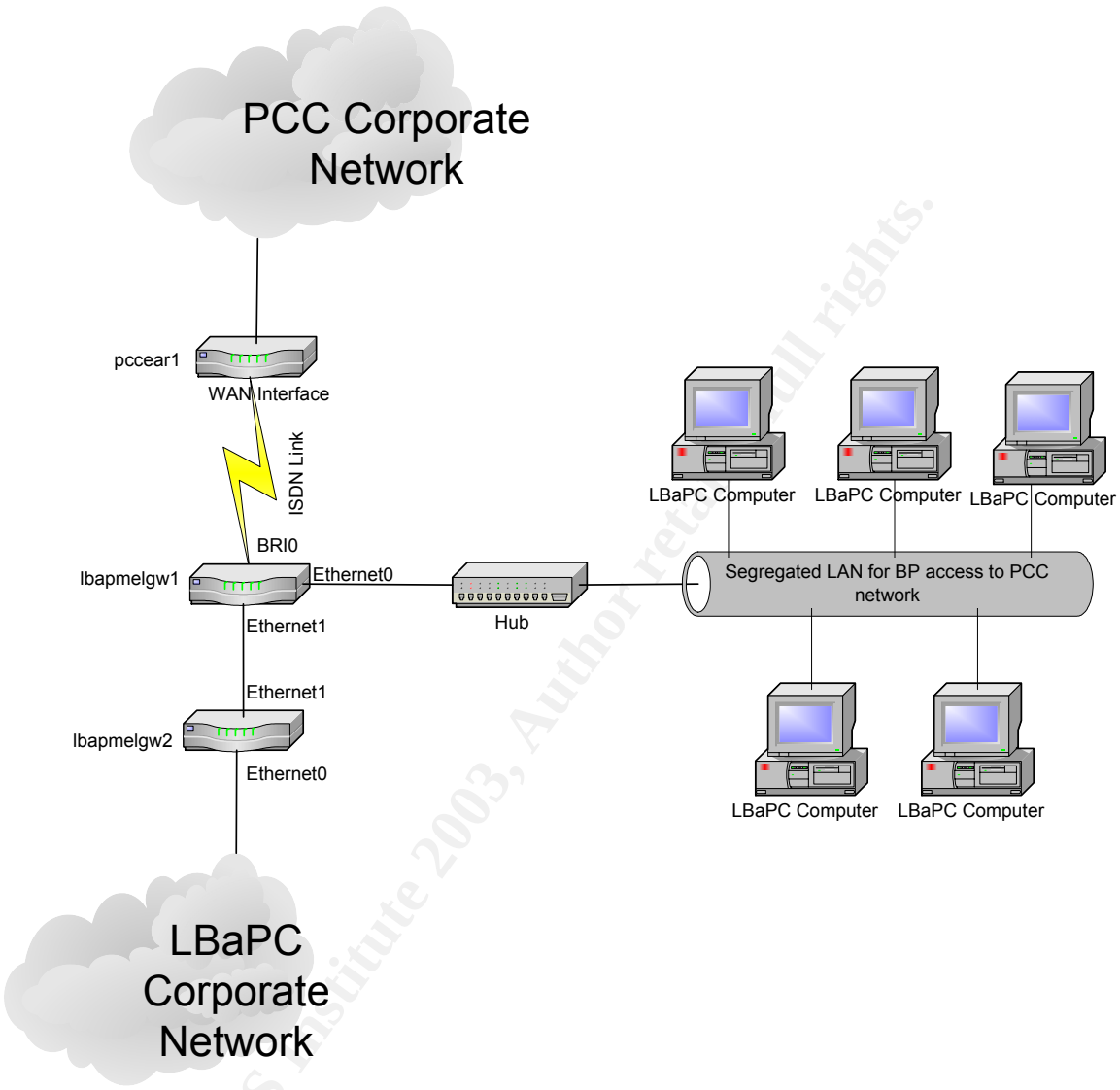


Figure 1: Network Diagram

Information on the routers current hardware configuration is shown below:

```
lbapmelgw1>show version
Cisco Internetwork Operating System Software
IOS (tm) 1600 Software (C1600-Y-M), Version 12.0(7)T,  RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 06-Dec-99 19:38 by phanguye
Image text-base: 0x02005000, data-base: 0x0257465C

ROM: System Bootstrap, Version 12.0(3)T, RELEASE SOFTWARE (fc1)
```

```
ROM: 1600 Software (C1600-RBOOT-R), Version 12.0(3)T,  RELEASE SOFTWARE (fc1)

lbapmelgw1 uptime is 8 weeks, 12 hours, 4 minutes
System returned to ROM by power-on
System image file is "flash:c1600-y-mz.120-7.T"

cisco 1605 (68360) processor (revision C) with 7680K/512K bytes of memory.
Processor board ID 21594342, with hardware revision 00000003
Bridging software.
X.25 software, Version 3.0.0.
Basic Rate ISDN software, Version 1.1.
2 Ethernet/IEEE 802.3 interface(s)
1 ISDN Basic Rate interface(s)
System/IO memory with parity disabled
8192K bytes of DRAM onboard
System running from RAM
7K bytes of non-volatile configuration memory.
4096K bytes of processor board PCMCIA flash (Read/Write)

Configuration register is 0x2102

lbapmelgw1>
```

Figure 2: lbapmelgw1 Router Configuration

```
lbapmelgw2#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-I-L), Version 12.1(10), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 06-Aug-01 17:08 by kellythw
Image text-base: 0x03041794, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
BOOTLDR: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTWA
E (fc1)

lbapmelgw2 uptime is 8 weeks, 2 days, 20 hours, 0 minutes
System returned to ROM by power-on
System image file is "flash:c2500-i-l.121-10.bin"

cisco 2500 (68030) processor (revision L) with 14336K/2048K bytes of memory.
Processor board ID 05615849, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

lbapmelgw2#
```

Figure 3: lbapmelgw2 Router Configuration

```
pccear1>show version
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-I-M), Version 12.2(10b), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 11-Jul-02 16:37 by pwade
Image text-base: 0x60008930, data-base: 0x609EE000

ROM: System Bootstrap, Version 11.1(20)AA1, EARLY DEPLOYMENT RELEASE SOFTWARE (f
c1)

pccear1 uptime is 10 weeks, 6 days, 18 hours, 13 minutes
System returned to ROM by power-on
System image file is "flash:c3640-i-mz.122-10b.bin"

cisco 3640 (R4700) processor (revision 0x00) with 124928K/6144K bytes of memory.
Processor board ID 13893878
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
Channelized E1, Version 1.0.
Bridging software.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
6 Ethernet/IEEE 802.3 interface(s)
34 Serial network interface(s)
1 Channelized E1/PRI port(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

pccear1>
```

Figure 4: pccear1 Router Configuration

The PCC network team provides support for the routers used for LBaP's connectivity. They are responsible for ensuring the configuration of the routers is maintained and any changes follow the correct processes and procedures. They also need to ensure that the configuration of the router is backed up appropriately.

Evaluate the Risk to the System.

There are inherent risks with connecting a business partner into a company's corporate network. In this instance, PCC has it's own team of Business Partner Connectivity consultants who are responsible for assessing the risk of each connection requested. The level of risk that is acceptable to PCC is often dependant on the business unit requesting the connectivity of the Business Partner, as the business unit has to sign off on the level of risk. In this situation, due to the unusual configuration of the connection there are a number of risks that need to be considered.

The configuration of the router between PCC's corporate network and LBaP is critical. The router must be configured such that the users on the segregated network are only able to access the applications they are authorized to access. If the router is not

configured correctly then there is the potential for the users to gain access to confidential information on the PCC corporate network. Similarly, the configuration of the router to allow access from the segregated network to the LBaP corporate network needs to be carefully controlled so that the users are able to access their nominated corporate resources but no one from PCC's corporate network can access the LBaP corporate network and vice versa.

The logging and auditing of traffic via the router is essential. Not only should there be logging switched on but the PCC network team should also be actively monitoring and auditing these logs to ensure that no unauthorised access is occurring. Without valid logging and auditing switched on it would be impossible for PCC to identify when unauthorised activity is occurring let alone addressing these issues with LBaP.

The patch management of the router is another area of risk. Cisco continuously release updated versions of their IOS to ensure that any vulnerability identified is corrected. If the routers do not have the latest IOS or mitigating actions implemented then this could potentially leave PCC open to attack via a vulnerability with the router IOS. The PCC network team should have a standard patch management process in place to protect the company against vulnerabilities on all the routers they manage.

During initial implementation there was a specific number of PCs identified that were allowed to access the PCC network. The router was configured to allow the entire segregated subnet access on the specific application ports. It is unclear if LBaP has added additional PCs to the segregated network. This means that there could be additional PCs being utilised to access PCC systems that are not meeting the required mitigating actions as detailed by the BP Consultant.

LBaP needs to have access to the systems between 7am and 7pm in order to provide support to PCC's customers and meet the Service Levels they have agreed to. Therefore, physical access to the router must be properly secured. Given the connectivity of the segregated LAN and the ISDN link to PCC's network, access to the router needs to be limited so that no unwarranted changes are made that would impact availability of access. It is also critical that any changes made to the router follow the correct change management procedures to ensure that no impact to availability is made. Changes should also be made outside business hours so that there is no availability impact.

Physical access to the PCs also needs to be considered. In this situation it is not possible to physically secure the PCs from the rest of LBaP's users, hence the need for educating the users on the proper security practices for screen savers and passwords. The risk being, if one of the users on the segregated LAN walks away from their PC without a screen saver set to lock the PC after a certain period of time, then anyone is able to walk up to that PC and gain access to PCC's systems that may contain confidential information.

Current State of Practice

In auditing the Business Partner connectivity to PCC there are three areas to take into consideration when looking at the current state of practice – the state of practice with a technical audit of the setup, the state of practice of the actual proposal put together by the BP consultant and the state of practice of other business partner/third party connectivity audits that may have been collated.

In looking at the proposal, it was clear that the BP consultant had put in some mitigating controls for the connectivity of LBaP to PCC's corporate network. These were easily transferable into a checklist format to determine if LBaP had put these mitigating controls in place and were meeting their obligations (Refer to Appendix A for the LBaP Project Proposal). An assessment checklist against PCC's corporate security policies for business partner connectivity was also created to utilise for this audit to ensure the company security policies are being adhered to (Refer to Appendix B for the assessment checklist).

For the technical state of practice, the first place that was investigated was the vendor web site. Cisco has published a checklist of sorts for improving router security, which is located at http://www.cisco.com/warp/public/707/21.html. This provides some good guidelines to start on router security although there is always the lingering question of whether Cisco will detail all the potential security vulnerabilities with their products.

The next place that was investigated was the Centre for Internet Security web site (www.cisecurity.com) where a lot of benchmarking tools are available. This led to the Router Assessment Tool, which is freely available from the site. The Router Assessment tool or RAT has been put together with the knowledge of experts in this field. The RAT is designed to assist with the auditing of routers and provides two levels of auditing. The first level is like a "must have" security configuration whilst the second level has "optional" security configurations depending on how your organisation has the router configured. Level 1 of the RAT is primarily based on the NSA Router Security Configuration Guide. This guide is freely available from www.cisecurity.com or http://www.nsa.gov/snac/cisco/guides/cis-2.pdf and goes into a lot of detail on securing IP routers in general. It also contains a specific section on the steps needed to secure Cisco routers in particular.

Additional resources were searched for information on both a technical router audit as well as anything in relation to a business partner/third party connectivity audit. These resources included:

- SANS reading room (www.rr.sans.org)
- SANS posted practicals for GIAC Systems and Network Auditor (www.giac.org/GSNA.php)
- AuditNet (www.auditnet.org)
- Information Systems Audit and Control Association – ISACA (www.isaca.org)
- Google (www.google.com)

All of these sources have provided good information on best practice for router security, which has provided a good background for the auditor. Unfortunately there was little to no information on business partner or third party connectivity auditing. This has meant for the business component of this audit there is a heavy reliance on the proposal that was put together by the business partner consultant and the PCC security policies.

Assignment 2: Create an Audit Checklist

Introduction

As part of the Business Partner Connectivity program, and in particular this proposal, an audit of the setup needs to be conducted every 12 months. As such, the following checklist will be utilised to audit the environment. Any tests that need to be run on the actual router will be conducted at a suitable time with LBaP to ensure that no impact to production occurs. The appropriate change request will also be raised for these tests to be conducted.

Objectives

The purpose of this audit is to verify the configuration of the router to ensure it still meets the original proposal and any changes that have been noted since. It will check to ensure any mitigating actions that were required by LBaP have been put in place and continue to be utilised whenever new staff or PCs are added to the segregated network. The audit will also check specific security policy items that need to be met with the PCC equipment.

Scope

This audit will focus on the security of the business partner connection, more specifically the router configuration, physical security and mitigating actions required by the business partner.

Definitions

The table below contains definitions of the terms used in the checklist:

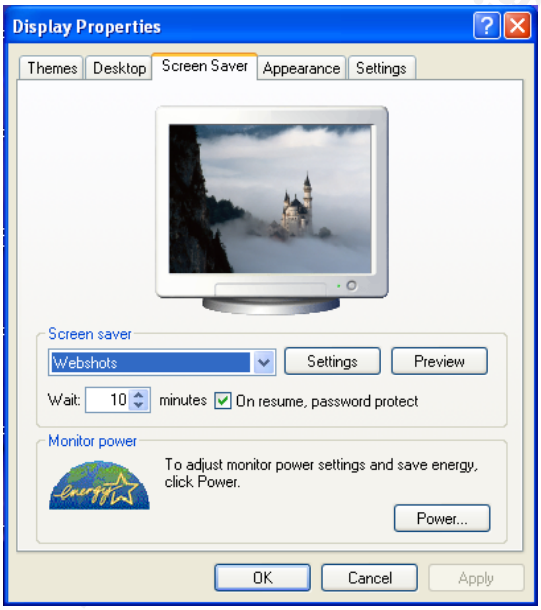
Term	Definition
Reference	Covers the source of the item being checked.
Control Objective	Details what the test is designed to achieve.
Risk	Identifies what risk is supposed to be addressed with the check. Contains a rating on the importance of the risk to either PCC or LBaP. This rating will take the form of High, Medium or Low. Details the likelihood and consequence if the item is not being complied with.
Compliance	Describes what is required for the system to be compliant with the test.
Testing	Details the steps to be taken to check if the system is compliant or not.
Objective/Subjective	An objective test is one where the test can be independently verified and is repeatable e.g.: output from a vulnerability scanner. A subjective test is much harder to verify and may take the form of interviews and rely on the judgment of the auditor.

Checklist

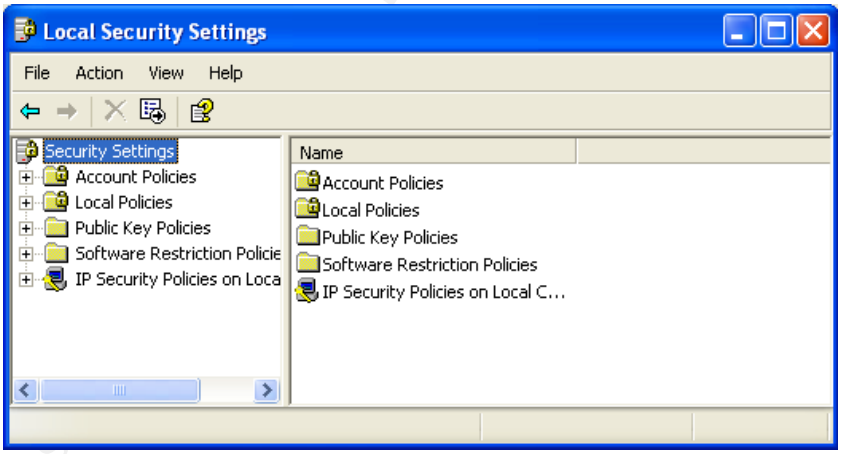
1. Physical Security	
Reference	LBaP Proposal 125 documentation: Original Request – August 2000 Subsequent revisions – March 2002 & 2003. Business Partner Network Security Checklist
Control Objective	Ensure that the appropriate physical security for the communication equipment rack is provided at the Business Partner site.
Risk	The router and corresponding ISDN connection may be compromised, mishandled or stolen resulting in monetary loss through the loss of equipment and productivity. LBaP would be unable to meet its SLA requirements and there would be a large impact on the brand image of both LBaP and PCC. This risk has a **high** rating due to the large reliance on the router and ISDN link for connectivity to systems to allow LBaP to provide services to PCC's customers and for the impact such an outage would have on brand image for both companies.
Compliance	The communication equipment rack must be housed in a secure environment such as a computer room. The site must have a burglar alarm that is operational and enabled. Access is only provided by the onsite Manager.
Testing	1. Conduct an onsite inspection of the computer room to confirm the location of the communication equipment rack. 2. Take photos of the communication equipment rack location, if possible, as evidence. 3. Interview the onsite contact to determine who has access to the computer room and how this access is controlled. Determine if the access procedure is documented and obtain a copy of the documentation if possible. 4. Identify the existence of the burglar alarm. 5. Interview the onsite contact to determine the existence of documented procedures for the burglar alarm. Obtain a copy of the documentation, if possible, as evidence. Also identify the hours of operation of the burglar alarm.
Objective/Subjective	Objective Tests – Location of the communication equipment rack and burglar alarm. Documented operation of the burglar alarm. Subjective Tests – Access control and burglar alarm procedures may vary over time and require an interview with an LBaP representative.

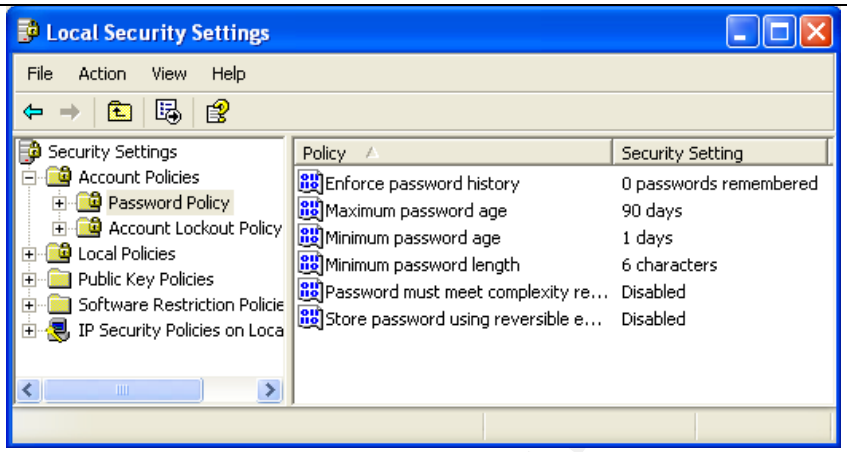
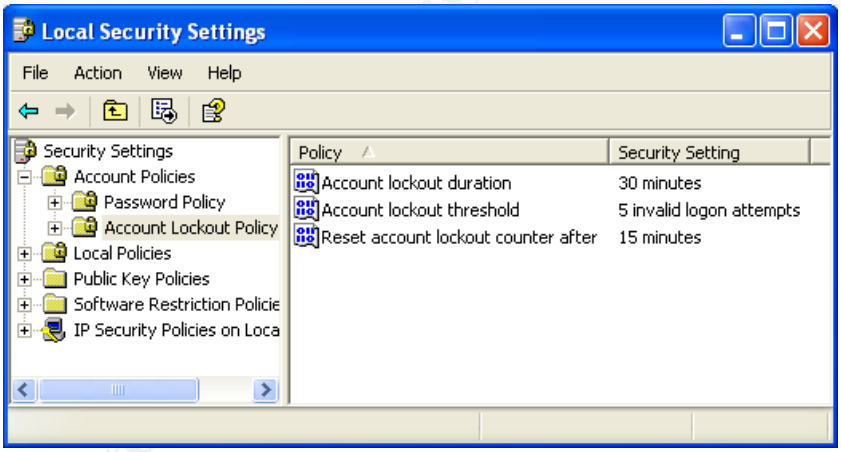
2. PCC Communication Equipment Location	
Reference	LBaP Proposal 125 documentation: Original Request – August 2000 Subsequent revisions – March 2002 & 2003. Business Partner Network Security Checklist
Control Objective	Confirm that PCC communication equipment (eg: hub, router etc) is physically located in a 19-inch rack within the physically secure area identified in Checklist item 1.
Risk	PCC supply all the communication equipment and rack to ensure that the equipment is easily identifiable when work needs to be carried out and to prevent other equipment being disconnected. The risk being that if the equipment is not easily identifiable, the connectivity to the PCC network may be disconnected by other parties working on other equipment within the secure area. The risk rating is **high** as there is the potential for connectivity to the PCC network being removed and LBaP being unable to meet their SLAs with PCC. There is also the potential for the brand image of PCC to be damaged should LBaP be unable to provide the service and support required to PCC's customers.
Compliance	The communication equipment must be physically located in a 19-inch rack.
Testing	1. Conduct an onsite inspection of the computer room and confirm that all PCC communication equipment is located in a 19-inch rack. 2. Take photos of the location of the PCC communication equipment as evidence.
Objective/Subjective	This is an objective test as the equipment is either located in a 19 inch rack or not.

3. Screen Saver Configuration	
Reference	LBaP Proposal 125 documentation: Original Request – August 2000 Subsequent revisions – March 2002 & 2003.
Control Objective	Ensure that adequate protection is in place to restrict access to the PCC corporate network and systems that are accessible from the PCs that are on the segregated network.
Risk	The PCC systems that LBaP users access from these PCs may be compromised if the PCs are left open to anyone who may be in the office. The information contained on the PCC systems are also company confidential and disclosure of such information may be detrimental to PCC's business. The risk has a **high** rating due to the type of information that is available on the systems LBaP users have access to and the potential impact disclosure of such information may have on

	PCC's brand image.
Compliance	The PCs on the segregated network must all have the screen saver enabled and set to time out after a specified period of time. The screen saver must also be setup to lock the PC and require a password to unlock the system.
Testing	Confirm the screen saver settings of all PCs on the segregated network through an onsite visit. 1. Right click on the desktop 2. Select Properties 3. Click on the Screen Saver tab to view the settings:  4. Obtain a screen capture from one of the PCs as evidence. If any of the PCs deviate from the required settings, obtain a screen capture as evidence and note the PC name.
Objective/Subjective	This is an objective test as the screen saver is either switched on and configured as required or not.

4. Password Practices	
Reference	LBaP Proposal 125 documentation: Original Request – August 2000 Subsequent revisions – March 2002 & 2003.
Control Objective	Ensure LBaP practices for protecting passwords are substantial to protect against unauthorised disclosure of passwords.
Risk	LBaP are utilising their own password configuration to authenticate the identity of the users accessing the PCs. Password disclosure and easy to guess passwords pose a threat to both LBaP's business and PCC's systems. If

	passwords are disclosed or cracked, LBaP's corporate network may be accessed and compromised. PCC's network may also be compromised using the open ports between the segregated network and the PCC network. The risk rating is **low** as only minimal ports are open between the segregated network and LBaP's network whilst access to PCC's network is on specific ports requires authentication on the system being accessed prior to access being granted.
Compliance	The PCs on the segregated network must all be complying with LBaP's password configuration minimum standards.
Testing	Conduct the following steps during the onsite visit: 1. Interview the onsite contact and determine the required password configuration. If possible, obtain a copy of the password standard/policy for LBaP to review against. 2. Check the password configuration settings for the PCs: - Click on Start, Programs, Administrative Tools, Local Security Policy. - The following should appear:  - Click on Account Policies - Double click on Password Policy - The following screen should appear:

	 - Click on Account Lockout Policy - The following screen should appear:  3. Attempt to change the password of an account so that it is in breach of the password settings and observe any errors that occur.
Objective/Subjective	Objective tests – Password configuration is meeting the LBaP standard. The configuration of the PCs as part of the domain and following the password standard.

5. AntiVirus Software	
Reference	Business Partner Network Security Checklist
Control Objective	Ensure that adequate protection is provided for the PCs from viruses, worms and Trojans using Antivirus software. Ensure that virus definition files are kept up to date to protect the PCC network and LBaP corporate network from viruses being propagated.
Risk	Without adequate Antivirus software on the PCs in the segregated network, there is the potential to introduce viruses to the segregated network via other means such as floppy

	disks being used with the PCs in the segregated network and email. This could then result in viruses being propagated to the PCC network and LBaP's corporate network. The risk associated with this is **high** as the users on the segregated network are able to access their email and the Internet where a high number of viruses find their way into a network. Virus infection has the potential to render the segregated network unusable and, if a virus propagates into the PCC or LBaP networks, have a large business impact on PCC and LBaP.
Compliance	Antivirus software must be installed on all PCs on the segregated network. Definition files must be kept up to date.
Testing	Log on to each PC and check for AntiVirus software being installed: 1. Click on Start, Programs 2. Look for an AntiVirus application such as Norton AntiVirus, Trend Micro etc. If the AntiVirus software is located check the definition file to confirm if it is up to date: 1. Click on Start, Programs, AntiVirus application 2. Locate the Virus Definition File Version 3. Confirm if this is the latest version by noting the current version installed and comparing it to that which is available via the vendor web site. Interview the onsite contact or IT contact and confirm if there is a documented procedure to update the definition files and how often these files are updated. Obtain a copy of the documentation if possible.
Objective/Subjective	Objective tests – Antivirus software installed on all PCs. Definition files are up to date. Documentation covering the procedure to update is in place. Subjective test – Definition files are updated as per the documented timeline.

6. Secure connectivity to the routers	
Reference	NSA Router Security Configuration Guide
Control Objective	Ensure that remote access to the routers is performed in a secure manner.
Risk	When connecting to the routers, utilising a secure method for sending username and password is critical to ensure that the security of the router configuration is maintained. If a secure method is not utilised then an attacker will be able to gain access to this information by sniffing the data off the network. The risk associated with this is **high** as once an attacker gains

	access to the username and password they can potentially change the configuration on the routers, impact the WAN link and gain access to confidential information from PCC and LBaP.
Compliance	Passwords must not be sent in the clear between the client and the router.
Testing	Interview the network engineers and ask them the following questions: - What method is employed to connect to the routers? Conduct a packet capture using Ethereal, version 0.9.11 or later, to confirm if the passwords are sent in the clear depending on the method being used to connect to the routers.
Objective/Subjective	Subjective – Interview of the network engineer Objective – Ethereal packet capture

7. Banner and configuration information	
Reference	Business Partner Network Security Checklist Improving Security on Cisco Routers
Control Objective	Ensure that no configuration information is shown prior to login on the router. Provide an adequate legal banner either before or after login on the router.
Risk	By providing router configuration information prior to login there is the potential to provide an attacker with enough information so that he/she knows what attack vector to use and does not even need to log in to the router. Without an adequate legal banner being presented, there is the possibility that legal recourse against an attacker, if caught, may not be possible. The risk associated with this is **medium** given the physical security that should be in place to protect the equipment.
Compliance	No configuration information, eg: IOS version, is to be shown prior to login. A legal login banner must be configured on the router.
Testing	1. Utilise the method identified in Checklist item 6 to connect to lbapmelgw1 eg: Telnet 2. Observe and do a screen capture of what appears prior to login. 3. If no legal banner appears prior to login, type in the username and password for the router. 4. Observe and do a screen capture of what appears post login. Repeat the above steps for lbapmelgw2.pcc.com and pccear1.pcc.com
Objective/Subjective	This is an objective test.

8. Router Password configurations	
Reference	Business Partner Network Security Checklist Improving Security on Cisco Routers NSA Router Security Configuration Guide
Control Objective	Ensure that the passwords in use to log in to the router and the enable password are meeting the PCC security policy and standard.
Risk	The PCC router passwords need to comply with the PCC security policy and standard for password management. Without following this standard, the router passwords may be easily crackable and may therefore allow easy access to the router configuration. An attacker would then be able to modify the router configuration to their own benefit once they cracked the passwords. The risk associated with this is **high** as the quality of passwords is essential to maintain the integrity of the router configuration and prevent unauthorised configuration changes. If the passwords do not meet the security policy and standard then it is in breach of the PCC security requirements.
Compliance	Passwords must be meeting the PCC password policy and standard.
Testing	1. Utilise the method identified in Checklist item 6 to connect to lbapmelgw1 eg: Telnet 2. Enter the login credentials to login to the router. 3. Type in “enable” 4. Type in the enable password 5. Type in “show running-config” 6. Check the results and look for the commands “enable secret 5”, “enable password 7”, and, under the VTY configurations, “password 7”. 7. If you find “enable password 7” and/or “password 7” under the VTY configurations, run these through the Cisco password cracker (www.alcrypto.co.uk/cisco) 8. Confirm if the cracked passwords meet the corporate password standard. 9. If you find “enable secret 5”, interview the network engineer responsible and ask what the password in use is. Assess whether this meets the current corporate standard. Repeat the above steps for lbapmelgw2.pcc.com
Objective/Subjective	Objective test – Cracking any passwords and assessing if they meet the corporate standard. Subjective test – Asking the network engineer what the enable secret password is to determine if it complies with the corporate standard.

9. Encryption level of the router password	
Reference	Business Partner Network Security Checklist NSA Router Security Configuration Guide Improving Security on Cisco Routers
Control Objective	Ensure that the router enable passwords have been set to enable secret to ensure they are encrypted.
Risk	As the enable password provides root access to the router it is essential that this be encrypted. This provides an extra layer of security, as it is very difficult to crack the enable secret password when it is encrypted on the router. It also means that if the configuration of the router is sent to anyone then the enable password is not sent as normal text or in the crackable format. The risk associated with this is **high,** as access to this password would allow an attacker to change anything on the routers and gain access to both the PCC network and the LBaP corporate network. This could result in confidential information from both companies being revealed and brand image being impacted.
Compliance	The enable password must be configured with encryption using the enable secret command to comply with the corporate policy.
Testing	1. Utilise the method identified in Checklist item 6 to connect to lbapmelgw1 eg: Telnet 2. Enter the login credentials to log on to the router 3. Type “enable” 4. Enter the enable password 5. Type “show running-config” 6. Check the results and look for the command “enable secret” or “enable password” 7. If the router has “enable secret” then this meets the corporate policy. If the router has “enable password” then this fails the test in meeting the corporate policy. Repeat this test with lbapmelgw2.pcc.com
Objective/Subjective	This is an objective test

10. Authentication of remote connectivity to the routers	
Reference	NSA Router Security Configuration Guide
Control Objective	Ensure that remote access to the routers has proper authentication implemented, i.e. individual username and password for each network engineer accessing the equipment.
Risk	Authentication on the routers is critical to ensuring only authorised network engineers have access to the equipment. Individual user accounts should be configured to assist with

	this. If authentication is not in place then an attacker could easily sniff the password information off the network and gain access to the equipment. The risk associated with this is **high** as an attacker gaining access to the routers would be able to change configuration information, impact the WAN link and potentially gain access to confidential information from PCC and LBaP.
Compliance	Authentication must be using username and password with the password meeting corporate standards.
Testing	1. Utilise the method identified in Checklist item 6 to connect to lbapmelgw1 eg: Telnet 2. Enter the login credentials to log on to the router 3. Observe whether a prompt appears for username followed by password or if just a password is prompted for. Repeat the above steps with lbapmelgw2
Objective/Subjective	Objective

11a. Router ACL configuration	
Reference	Business Partner Network Security Checklist LBaP Proposal 125 documentation: Original Request – August 2000 Subsequent revisions – March 2002 & 2003.
Control Objective	Check that the ACL configuration on the routers matches the ports required that are documented in the LBaP proposal. No other ports should be open on the routers.
Risk	Incorrect configuration of the routers may allow unauthorised access to the PCC network. This would leave the PCC network open to attack from the LBaP segregated network. The risk associated with this is **high** as there is the potential for unauthorised access to the PCC network, company confidential information being accessed and the brand image of PCC and LBaP being damaged.
Compliance	The routers ACL configuration must match that documented in the LBaP proposal document.
Testing	1. Utilise the method identified in Checklist item 6 to connect to lbapmelgw1 eg: Telnet 2. Enter the login credentials to connect to the router 3. Type in “enable” 4. Enter the enable password 5. Type in “show running-config” 6. Check the results and look for all the lines starting with “access-list” that are associated with the LBaP business partner connection. 7. Take a copy of the access lists and compare the IP

	addresses and ports to those in the project proposal document. Repeat the above steps for lbapmelgw2.pcc.com and pccear1.pcc.com.
Objective/Subjective	This is an objective test as the ACLs are either configured correctly or incorrectly.

11b. Overall Router configuration	
Reference	Centre for Internet Security Router Assessment Tool
Control Objective	Test the overall router configuration utilising the Router Assessment Tool as a basis for good configuration of routers.
Risk	Incorrect configuration of the routers may allow unauthorised access to the PCC network. This would leave the PCC network open to attack from the LBaP segregated network. The risk associated with this is **high** as there is the potential for unauthorised access to the PCC network, company confidential information being accessed and the brand image of PCC and LBaP being damaged.
Compliance	Items rated with an Importance from 10 – 7 must all be rated with a Pass.
Testing	Use CISecurity's Router Assessment Tool to test for weaknesses/vulnerabilities with the routers: 1. Obtain the results of the show running-config from lbapmelgw1 2. Copy results into a text file and save the file eg: lbapmelgw1 3. Ensure Perl is installed 4. Ensure RAT is installed 5. Open a Dos prompt 6. Change directory to where RAT is installed, then change to the bin directory 7. Type in "perl rat" followed by the filename eg: "perl rat lbapmelgw1" 8. Review results located in the html file eg: lbapmelgw1.html Repeat steps 1 – 9 for lbapmelgw2 and pccear1.
Objective/Subjective	This is an objective test as the items with Importance 10 – 7 either Pass or Fail.

12. VTY Access Restrictions	
Reference	NSA Router Security Configuration Guide Improving Security on Cisco Routers
Control Objective	Ensure that the VTY access is restricted such that the Business Partner is not able to gain telnet access to either of the routers.
Risk	Only the PCC network engineers should be able to gain access

	to the routers using a VTY session. LBaP personnel should not be able to gain access using a VTY session. This is very important, as access to the routers via such a session would allow changes to be made to the routers if the LBaP personnel had the right passwords. The risk associated with this is **high** as no one at the business partner site should have telnet access to the routers as this may result in the ACL configurations being tampered with and unauthorised access to the PCC network being obtained.
Compliance	VTY sessions must be restricted to only PCC network access.
Testing	1. Utilise the method identified in Checklist item 6 to connect to lbapmelgw1 eg: Telnet 2. Enter the login credentials to login to the router 3. Type “enable” 4. Enter the enable password 5. Type in “show running-config” 6. Check the results and look for the command “line VTY” 7. Under each line VTY section look for the command “access-class” and the corresponding number 8. Check the “show running-config” results again and look for the corresponding number next to the “access-class” in the “access-list” listing. 9. Check the IP addresses listed in the “access-list” command to confirm that none of IP addresses are from the LBaP corporate network or the segregated network. Repeat the above steps for lbapmelgw2.pcc.com
Objective/Subjective	This is an objective test

13. Access between PCC network, LBaP corporate Network and the segregated network	
Reference	LBaP Proposal 125 documentation: Original Request – August 2000 Subsequent revisions – March 2002 & 2003.
Control Objective	Access from the LBaP corporate network to the PCC network and vice versa must not be possible. Access from the segregated network to the LBaP network should be open but access from the LBaP network to the segregated network should not be possible.
Risk	If access from the LBaP corporate network to the PCC network is possible then this exposes the PCC network to potential propagation of viruses, worms, Trojans and attacks from the LBaP corporate network. It also reduces the amount of control PCC have over the environment that is connecting to its network. This is also applicable for connectivity from the PCC network to LBaP’s corporate network. If access from the LBaP

	network is allowed into the segregated network then this could provide another route to obtain unauthorised access to the PCC network thus exposing PCC's network and the segregated network. The risk associated with this **high** as this contravenes the proposal document, PCC's corporate security policies and increases the exposure of PCC's corporate network to an environment over which it has no control.
Compliance	No access is allowed between the PCC network and the LBaP corporate network and vice versa. No access is allowed from the LBaP corporate network to the segregated network. Access is allowed from the segregated network to the LBaP corporate network.
Testing	1. Utilise the ACL configurations obtained using the show running-config command in checklist item 11a. 2. Check the ACL configurations for lbapmelgw1, lbapmelgw2 and pccear1 to ensure no access between PCC and LBaP and vice versa has been configured on the routers. Ensure no access has been configured between LBaP and the segregated network. Ensure access between the segregated network and LBaP is configured. Test the access from the LBaP corporate network to the PCC network using the following steps: 1. Open a Dos prompt on a PC connected to the LBaP corporate network 2. Type in tracert pccdns.pcc.com 3. Observe where the traffic is attempted to be routed to and ensure this is not to the PCC network. Test the access from the LBaP corporate network to the segregated network using Traceroute. 1. Open a Dos prompt on a PC connected to the LBaP corporate network 2. Type in tracert 192.168.32.1 3. Observe where the traffic is attempted to be routed to and ensure this is not to the segregated network Test the access from the segregated network to the LBaP corporate network using the following steps: 1. Open a Dos prompt on a PC connected to the LBaP corporate network 2. Type in tracert 172.31.10.253 3. Traffic should be routed out the interface connecting to the LBaP network.

	Test the access from the PCC network to the LBaP corporate network using the following steps: 1. Open a Dos prompt on a PC connected to the PCC network 2. Type in tracert 172.31.10.253 3. Observe where the traffic is attempted to be routed to and ensure this is not to the LBaP corporate network.
Objective/Subjective	This is an objective test as access is either allowed or denied.

14. Unauthorised Access	
Reference	Business Partner Network Security Checklist LBaP Proposal 125 documentation: Original Request – August 2000 Subsequent Revisions – March 2002 & 2003
Control Objective	No unauthorised access using Telnet, VT3K, FTP, HTTP, Rexec, rlogin, remote shell, NetBIOS, SMTP to the PCC network.
Risk	All the above methods of access via the router present a risk to the PCC network due to the nature of the applications themselves, eg: telnet passes all data in the clear, there are known methods of attack using the FTP and HTTP ports. The risk associated with this is **medium** as none of these applications are required by LBaP and should therefore not be configured on the routers.
Compliance	None of the applications listed are configured for access via the routers.
Testing	1. Utilise the results of the show running-config from checklist item 11a. 2. Check the ACL configurations to ensure none of the above application ports have been opened unless in the approved port list in the proposal document.
Objective/Subjective	This is an objective test as the ports are either open on the router or not.

15. Router Patch Management	
Reference	Business Partner Network Security Checklist Cisco – Improving Security on Cisco Routers NSA Router Security Configuration Guidelines
Control Objective	Ensure adequate protection is provided from an attack utilising vulnerabilities in the router IOS to the PCC network and the LBaP corporate network by keeping the IOS version on the router up to date.
Risk	Cisco continuously release updated IOS which resolve issues with the router IOS. The lack of updating of the IOS may result in the PCC network being attacked utilising a vulnerability that

	exists with the current IOS level on the router. The risk associated with this is **medium** based on the physical security requirements being in place and the need for token cards to gain access to the PCC network.
Compliance	Router IOS versions must be up to date or risks mitigated and documented appropriately.
Testing	1. Utilise the method identified in Checklist item 6 to connect to lbapmelgw1 eg: Telnet 2. Enter the login credentials to connect to the router 3. Type in “show version” 4. Check the results and look for the line starting with “IOS”. This should show the IOS version eg: Version 12.0 (7)T. 5. Check the results and look for the line starting with “cisco xxxx processor” to confirm the model of Cisco router in use. 6. Compare this with the current IOS version available from Cisco for the Cisco router and determine if there is a gap between the current IOS available and that which is installed on the router. 7. Repeat steps 1 – 7 for lbapmelgw2.pcc.com and pccear1. Determine if a patch management process is in place to ensure patching is kept up to date.
Objective/Subjective	The patch level is an objective test as it is either up to date or not. The existence of a patch management process is both objective and subjective. A documented process is an objective test. However, whether this process is actually followed by the network engineer is a subjective test as it involves asking the network engineer.

16. Logging	
Reference	Business Partner Network Security Checklist Improving Security on Cisco Routers NSA Router Security Configuration Guidelines
Control Objective	Adequate logging is configured on the router to ensure that any incidents have the appropriate evidence for investigation.
Risk	Logging should be switched on to ensure that any unauthorised access is recorded. If logging is not switched on and/or configured correctly then unauthorised access will not be identified which may result in company confidential information being accessed. The risk associated with this is **high** as without logging it is not possible to identify any attacks that may be occurring on the

	network. This also means that there is no evidence to utilise for investigative work.
Compliance	Logging must be switched on and logging to a separate system to allow for investigative purposes. Retention of the log files must meet corporate policy.
Testing	1. Utilise the method identified in Checklist item 6 to connect to lbapmelgw1 eg: Telnet 2. Type in the login credentials to log into the router. 3. Type in "enable" 4. Type in the enable level password 5. Type in "show running-config" 6. Check the results and look for the command "logging buffered" to confirm that logging is switched on. 7. Do a screen capture to obtain proof that logging is switched on. 8. Check the results and look for the command "logging" followed by an IP address that correlates to a server. 9. Do a screen capture to obtain proof that logs are being sent to a system. 10. Check the results from Checklist item 11a for any log references for the access lists. The word "log" should be found at the end of each access list. 11. Interview the system owner to determine the retention period of the logs and backups that are performed on the system. The retention period must meet the corporate policy Repeat the above steps for lbapmelgw2.pcc.com and pccear1.pcc.com
Objective/Subjective	Objective Tests – Items 1 – 10. Subjective Test – Interview with the system owner for information on the retention period.

17. Auditing and monitoring	
Reference	Business Partner Network Security Checklist
Control Objective	Monitoring and auditing of the log files for analysis must be provided. Analysis may take the form of performance analysis or for security incident analysis.
Risk	Although having logging enabled provides some level of information, without regularly monitoring and auditing the logs it is not possible to pick up possible unauthorised access attempts to the PCC network. It would also not be possible to identify performance issues with the equipment that are hindering the ability of LBaP to provide adequate support to PCC customers. The risk associated with this is **high** as the ability to monitor

	and audit log files are critical to ensuring the PCC network is protected from unauthorised access. LBaP must also be able to meet their SLAs and provide the required level of support to PCC customers. Without this, there is potential brand image impact to PCC.
Compliance	Monitoring must be enabled. Regular audits of the log information must be scheduled.
Testing	Interview the network engineer and obtain the following information: - Check that monitoring is enabled and any events are being flagged. - Check if any audits are occurring on the log information for areas such as performance issues.
Objective/Subjective	Objective test – Monitoring is enabled and events are being flagged. Subjective test – Audits are occurring, as this is reliant on information from the network engineer.

18. Router configuration backup	
Reference	Business Partner Network Security Checklist
Control Objective	Ensure that the router configurations are being backed up on a regular basis to provide a method to restore the exact configuration should a failure occur.
Risk	Without adequate backup procedures it would not be possible to recover the router easily and within a quick timeframe to ensure that LBaP continues to service PCC's customer to the level required. The risk associated with this is **high** as there is no hot spare router that contains an up to date configuration that matches the current router. This means that the network team will have to configure a replacement router in the event of a failure and then send it out on site which may result in a long period of downtime for LBaP where they are unable to meet their SLAs and damage occurs to PCC's brand image.
Compliance	There must be a backup procedure in place for the router at LBaP.
Testing	Interview the network engineer responsible and ask the following questions: - Is there a backup procedure in place for the router configuration? - If so, can evidence be provided either via a script being run and/or a cron/at job that is scheduled? - Is the backup procedure documented if there is one? - How long are the backups kept for? If possible, obtain a logon to the server where the backups are kept and check for backups of lbapmelgw1, lbapmelgw2 and

	pccear1.
Objective/Subjective	The backup procedure being in place and documented is a subjective test as it is based on an interview with the network engineer and there is nothing to prove that the procedure is actually being followed.

19. Change Management	
Reference	Auditor's own knowledge (IT Service Management)
Control Objective	Ensure that an adequate means of tracking changes to the configuration of the router, handle patch management and outages is in place.
Risk	A change management process is critical to ensuring that any changes occurring to the infrastructure are tracked and approved appropriately. Change management also helps to keep a configuration management system up to date. Without adequate change management it is not possible to track what has been done with or to equipment that may result in outages and cause LBaP to miss their SLAs with PCC. The risk associated with this is **low** as the configuration of the router rarely changes. Any configuration changes would happen on a yearly basis when the proposal is reviewed.
Compliance	The network engineers must follow the change management process when making any changes to the router.
Testing	1. Log into the Change Management system 2. Conduct a search for any change requests raised that corresponds to LBaP and the recent updates requested as documented in the Project Proposal History. 3. Obtain a copy of the change requests as proof that change management is being followed. Interview the network engineer and ask the following: 1. Is the change management process documented? 2. If so, please provide a copy of this documentation. 3. Is the change management process followed? 4. If so, how diligently is this followed by all network engineers that may work on this business partner connection?
Objective/Subjective	Objective Test – Viewing past changes in the system. Documented change management process. Subjective Tests – Interview based questions in relation to the change management process being followed in all situations.

20. Documentation and Diagrams for LBaP connection	
Reference	Business Partner Network Security Checklist
Control Objective	Documentation and diagrams for the business partner connection are up to date to ensure that the correct

	configuration of the router is in place.
Risk	The lack of up to date documentation may result in the incorrect configuration of the router by a new network engineer. This could expose the PCC network to unauthorised access to company confidential information. The risk associated with this is **medium** as regular audits take place to ensure that the documentation and configuration is kept up to date.
Compliance	All documentation associated with this proposal must be correct.
Testing	Compare the audit results with the current documentation to ensure it is up to date.
Objective/Subjective	This is an objective test as the documentation either matches the audit results or the current implementation is not in accordance with the documentation.

21. Solution description accurately reflects onsite configuration	
Reference	Business Partner Network Security Checklist
Control Objective	Ensure that the documented solution description accurately reflects the onsite configuration.
Risk	The solution description not accurately reflecting the onsite configuration may have numerous impacts. For example, an increase in the number of PCs that are on the segregated network may mean that the equipment supplied by PCC is now no longer adequate, the link may not be the right size, site contacts may have changed etc. The risk associated with this is **low,** as impacts to performance would be picked up as part of normal business. Changes in site contacts are the responsibility of the business unit to keep up to date as they are in constant contact with the business partner.
Compliance	The solution description documented in LBaP Proposal 125 must accurately reflect the current onsite configuration.
Testing	Audit results to be compared with the solution description.
Objective/Subjective	This is an objective test as the solution description either matches the audit results or not.

Assignment 3: Audit Evidence

Introduction

The following checklist items were considered to be the most critical for the connection between PCC and LBaP.

Checklist Results

3. Screen Saver Configuration

Test:

Check the screen saver settings for compliance.

Results:

Note: Only one screen capture is shown here as all PCs were configured the same.

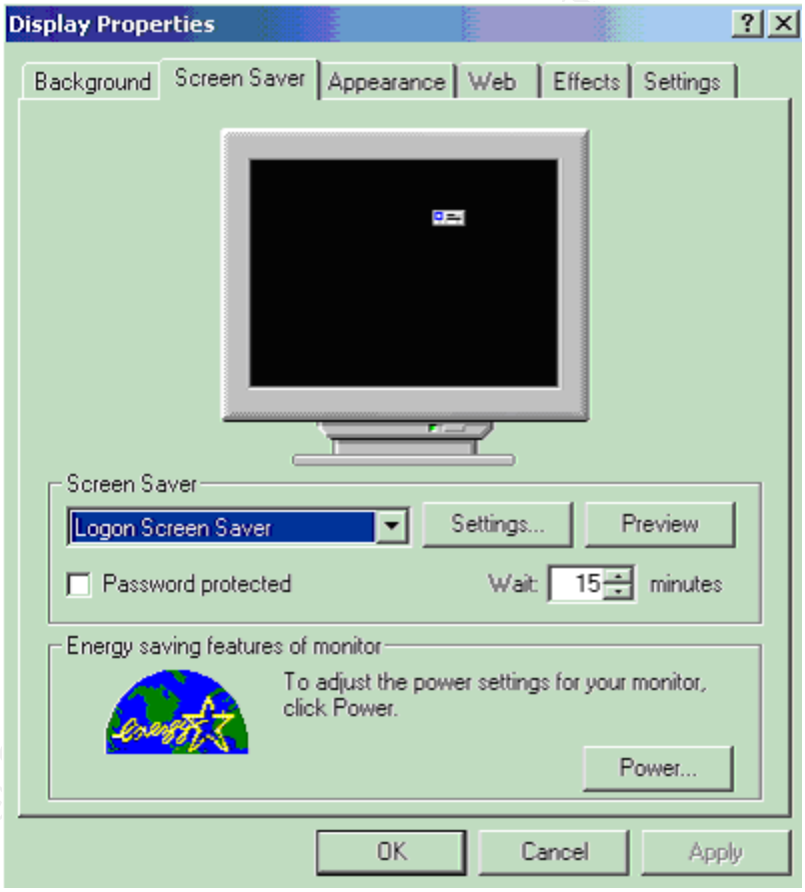


Figure 5: PC Screen Saver settings

Compliance:

Fail as although the screen saver is switched on it is not set to password protect the PC. This means that anyone can potentially gain access to any of the PCC systems that are logged into at the time.

4. Password Practices

Test:

Determine the LBaP password policy/standard.

Result:

The LBaP password standard is as follows:
Minimum length – 6 characters
Password Age – 90 days
Password History – last 5 passwords
Password Complexity – alphanumeric
Account Lockout – after 5 failed attempts

Compliance:

N/A as this is just to show the company standard.

Test:

Confirm the password configuration on the PCs.

Results:

Note: Only one screen capture is presented as all PCs are configured with the same settings.

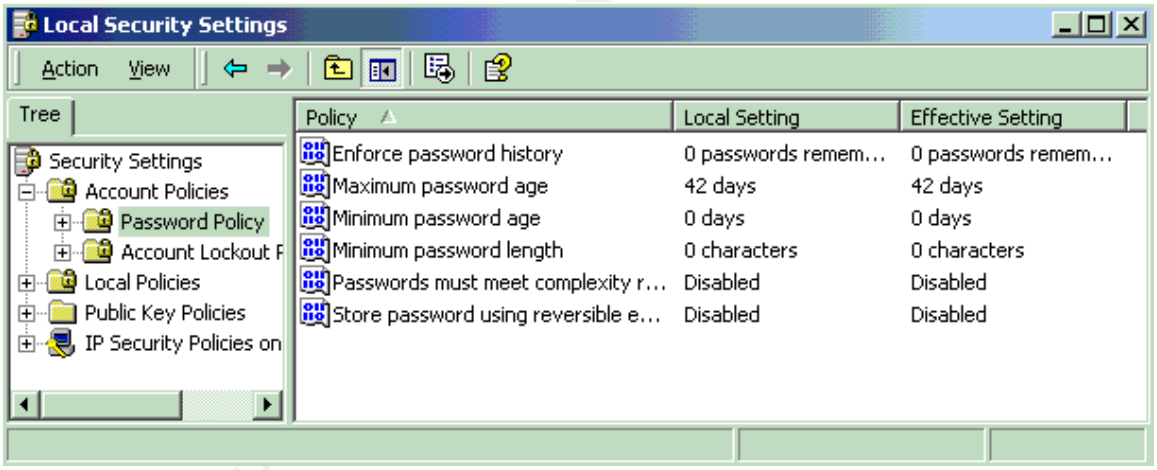


Figure 6: PC Password Settings

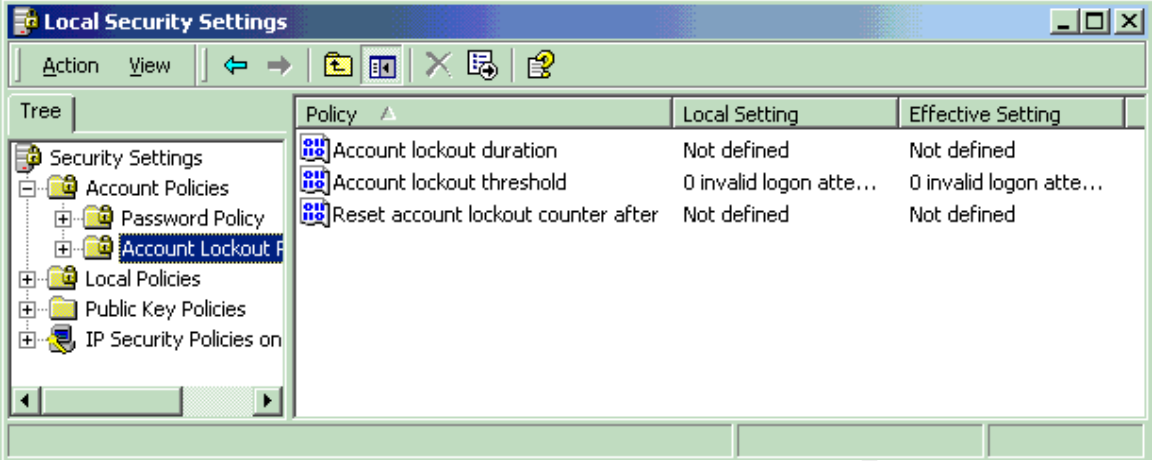


Figure 7: Account Lockout Configuration

Compliance:
Fail. None of the PCs are configured to meet the company standard. LBaP should also consider reviewing their standard and making it more stringent.

Test:
Attempt to change the password to one that is in breach of the settings and observe any error messages.

Results:
It is impossible to breach the settings of the PCs as they are all configured to allow blank passwords (see the screen capture in Figure 6 and refer to the line Minimum password length). This was tested and it was possible to enter a blank password.

Compliance:
Not Applicable.

6. Secure connectivity to the routers

Test:
Interview the network engineer to determine the method of connectivity to the routers.

Results:
Telnet is utilised to connect to lbapmelgw1 and lbapmelgw2.

Compliance:
Fail as password details are being sent in the clear when using telnet. However, from reviewing the Cisco website and the NSA Router Security Configuration Guide, there are versions of the Cisco IOS that support secure methods of communication such as SSH.

Test:
Run an Ethereal packet capture on lbapmelgw1 to confirm that the password is easily sniffed off the network.

Results:
Note: actual passwords have been removed from the copied results.

```
User Access Verification

Password: password obtained

lbapmelgw1>en

Password: password obtained
```

Figure 8: Ethereal packet capture for lbapmelgw1

Compliance:
This item passes, as it is possible to sniff the password off the network using Ethereal. However, the ideal result with this item would be a fail as this would indicate that the password is encrypted in some way thus protecting the information and reducing exposure to attack.

Test:
Run an Ethereal packet capture on lbapmelgw2 to confirm that the password is easily sniffed off the network.

Results:
Note: actual passwords have been removed from the copied results.

```
User Access Verification

Password: password obtained

lbapmelgw2>en

Password: password obtained
```

Figure 9: Ethereal packet capture for lbapmelgw2

Compliance:
This item passes, as it is possible to sniff the password off the network using Ethereal. However, the ideal result with this item would be a fail, as this would indicate that the password is encrypted in some way thus protecting the information and reducing exposure to attack.

7. Banner and configuration information

Test:
Connect to the routers and observe if any configuration information in relation to the router IOS or organisation information is provided.

Result:

```
                    PCC Internet
                  State, COUNTRY
                  ----------

                NAME: lbapmelgw1.pcc.com.

        Primary Contact:        Mon - Fri, 7am - 7pm
        PCC Network Team;       234-5678
        Backup/After hours Contact: 24 x 7 HRS
        Operation Services;     876-5432

This is a private system operated for and by the PYP Computer Corporation. Authorization from
PCC management is required to use this system.  Use by unauthorized persons is prohibited.
```

Figure 10: lbapmelgw1 Banner configuration

```
                    PCC Internet
                  State, COUNTRY
                  ----------

                NAME: lbapmelgw2.pcc.com

        Backup/After hours Contact: 24 x 7 HRS
        Operation Services;     876-5432

This is a private system operated for and by the PYP Computer Company. Authorization from PCC
management is required to use this system.  Use by unauthorized persons is prohibited.
```

Figure 11: lbapmelgw2 Banner Configuration

```
                  *** PCC $(hostname)  ***
                PCC EXTERNAL ACCESS Router (EAR)
                    Sponsored by PCC

        For Fault Reporting, please contact
        PCC Helpdesk (820-1849)
        OR email :pcc-bp_pdl@pcc.com or pcc-extaccess_pdl@pcc.com

This is private system operated for and by PYP Computer Company. Authorization from PCC
management is required to use this system. Use by unauthorised persons is prohibited.
```

Figure 12: pccear1 Banner configuration

Compliance:
Fail. The current banner provides too much information about the PCC organisation including contact phone numbers.

Test:
Check the legal banner and confirm if it meets the PCC corporate standard.

Results:
See above screen capture that includes the legal banner.

Compliance:
Fail. The legal banner should be following the corporate standard, which is “This is a private system operated for PYP Computer Company business. Authorisation from PCC management is required to use this system. Use by unauthorised person is prohibited. WARNING – This computer system is accessed by authorised users of PCC. All security and control procedures must be strictly followed.”

8. Router Password configurations

Test:
Check the show running-config results for the password settings on lbapmelgw1. Attempt to crack any passwords that are set to “enable password 7” or “password 7” for the VTY configurations and confirm if they are meeting the corporate password standards.

Results:
Note: the results shown have been modified to just show the relevant password section to enhance readability and any encrypted passwords have been removed.

```
lbapmelgw1#show running-config
Building configuration...
…
enable secret 5 "password removed".
…
line con 0
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
 transport preferred none
 transport input none
 escape-character 3
line vty 0 2
 access-class 1 in
 access-class 1 out
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
 transport preferred none
 escape-character 3
line vty 3
 access-class 20 in
 access-class 20 out
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
 transport preferred none
 escape-character 3
```

```
line vty 4
 access-class 20 in
 access-class 20 out
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
 transport preferred none
 escape-character 3
!
end

lbapmelgw1#
```

Figure 13: lbapmelgw1 password configurations

All VTY passwords were successfully cracked and found not to meet the corporate standard. The network engineer was interviewed and the enable secret password was found not to meet the corporate standard.

Compliance:
Pass on enable secret password being utilised.
Fail on compliance of VTY passwords and enable secret password to the corporate standard.

Test:
Check the show running-config results for the password settings on lbapmelgw2. Attempt to crack any passwords that are set to "enable password 7" or "password 7" for the VTY configurations and confirm if they are meeting the corporate password standards.

Results:

Note: the results shown have been modified to just show the relevant password section to enhance readability and any encrypted passwords have been removed.

```
lbapmelgw2#show running-config
Building configuration...
...
enable password 7 "password removed"
...
line con 0
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
 transport preferred none
 escape-character 3
line aux 0
line vty 0 2
 access-class 1 in
```

```
 access-class 1 out
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
 transport preferred none
 escape-character 3
line vty 3 4
 access-class 20 in
 access-class 20 out
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
 transport preferred none
 escape-character 3
!
end

lbapmelgw2#
```

Figure 14: lbapmelgw2 password configurations

The enable password was successfully cracked and found not to meet the corporate standard. All VTY passwords were successfully cracked and found not to meet the corporate standard.

Compliance:
Fail as all passwords were cracked and found not to meet the corporate standard. The enable secret 5 is also not in use.

9. Encryption level of the router password

Test:
Check to ensure the enable password has been set to "enable secret" on lbapmelgw1.

Results:
Note: Results shown have been modified to show just the enable password section to enhance readability. Encrypted passwords have been removed.

```
lbapmelgw1#show running-config
Building configuration...

Current configuration:
...
enable secret 5 "password removed".
```

Figure 15: lbapmelgw1 enable password configuration

Compliance:
Pass

Test:
Check to ensure the enable password has been set to “enable secret” on lbapmelgw2.

Results:
Note: Results shown have been modified to show just the enable password section to enhance readability. Encrypted passwords have been removed.

```
lbapmelgw2#show running-config
Building configuration...

Current configuration :
…
enable password 7 "password removed"
```

Figure 16: lbapmelgw2 enable password configuration

Compliance:
Fail as the password used for enable access is set to “enable password 7” rather than “enable secret”. This is easily configurable with all Cisco routers.

10. Authentication of remote connectivity to the routers

Test:
Determine the login credentials requested when connecting to lbapmelgw1.

Results:

```
                    PCC Internet
                  State, COUNTRY
                  ---------------

                NAME: lbapmelgw1.pcc.com.

        Primary Contact:        Mon - Fri, 7am - 7pm
        PCC Network Team;       234-5678
        Backup/After hours Contact: 24 x 7 HRS
        Operation Services;     876-5432

This is a private system operated for and by the PYP Computer Corporation. Authorization from
PCC management is required to use this system.  Use by unauthorized persons is prohibited.

User Access Verification

Password:
```

Figure 17: lbapmelgw1 authentication prompt

Compliance:
Fail as the router is only prompting for a password. It is possible to configure the Cisco router to prompt for a username and password (this may be an individual or generic account) or utilise an authentication server such as TACACS+.

Test:
Determine the login credentials requested when connecting to lbapmelgw2.

Results:

```
                    PCC Internet
                    State, COUNTRY
                    --------------------

                    NAME: lbapmelgw2.pcc.com

        Backup/After hours Contact: 24 x 7 HRS
        Operation Services;       876-5432

This is a private system operated for and by the PYP Computer Company. Authorization from PCC
management is required to use this system.  Use by unauthorized persons is prohibited.

User Access Verification

Password:
```

Figure 18: lbapmelgw2 authentication prompt

Compliance:
Fail as the router is only prompting for a password. It is possible to configure the Cisco router to prompt for a username and password (this may be an individual or generic account) or utilise an authentication server such as TACACS+.

11a. Router ACL Configuration

Test:
Connect to the router lbapmelgw1 and obtain the ACL listing.

Results:
The following results show the access lists on the Ethernet1 interface between the segregated network and the DMZ. Access lists 1, 20 & 21 relate to the access lists on the VTY and will be covered in checklist item 20. Access list 100 is the outbound access from the segregated network to the DMZ. Access list 100 is inbound access from the DMZ to the segregated network. There are no access lists on the Ethernet0 or BRI0 interfaces on lbapmelgw1.

```
access-list 1 permit 192.168.47.230
access-list 1 permit 192.168.255.250
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 1 deny   any
access-list 20 permit 10.30.152.10
access-list 20 permit 10.23.67.254
access-list 20 permit 10.0.193.2
access-list 20 deny   any
access-list 21 permit 10.30.152.10
access-list 21 permit 10.23.67.254
access-list 21 deny   any
```

```
access-list 100 permit icmp 192.168.32.0 0.0.0.255 172.31.10.0 0.0.0.255 echo
access-list 100 permit icmp 192.168.32.0 0.0.0.255 192.168.47.228 0.0.0.3 echo
access-list 100 permit tcp 192.168.32.0 0.0.0.255 172.31.10.0 0.0.0.255
access-list 100 permit tcp 192.168.32.0 0.0.0.255 192.168.47.228 0.0.0.3
access-list 100 permit tcp 172.26.77.128 0.0.0.15 192.168.32.0 0.0.0.255 established
access-list 100 permit tcp 172.26.77.128 0.0.0.15 192.168.32.0 0.0.0.255 eq 8080
access-list 100 permit tcp 172.26.77.128 0.0.0.15 192.168.32.0 0.0.0.255 eq www
access-list 100 deny   ip any any
access-list 101 permit icmp 172.31.10.0 0.0.0.255 192.168.32.0 0.0.0.255 echo-reply
access-list 101 permit icmp 192.168.47.228 0.0.0.3 192.168.32.0 0.0.0.255 echo-reply
access-list 101 permit icmp 192.168.47.228 0.0.0.3 192.168.47.228 0.0.0.3 echo-reply
access-list 101 permit icmp 172.31.10.0 0.0.0.255 192.168.47.228 0.0.0.3 echo-reply
access-list 101 permit tcp 172.31.10.0 0.0.0.255 192.168.32.0 0.0.0.255 established
access-list 101 permit tcp 192.168.47.228 0.0.0.3 192.168.47.228 0.0.0.3 established
access-list 101 permit tcp 192.168.32.0 0.0.0.255 172.26.77.128 0.0.0.15 eq 8080
access-list 101 permit tcp 192.168.32.0 0.0.0.255 172.26.77.128 0.0.0.15 eq www
access-list 101 permit tcp 192.168.32.0 0.0.0.255 172.26.77.128 0.0.0.15 established
access-list 101 deny   ip any any
```

Figure 19: ACLs for lbapmelgw1

Compliance:
Fail. With access list 101, there are three entries that imply the source address is the same network as that connected to lbapmelgw1's Ethernet0 interface – eg: access-list 101 permit TCP 192.168.32.0 0.0.0.255 172.26.77.128 0.0.0.15 eq 8080. Whilst it would be technically possible that this subnet space was used within the LBaP corporate network it would never receive return traffic as lbapmelgw1 would route any traffic destined for this subnet via Ethernet0 not Ethernet1. As such the corresponding entry in access list 100 (outgoing from Ethernet1 to the DMZ/LBaP corporate network) would never see matches. Added to this, there is no network with the range 172.26.77.x connected to lbapmelgw1. This configuration is also not referenced in the proposal document.

Test:
Connect to the router pccear1 and obtain the ACL listing.

Results:
The following results show the access lists on the WAN interface for the LBaP link on pccear1. Access list 140 is the outbound access from the PCC network to LBaP segregated network. Access list 141 is the inbound access from the LBaP network to the PCC network. All other access lists on this router are not applicable to the LBaP connection and are therefore excluded from the test results.

Note: additional white space has been added to the results to improve readability.

```
access-list 140 permit icmp host  10.0.193.2 host 192.168.47.106
access-list 140 permit icmp host  10.0.193.2 host 192.168.32.1

access-list 140 permit tcp host 10.0.232.218 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.0.232.219 192.168.32.0 0.0.0.127 established
access-list 140 permit udp host 10.0.232.218 192.168.32.0 0.0.0.127 gt 1023
```

```
access-list 140 permit udp host 10.0.232.219 192.168.32.0 0.0.0.127 gt 1023
access-list 140 permit udp host 10.0.232.241 192.168.32.0 0.0.0.127 gt 1023
access-list 140 permit udp host 10.0.232.242 192.168.32.0 0.0.0.127 gt 1023
access-list 140 permit tcp host 10.19.200.13 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.28.132.91 192.168.32.0 0.0.0.127 established
access-list 140 permit udp host 10.28.132.91 192.168.32.0 0.0.0.127 gt 1023
access-list 140 permit tcp host 10.28.132.152 192.168.32.0 0.0.0.127 established
access-list 140 permit udp host 10.28.132.152 192.168.32.0 0.0.0.127 gt 1023
access-list 140 permit udp host 10.28.133.60 192.168.32.0 0.0.0.127 range 1289 1290
access-list 140 permit udp host 10.28.133.65 192.168.32.0 0.0.0.127 range 1289 1290
access-list 140 permit tcp host 10.56.8.57 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.66.153.35 192.168.32.0 0.0.0.127 established
access-list 140 permit udp host 10.66.154.199 192.168.32.0 0.0.0.127 eq 1269
access-list 140 permit udp host 10.66.154.199 192.168.32.0 0.0.0.127 gt 1023
access-list 140 permit tcp host 10.66.156.77 192.168.32.0 0.0.0.127 established
access-list 140 permit udp host 10.66.156.77 192.168.32.0 0.0.0.127 gt 1023
access-list 140 permit tcp host 10.66.156.78 192.168.32.0 0.0.0.127 established
access-list 140 permit udp host 10.66.156.78 192.168.32.0 0.0.0.127 gt 1023
access-list 140 permit tcp host 10.68.1.29 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.68.10.213 192.168.42.0 0.0.0.127 established
access-list 140 permit tcp host 10.68.10.214 192.168.42.0 0.0.0.127 established
access-list 140 permit udp host 10.68.10.220 192.168.42.0 0.0.0.127 eq 1269
access-list 140 permit tcp host 10.73.170.149 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.73.170.250 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.76.192.60 192.168.32.0 0.0.0.127 established
access-list 140 permit udp host 10.76.192.64 192.168.32.0 0.0.0.127 eq 1503
access-list 140 permit tcp host 10.76.192.64 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.85.49.5 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.192.0.254 192.168.42.0 0.0.0.127 established
access-list 140 permit tcp host 10.208.1.11 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.224.0.55 192.168.42.0 0.0.0.127 established
access-list 140 permit tcp host 10.176.212.70 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.176.212.75 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.176.212.74 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.172.40.177 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.110.16.87 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.176.212.45 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 10.176.4.97 192.168.32.0 0.0.0.127 established
access-list 140 deny   ip 10.0.0.0 0.255.255.255 any

access-list 140 permit tcp host 192.168.6.182 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 192.168.13.70 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 192.168.40.100 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 192.168.40.101 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 192.168.43.4 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.16.64.56 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.20.118.44 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.20.118.93 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.20.118.97 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.20.118.128 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.20.164.28 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.20.164.84 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.20.164.85 192.168.32.0 0.0.0.127 established
```

```
access-list 140 permit tcp host 172.20.165.133 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.22.10.28 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.22.11.40 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.26.64.39 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.26.77.91 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp host 172.26.77.95 192.168.32.0 0.0.0.127 established
access-list 140 permit tcp 172.26.77.128 0.0.0.15 192.168.32.0 0.0.0.255 established
access-list 140 deny   ip any any
```

Figure 20: ACL 140 for pccear1

```
access-list 141 deny   ip 10.0.0.0 0.255.255.255 any
access-list 141 permit icmp host 192.168.47.106 host 10.0.193.2
access-list 141 permit icmp host 192.168.32.1 host 10.0.193.2

access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.0.232.218 range 5201 5202
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.0.232.218 range 9500 9699
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.0.232.219 range 5201 5202
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.0.232.219 range 9500 9699
access-list 141 permit udp 192.168.32.0 0.0.0.127 host 10.0.232.218 eq 1289
access-list 141 permit udp 192.168.32.0 0.0.0.127 host 10.0.232.219 eq 1289
access-list 141 permit udp 192.168.32.0 0.0.0.127 host 10.0.232.241 eq 1289
access-list 141 permit udp 192.168.32.0 0.0.0.127 host 10.0.232.242 eq 1289
access-list 141 permit udp 192.168.32.0 0.0.0.127 host 10.28.132.91 range 1289 1290
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.28.132.91 range 5201 5202
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.28.132.91 range 9500 9699
access-list 141 permit udp 192.168.32.0 0.0.0.127 host 10.28.132.152 range 1289 1290
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.28.132.152 range 5201 5202
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.28.132.152 range 9500 9699
access-list 141 permit udp 192.168.32.0 0.0.0.127 host 10.28.133.60 range 1289 1290
access-list 141 permit udp 192.168.32.0 0.0.0.127 host 10.28.133.65 range 1289 1290
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.56.8.57 eq 5729
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.66.153.35 eq 5022
access-list 141 permit udp 192.168.32.0 0.0.0.127 host 10.66.154.199 eq 1269
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.66.156.77 range 5804 5805
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.66.156.77 range 9500 9699
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.66.156.78 range 5804 5805
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.66.156.78 range 9500 9699
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.68.1.29 eq 1570
access-list 141 permit tcp 192.168.42.0 0.0.0.127 host 10.68.10.213 range 5804 5805
access-list 141 permit tcp 192.168.42.0 0.0.0.127 host 10.68.10.213 range 9700 9899
access-list 141 permit tcp 192.168.42.0 0.0.0.127 host 10.68.10.214 range 5804 5805
access-list 141 permit tcp 192.168.42.0 0.0.0.127 host 10.68.10.214 range 9700 9899
access-list 141 permit udp 192.168.42.0 0.0.0.127 host 10.68.10.220 eq 1269
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.73.170.149 eq 5012
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.73.170.149 eq 5102
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.73.170.250 eq 1494
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.76.192.60 eq www
access-list 141 permit udp 192.168.32.0 0.0.0.127 host 10.76.192.64 eq 1503
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.76.192.64 range 1504 1505
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.85.49.5 eq 25
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.85.49.5 eq 110
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.85.49.5 eq 143
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.85.49.5 eq 389
```

```
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.85.49.5 eq 5729
access-list 141 permit tcp 192.168.42.0 0.0.0.127 host 10.192.0.254 eq 443
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.208.1.11 eq 443
access-list 141 permit tcp 192.168.42.0 0.0.0.127 host 10.224.0.55 eq 443
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.176.212.70 eq 1433
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.176.212.75 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.176.212.74 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.172.40.177 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.110.16.87 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.176.212.45 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 10.176.4.97 eq www
access-list 141 deny   ip any 10.0.0.0 0.255.255.255

access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 192.168.6.182 eq 3467
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 192.168.6.182 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 192.168.13.70 eq 8081
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 192.168.13.70 eq 8087
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 192.168.40.101 eq 8081
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 192.168.40.101 eq 8087
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 192.168.43.4 eq 80
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.16.64.56 eq 443
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.118.93 eq 8483
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.118.93 eq 446
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.118.97 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.118.128 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.118.44 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.164.28 eq 4100
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.164.84 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.164.84 eq 443
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.164.85 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.164.85 eq 443
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.164.85 eq 4100
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.20.165.133 range 2004 2005
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.22.11.40 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.22.10.28 eq 4100
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.26.64.39 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.26.77.91 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.26.77.91 eq 443
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.26.77.95 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.26.77.95 eq 443
access-list 141 permit tcp 192.168.32.0 0.0.0.127 host 172.26.77.95 eq 4100

access-list 141 permit tcp 192.168.32.0 0.0.0.127 172.26.77.128 0.0.0.15 eq www
access-list 141 permit tcp 192.168.32.0 0.0.0.127 172.26.77.128 0.0.0.15 eq 8080
access-list 141 deny   ip any any
```

Figure 21: ACL 141 for pccear1

Compliance:

Fail. The vast majority of ACLs configured on the router are not listed in the proposal document. There is also one system in the proposal that does not appear to be contained in the ACLs – 172.26.66.72. It is clear that either the ACLs have been

configured incorrectly on the router or the proposal document has not been kept up to date as required. These ACLs need to be reviewed and corrected as appropriate.

Test:
Connect to the router lbapmelgw2 and obtain the ACL listing.

Results:
The following results show the access lists on the VTY sessions. There are no other access lists on the Ethernet1 or Ethernet0 interfaces.

```
access-list 1 permit 172.31.10.0 0.0.0.255
access-list 1 permit 192.168.47.220 0.0.0.3
access-list 1 permit 192.168.47.228 0.0.0.3
access-list 1 deny   any
access-list 20 permit 192.168.47.220 0.0.0.3
access-list 20 permit 192.168.47.228 0.0.0.3
access-list 20 deny   any
```

Figure 22: ACLs for lbapmelgw2

Compliance:
Pass, as the proposal document does not indicate that any ACLs should be configured on lbapmelgw2. VTY session access lists will be covered in checklist item 20.

11b. Overall Router Configuration

Test:
Run CISecurity's Router Assessment Tool on lbapmelgw1

Results:

lbapmelgw1 Audit Date: Wed Jun 18 03:37:47 2003 GMT					
Importance	**Pass/Fail**	**Rule Name**	**Device**	**Instance**	**Line Number**
10	FAIL	IOS - Apply telnet ACL	lbapmelgw1	vty 0 2	155
10	FAIL	IOS - Apply telnet ACL	lbapmelgw1	vty 3	164
10	FAIL	IOS - Apply telnet ACL	lbapmelgw1	vty 4	173
10	FAIL	IOS - Define telnet ACL	lbapmelgw1	n/a	1
10	Pass	IOS - enable secret	lbapmelgw1		
10	Pass	IOS - forbid SNMP community private	lbapmelgw1		
10	Pass	IOS - forbid SNMP community public	lbapmelgw1		
10	Pass	IOS - login	lbapmelgw1		
10	Pass	IOS - no ip http server	lbapmelgw1		
10	FAIL	IOS - no snmp-server	lbapmelgw1	n/a	120
10	Pass	IOS - require line passwords	lbapmelgw1		
7	Pass	IOS - encrypt passwords	lbapmelgw1		
7	FAIL	IOS - exec-timeout	lbapmelgw1	con 0	147

7	FAIL	IOS - exec-timeout	lbapmelgw1	vty 0 2	155
7	FAIL	IOS - exec-timeout	lbapmelgw1	vty 3	164
7	FAIL	IOS - exec-timeout	lbapmelgw1	vty 4	173
7	FAIL	IOS - no cdp run	lbapmelgw1	n/a	1
7	Pass	IOS - no ip source-route	lbapmelgw1		
7	Pass	IOS - no service config	lbapmelgw1		
7	Pass	IOS 12 - no directed broadcast	lbapmelgw1		
7	Pass	IOS 12 - no tcp-small-servers	lbapmelgw1		
7	Pass	IOS 12 - no udp-small-servers	lbapmelgw1		
5	Pass	IOS - enable logging	lbapmelgw1		
5	FAIL	IOS - logging buffered	lbapmelgw1	n/a	1
5	FAIL	IOS - no ip bootp server	lbapmelgw1	n/a	1
5	FAIL	IOS - no ip proxy-arp	lbapmelgw1	Ethernet0	34
5	FAIL	IOS - no ip proxy-arp	lbapmelgw1	Ethernet1	40
5	FAIL	IOS - no ip proxy-arp	lbapmelgw1	BRI0	48
5	FAIL	IOS - ntp server	lbapmelgw1	n/a	1
5	FAIL	IOS - ntp source	lbapmelgw1	n/a	1
5	FAIL	IOS - set syslog server	lbapmelgw1	n/a	1
5	FAIL	IOS - vty transport telnet	lbapmelgw1	vty 0 2	155
5	FAIL	IOS - vty transport telnet	lbapmelgw1	vty 3	164
5	FAIL	IOS - vty transport telnet	lbapmelgw1	vty 4	173
5	Pass	IOS 12 - no finger service	lbapmelgw1		
3	FAIL	IOS - clock timezone	lbapmelgw1	n/a	1
3	Pass	IOS - disable aux	lbapmelgw1		
3	FAIL	IOS - logging console critical	lbapmelgw1	n/a	1
3	FAIL	IOS - logging trap debugging	lbapmelgw1	n/a	1

Summary for lbapmelgw1

#Checks	#Passed	#Failed	%Passed
39	15	24	38

Perfect Weighted Score	Actual Weighted Score	%Weighted Score
264	115	43

Overall Score (0-10)
4.3

Note: PerfectWeightedScore is the sum of the importance value of all rules. ActualWeightedScore is the sum of the importance value of all rules passed, minus the sum of the importance each instance of a rule failed.

Figure 23: Router Assessment Tool results for lbapmelgw1

Compliance:
Fail. The majority of tests performed by the RAT show that there is a great deal of work that needs to be done on the configuration of lbapmelgw1 to improve it's security.

Test:
Run CISecurity's Router Assessment Tool on lbapmelgw2.

Results:

lbapmelgw2 Audit Date: Wed Jun 18 03:38:27 2003 GMT					
Importance	**Pass/Fail**	**Rule Name**	**Device**	**Instance**	**Line Number**
10	FAIL	IOS - Apply telnet ACL	lbapmelgw2	vty 0 2	88
10	FAIL	IOS - Apply telnet ACL	lbapmelgw2	vty 3 4	97
10	FAIL	IOS - Define telnet ACL	lbapmelgw2	n/a	1
10	FAIL	IOS - enable secret	lbapmelgw2	n/a	1
10	Pass	IOS - forbid SNMP community private	lbapmelgw2		
10	Pass	IOS - forbid SNMP community public	lbapmelgw2		
10	FAIL	IOS - login	lbapmelgw2	aux 0	87
10	FAIL	IOS - no ip http server	lbapmelgw2	n/a	51
10	FAIL	IOS - no snmp-server	lbapmelgw2	n/a	60
10	FAIL	IOS - require line passwords	lbapmelgw2	aux 0	87
7	Pass	IOS - encrypt passwords	lbapmelgw2		
7	FAIL	IOS - exec-timeout	lbapmelgw2	con 0	80
7	FAIL	IOS - exec-timeout	lbapmelgw2	aux 0	87
7	FAIL	IOS - exec-timeout	lbapmelgw2	vty 0 2	88
7	FAIL	IOS - exec-timeout	lbapmelgw2	vty 3 4	97
7	FAIL	IOS - no cdp run	lbapmelgw2	n/a	1
7	Pass	IOS - no ip source-route	lbapmelgw2		
7	Pass	IOS - no service config	lbapmelgw2		
7	Pass	IOS 12 - no directed broadcast	lbapmelgw2		
7	Pass	IOS 12 - no tcp-small-servers	lbapmelgw2		
7	Pass	IOS 12 - no udp-small-servers	lbapmelgw2		
5	Pass	IOS - enable logging	lbapmelgw2		
5	FAIL	IOS - logging buffered	lbapmelgw2	n/a	1
5	FAIL	IOS - no ip bootp server	lbapmelgw2	n/a	1
5	FAIL	IOS - no ip proxy-arp	lbapmelgw2	Ethernet0	24
5	FAIL	IOS - no ip proxy-arp	lbapmelgw2	Ethernet1	29
5	FAIL	IOS - no ip proxy-arp	lbapmelgw2	Serial0	34
5	FAIL	IOS - no ip proxy-arp	lbapmelgw2	Serial1	39
5	FAIL	IOS - ntp server	lbapmelgw2	n/a	1
5	FAIL	IOS - ntp source	lbapmelgw2	n/a	1
5	FAIL	IOS - set syslog server	lbapmelgw2	n/a	1
5	FAIL	IOS - vty transport telnet	lbapmelgw2	vty 0 2	88
5	FAIL	IOS - vty transport telnet	lbapmelgw2	vty 3 4	97
5	Pass	IOS 12 - no finger service	lbapmelgw2		
3	FAIL	IOS - clock timezone	lbapmelgw2	n/a	1

3	FAIL	IOS - disable aux	lbapmelgw2	aux 0	87
3	FAIL	IOS - logging console critical	lbapmelgw2	n/a	1
3	FAIL	IOS - logging trap debugging	lbapmelgw2	n/a	1

Summary for lbapmelgw2

#Checks	#Passed	#Failed	%Passed
38	10	28	26

Perfect Weighted Score	Actual Weighted Score	%Weighted Score
254	72	28

Overall Score (0-10)
2.8

Note: PerfectWeightedScore is the sum of the importance value of all rules. ActualWeightedScore is the sum of the importance value of all rules passed, minus the sum of the importance each instance of a rule failed.

Figure 24: Router Assessment Tool results for lbapmelgw2

Compliance:
Fail. The results from the RAT show that there are a number of actions that need to take place to improve the security of the router.

Test:
Run CISecurity's Router Assessment Tool on pccear1.

Results:

Pccear1

Audit Date: Fri Jun 27 03:51:56 2003 GMT

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	FAIL	IOS - Apply telnet ACL	pccear1	vty 0 3	1990
10	FAIL	IOS - Apply telnet ACL	pccear1	vty 4	1998
10	FAIL	IOS - Define telnet ACL	pccear1	n/a	1
10	Pass	IOS - enable secret	pccear1		
10	Pass	IOS - forbid SNMP community private	pccear1		
10	Pass	IOS - forbid SNMP community public	pccear1		
10	FAIL	IOS - login	pccear1	aux 0	1981
10	Pass	IOS - no ip http server	pccear1		
10	FAIL	IOS - no snmp-server	pccear1	n/a	1943
10	FAIL	IOS - require line passwords	pccear1	con 0	1967
10	FAIL	IOS - require line passwords	pccear1	vty 0 3	1990

10	FAIL	IOS - require line passwords	pccear1	vty 4	1998
7	Pass	IOS - encrypt passwords	pccear1		
7	Pass	IOS - exec-timeout	pccear1		
7	FAIL	IOS - no cdp run	pccear1	n/a	1
7	Pass	IOS - no ip source-route	pccear1		
7	Pass	IOS - no service config	pccear1		
7	Pass	IOS 12 - no directed broadcast	pccear1		
7	Pass	IOS 12 - no tcp-small-servers	pccear1		
7	Pass	IOS 12 - no udp-small-servers	pccear1		
5	Pass	IOS - enable logging	pccear1		
5	FAIL	IOS - logging buffered	pccear1	n/a	1
5	FAIL	IOS - no ip bootp server	pccear1	n/a	1
5	FAIL	IOS - no ip proxy-arp	pccear1	Loopback 0	58
5	FAIL	IOS - no ip proxy-arp	pccear1	Ethernet0/0	62
5	FAIL	IOS - no ip proxy-arp	pccear1	Ethernet0/1	68
5	FAIL	IOS - no ip proxy-arp	pccear1	Ethernet 1/0	74
5	FAIL	IOS - no ip proxy-arp	pccear1	Ethernet 1/1	79
5	FAIL	IOS - no ip proxy-arp	pccear1	Ethernet 1/2	85
5	FAIL	IOS - no ip proxy-arp	pccear1	Ethernet 1/3	
5	FAIL	IOS - no ip proxy-arp	pccear1	Serial2/0	100
5	FAIL	IOS - no ip proxy-arp	pccear1	Serial2/0.16	113
5	FAIL	IOS - no ip proxy-arp	pccear1	Serial2/1	121
5	FAIL	IOS - no ip proxy-arp	pccear1	Serial2/2	128
5	FAIL	IOS - no ip proxy-arp	pccear1	Serial2/3	138
5	FAIL	IOS - no ip proxy-arp	pccear1	Serial3/0:15	143
5	FAIL	IOS - no ip proxy-arp	pccear1	Dialer1	152
5	FAIL	IOS - no ip proxy-arp	pccear1	Dialer2	168
5	FAIL	IOS - no ip proxy-arp	pccear1	Dialer3	184
5	FAIL	IOS - no ip proxy-arp	pccear1	Dialer4	200
5	FAIL	IOS - no ip proxy-arp	pccear1	Dialer5	216
5	FAIL	IOS - no ip proxy-arp	pccear1	Dialer7	230
5	FAIL	IOS - no ip proxy-arp	pccear1	Dialer9	236
5	FAIL	IOS - no ip proxy-arp	pccear1	Dialer10	251
5	FAIL	IOS - no ip proxy-arp	pccear1	Dialer11	258
5	FAIL	IOS - no ip proxy-arp	pccear1	Dialer12	270
5	FAIL	IOS - no ip proxy-arp	pccear1	Dialer13	277
5	FAIL	IOS - ntp server	pccear1	n/a	1
5	FAIL	IOS - ntp source	pccear1	n/a	1
5	FAIL	IOS - set syslog server	pccear1	n/a	1
5	FAIL	IOS - vty transport telnet	pccear1	vty 0 3	1990
5	FAIL	IOS - vty transport telnet	pccear1	vty 4	1998
5	Pass	IOS 12 - no finger	pccear1		

		service			
3	FAIL	IOS - clock timezone	pccear1	n/a	1
3	Pass	IOS - disable aux	pccear1		
3	FAIL	IOS - logging console critical	pccear1	n/a	1
3	FAIL	IOS - logging trap debugging	pccear1	n/a	1

Summary for pccear1

#Checks	#Passed	#Failed	%Passed
57	14	43	24

Perfect Weighted Score	Actual Weighted Score	%Weighted Score
353	102	28

Overall Score (0-10)
2.8

Note: PerfectWeightedScore is the sum of the importance value of all rules. ActualWeightedScore is the sum of the importance value of all rules passed, minus the sum of the importance each instance of a rule failed.

Figure 25: Router Assessment Tool Results for pccear1

Compliance:
Fail. The results from the RAT show that there are a number of actions that need to take place to improve the security of the router.

12. VTY Access Restrictions

Test:
Check the VTY access list and confirm that none of the IP addresses are from the LBaP corporate network or the segregated network for lbapmelgw1 and lbapmelgw2.

Results:

```
line vty 0 2
 access-class 1 in
 access-class 1 out
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
 transport preferred none
 escape-character 3
line vty 3
 access-class 20 in
 access-class 20 out
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
```

```
 transport preferred none
 escape-character 3
line vty 4
 access-class 20 in
 access-class 20 out
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
 transport preferred none
 escape-character 3
```

Figure 26: lbapmelgw1 VTY configuration

```
access-list 1 permit 192.168.47.230
access-list 1 permit 192.168.255.250
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 1 deny   any
access-list 20 permit 10.30.152.10
access-list 20 permit 10.23.67.254
access-list 20 permit 10.0.193.2
access-list 20 deny   any
access-list 21 permit 10.30.152.10
access-list 21 permit 10.23.67.254
access-list 21 deny   any
```

Figure 27: lbapmelgw1 VTY Access Lists

```
line vty 0 2
 access-class 1 in
 access-class 1 out
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
 transport preferred none
 escape-character 3
line vty 3 4
 access-class 20 in
 access-class 20 out
 exec-timeout 15 0
 password 7 "password removed"
 no vacant-message
 login
 transport preferred none
 escape-character 3
```

Figure 28: lbapmelgw2 VTY configuration

```
access-list 1 permit 172.31.10.0 0.0.0.255
access-list 1 permit 192.168.47.220 0.0.0.3
access-list 1 permit 192.168.47.228 0.0.0.3
access-list 1 deny   any
access-list 20 permit 192.168.47.220 0.0.0.3
access-list 20 permit 192.168.47.228 0.0.0.3
access-list 20 deny   any
```

Figure 29: lbapmelgw2 VTY Access Lists

Compliance:
The access lists on lbapmelgw1 pass, as they do not allow access from the LBaP corporate network or the segregated network. However, there is a superfluous access list in the form of access list 21 which could be removed. The access list on lbapmelgw2 pass, as they do not allow access from the LBaP corporate network or the segregated network. However, the IP address 192.168.47.220 does not appear to be a valid IP address for this implementation and should be reviewed for its validity.

15. Router Patch Management

Test:
Connect to the router lbapmelgw1 and determine the IOS version.

Results:

```
lbapmelgw1>show version
Cisco Internetwork Operating System Software
IOS (tm) 1600 Software (C1600-Y-M), Version 12.0(7)T,  RELEASE SOFTWARE (fc2)
```

Figure 30: lbapmelgw1 show version

Compliance:
Fail. IOS releases are now at 12.3 however due to the End of Life of the 1600 series of routers only limited feature set of IOS 12.3 will be supported. The hardware configuration of the router may also preclude the ability to upgrade to the latest IOS.

Test:
Connect to the router lbapmelgw2 and determine the IOS version.

Results:

```
lbapmelgw2#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-I-L), Version 12.1(10), RELEASE SOFTWARE (fc1)
```

Figure 31: lbapmelgw2 show version

Compliance:
Fail. Cisco has released IOS version 12.3.

Test:
Connect to the router pccear1 and determine the IOS version

Results:

```
pccear1>show version
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-I-M), Version 12.2(10b), RELEASE SOFTWARE (fc1)
```

Figure 32: pccear1 show version

Compliance:
Fail. Cisco has released IOS version 12.3

Test:
Determine if a patch management process is in place to ensure patching is kept up to date.

Results:
There is no patch management process in place and there appears to be no subscription to alert lists such as CERT or Cisco's alert notifications.

Compliance:
Fail. This is not complying with the corporate standards that stipulate a patch management process be documented and followed for all network equipment. This is exposing the PCC network with any business partner connection.

16. Logging

Test:
Connect to the routers and determine if logging is switched on.

Results:
Note: the results shown have been modified to just show the relevant logging section to enhance readability.

```
lbapmelgw1#show running-config
...
...
logging buffered 10000 debugging
```

Figure 33: lbapmelgw1 logging screen capture

```
lbapmelgw2#show running-config
...
...
logging buffered 10000 debugging
```

Figure 34: lbapmelgw2 logging screen capture

```
pccear1#show running-config
...
...
logging buffered 200000 debugging
```

Figure 35: pccear1 logging screen capture

Compliance:
Pass as logging is enabled

Test:
Check the access lists from Checklist Item 11a and review to determine if access is being logged.

Results:
No “log” statement found at the end of any of the access lists.

Compliance:
Fail. There is no evidence that any logging is being done on any of the access lists, as there is no “log” statement found at the end of each access list. It is therefore not possible to find out if any access is being attempted on ports that are denied and the network team would not be aware of any unauthorised attempts to access the PCC network.

Test:
Check the “show running-config” results to determine if logging information is being sent to a server to allow for retention for investigative purposes.

Result:
No entry in the “show running-config” results with the command “logging” followed by an IP address on lbapmelgw1, lbapmelgw2 or pccear1. Therefore the log files are not being sent to a server to allow for retention and investigative purposes.

Compliance:
Fail, as the logs from the routers should be sent to a server to ensure that any incidents are identified and evidence to support investigations is available.

Test:
Ensure the retention period of the log files meet the corporate policy

Result:
No interview conducted as no logs are being stored on a system

Compliance:
Fail.

17. Auditing and Monitoring
Test:
Interview the network engineer to determine the level of auditing and monitoring, if any.

Results:
Q. Is there any monitoring performed on the routers lbapmelgw1 and lbapmelgw2?
A. No. The router logs are not being sent to a server and hence cannot be monitored. See checklist item 12 for supporting evidence of no server storing the log files.
Q. Is there any auditing performed on the router logs to address areas such as performance issues, intrusion attempts etc?
A. No. Only investigated when users log a call in relation to performance issues.

Compliance:
Fail. The network team is unable to identify any intrusion attempts or attacks that may be occurring at any time. There is no evidence being gathered to support any investigations that may be possible. Any support would be done in a reactive manner rather than a proactive manner.

Measure Residual Risk

As a result of conducting the audit on the connection between PCC and LBaP it is clear that there are a number of areas that need to be improved to reduce risk. Many of these areas should already have been implemented as part of the proposal, which was designed to mitigate a number of risks.

The majority of the technical risks can easily be mitigated by doing a thorough clean up of the router configurations. ACLs, authentication, legal banners, passwords etc can all be rectified but require the commitment of resources to complete. Given the large gap between what is configured on the routers and what is documented in the proposal, there is a high exposure to PCC. Users on the segregated network appear to have access to systems they do not need access to. This has the potential for unauthorised access to PCC systems and disclosure of company confidential information. The upgrade of the routers to the latest IOS needs to be considered carefully. Upgrading the IOS on a router tends to require more memory in the router and not all the feature sets of the new IOS may be available with the model of router in use. PCC needs to weigh up the cost associated with an upgrade versus the risk and other mitigating actions they can/have already in place. For example, the firewall between pccear1 and the internal PCC network may be configured to prevent known attacks from penetrating the PCC network.

The physical security at LBaP is of a high standard with access cards required for all areas of the building, especially the computer room where the PCC equipment is located. However, the password configuration and screen saver settings need to be improved. This is a simple matter of bringing the password configuration up to the LBaP corporate standard and enabling the password protect component of the screen saver. Given the small number of PCs this would require little effort on behalf of the business partner and would be a “quick win” for tightening the desktop PC security.

Providing some of the actions mentioned above are performed the residual risk falls within tolerable levels in order for PCC to balance business needs with security requirements. Given the scope of the audit and the controls described in each checklist item, the control objectives were achieved with this audit.

Is the system auditable?

Given the scope of this audit, the majority of areas were auditable. The fact that PCC have a defined process in place for assessing and approving business partner connections has also assisted with ensuring there are defined policies and processes to audit against. However, there was one area where validation was not possible.

Although logging was enabled on all three routers, none of the logs were being stored on a server where they could be monitored and audited. This means that it is not possible to validate that any performance issues are picked up in a proactive rather than reactive manner, any attacks or intrusion attempts would go unnoticed and any errors being logged by the routers would not be identified. In order to mitigate this risk, the logs need to be sent to a server for monitoring and auditing. This will also result in being able to validate this audit item during future audits of this business partner connection.

Assignment 4: Audit Report

Executive Summary

This audit reviewed the connection of the business partner LBaP to PCC's corporate network. The audit covers the adherence of the business partner to the mitigating options identified in the proposal document for this business partner, adherence of the hardware configuration to that documented in the proposal and adherence to PCC's security policies, processes and standards.

The major area of concern is with the configuration of the routers connecting LBaP to PCC. Based on the results from the audit, there are a number of entries on the router controlling access to the PCC systems that should not be there. This is providing LBaP employees with greater access to the PCC systems to which they do not have authorised access. The resulting impact could be exposure of company confidential information that could harm PCC's brand image. There is also the potential that information could be changed on these systems as well as being open to attacks such as viruses, Trojans and denial of service attacks.

An onsite inspection at LBaP found that there were good security controls in place to ensure unauthorised access into the building, different areas of the building and the computer room was not possible. Some additional actions need to be taken with the PCs that are used for connection to PCC as it was found that the mitigating actions detailed in the proposal had not been implemented. Implementation of these actions – LBaP password standard and password protected screen saver – will help to provide additional security and prevent unauthorised access to the PCC systems and network.

Overall there are a number of areas that can be reviewed and cleaned up with minimal effort and security of the connectivity between PCC and LBaP will be much improved. Other areas may need more consideration to determine the benefit to the business versus the cost of updating hardware or software that is in use.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit findings

The following findings were discovered during the audit of the business partner connection between PCC and LBaP. This section will provide more detail on the major areas of concern that need to be addressed as a priority. The priority is rated according to four categories – Critical, High, Medium and Low.

Audit Finding #1: Router Configurations

Priority: Critical

Reference: Checklist item 6, page 33
Checklist item 7, page 34
Checklist item 11a, page 40
Checklist item 11b, page 45
Checklist item 12, page 50

Observation:

The configurations of the three routers audited – lbapmelgw1, lbapmelgw2 and pccear1 – all need to be reviewed and cleaned up. When comparing the proposal document with what was actually configured in the ACLs for pccear1 (see figures 20 & 21) it was found that there were a large number of servers configured that were not documented at all. Although lbapmelgw1 and lbapmelgw2 had few problems with their ACLs (see figures 19 & 22) there were still some redundant access lists discovered. The VTY access lists (see figures 26, 27,28 & 29) also need to be cleaned up, as there are some redundant entries. The Router Assessment Tool found a high number of configuration failures on all three routers (see figures 23, 24 & 25). The banner configuration (see figures 10, 11 & 12) on all three routers is not meeting the PCC standard and is providing too much information about PCC. None of the communication with the routers is encrypted making it easy to sniff passwords off the network.

Background/Risk:

Incorrect configuration on the routers may result in unauthorised access to the PCC systems. This could result in company confidential information being accessed and either released to the general public or changed in a damaging way. It may also be possible for viruses or Trojans to propagate from the segregated network to the PCC network and vice versa on the access that is not meant to be open between PCC and the segregated network. Denial of service attacks may also potentially be launched against the systems utilising the configuration weaknesses found by the RAT resulting in PCC and LBaP being unable to provide the required service to their customers. This would result in damage to the brand image of both companies and customer satisfaction issues. The additional information provided in the banner message may result in an attacker utilising social engineering to gain access to the routers or the systems. This could again result in an attack against PCC and/or LBaP that would damage the brand image of both companies.

Audit Recommendations:
The ACLs for pccear1 need to be reviewed against the proposal document and the actual access required by LBaP to deliver services. The change management system should also be reviewed, as there may be changes that have occurred but have not been transposed into the proposal document. Any access that is not required should be removed as a priority. The redundant ACLs and VTY ACLs discovered on lbapmelgw1 and lbapmelgw2 need to be removed. A more stringent review process needs to be put in place to ensure that proposal documentation is kept up to date and reviews of what is actually configured occur on a regular basis.

The areas that failed the Router Assessment Tool need to be reviewed and corrected accordingly. The areas that were rated a 10 or 7 should be corrected as a priority. The fix script produced by the RAT may be utilised to assist with correcting these items. A standard configuration that addresses the areas identified as failures by the RAT needs to be documented for all business partner routers so that future implementations follow this standard.

The banner message needs to have the additional support information removed and the legal notice updated to be in keeping with the corporate standard for all devices.

The use of encryption to connect to the routers should be investigated to determine if there is a more secure method of connectivity.

Costs:
The costs for making these changes are in person hours. It is estimated that reviewing the ACLs against the proposal document, any changes that may not have been documented and reviewing what LBaP actually need access to would take approximately 4 business days. This time includes following up any undocumented changes to ensure that the appropriate approvals have been gained from the relevant parties. The actual configuration changes to the ACLs, legal notice banner and implementation of the RAT recommendations would take approximately 1 day. All configuration changes need to be made carefully and using appropriate change management controls. Lead-time for change management also needs to be taken into consideration and may be from 3 days to two weeks depending on the potential impact of changes.

Investigation into a more secure method of connectivity eg: using SSH may be done over a longer period of time. The ability to implement a more secure method of connectivity may be dependant on the version of the IOS running on the router. If an upgrade to the IOS is required to support a secure method of connectivity, then additional hardware such as RAM and Flash may be required.

Compensating Controls:
Access to the PCC systems requires authentication in the form of username and password. Access is also limited to specific ports for those systems thus restricting the

connection from the segregated network. PCC personnel are also the only people authorised and able to make changes to the access lists.

Audit Finding #2: Router passwords
Priority: High
Reference: Checklist item 8, page 36
Checklist item 9, page 38

Observation:
The passwords in use on the routers does not meet the PCC corporate standards (see checklist item 8) and not all the routers are using the "enable secret 5" level of password encryption (see figures 15 & 16).

Background/Risk:
Passwords that are easy to guess means that an attacker may be able to gain access to the routers quickly and easily through a brute force attack on the password. An attacker would then be able to log into the router and obtain administrative privileges to the router. They would then be able to make any changes to the router they wished. The results could be removing access for the LBaP segregated network. LBaP would then be unable to meet their SLA, PCC's brand image would be damaged and PCC would have customer satisfaction issues. Another potential result could be to open up full access to the PCC network. This would allow the attacker full access to the PCC network with the potential to cause large amounts of damage to the PCC network and access to confidential information.

The encryption of the enable password is also critical, as this is equivalent to root access to the router. If the router configuration is being transferred across the network, for example: backup of the router configuration, then it is possible to obtain the enable password during this transfer if "enable password 7" is configured. If "enable secret 5" is configured then, although this can be obtained during the transfer, there are currently no known password cracking tools for this level of password encryption. Obtaining this information would allow an attacker full access to changing the configuration of the routers. This has the same potential result as an easily guessable password.

Audit Recommendations:
The passwords currently configured on the routers need to be changed to meet the corporate standard (minimum 8 characters, three out of the following four items – uppercase, lowercase, numeric, special character). The use of the enable secret command needs to be implemented on lbapmelgw2 to ensure that the enable password is being encrypted with the highest method currently available. This needs to be included in the standard configuration documentation for business partner routers to ensure future routers are configured in a standardised and secure manner.

Cost:
The costs for making these changes is in providing adequate resources with the correct skill set to make the changes. The time taken to make these changes would be

approximately half an hour. Change management controls need to be followed accordingly.

Compensating Controls:
There are no compensating controls for this finding.

Audit Finding #3: Authentication
Priority: High
Reference: Checklist item 10, page 39

Observation:
When connecting to the routers lbapmelgw1 and lbapmelgw2, it was found that there was no prompt for a username, only a password (see figures 33 and 34).

Background/Risk:
Only having the password configured reduces the amount of information an attacker needs to acquire before being able to log onto one of the routers. All an attacker needs is the password and he is able to gain access to the router(s). This would potentially expose PCC to an attack, loss of confidential information, loss of brand image and customer satisfaction issues if access from LBaP is removed.

Audit Recommendations:
As a priority, either a generic username/password or individual usernames/passwords for each network engineer that needs to work on the business partner routers should be configured on the routers. This will help to provide another layer of defence to the routers. This needs to be included in the standard configuration documentation for business partner routers to ensure future routers are configured in the same manner. Investigation should also be conducted into the viability of using a solution such as TACACS+ to assist with the management of individual user accounts.

Cost:
Initial cost will be associated with the time needed to configure user accounts on the routers. This would take approximately 5 minutes per account. Investigation into a solution such as TACACS+ may be done over a more extended period of time. If there is already a TACACS+ system in use it may be possible to leverage off this system.

Compensating Controls:
There are no compensating controls for this finding.

Audit Finding #4: Log file monitoring and auditing
Priority: High
Reference: Checklist item 16, page 53
Checklist item 17, page 54

Observation:
Although logging was enabled on both routers (see figures 19, 20 & 21), none of this logging information was being sent to a remote server for monitoring and auditing purposes (see test results for Checklist items 12 and 13). There is also no logging being done on any of the access lists, especially those access lists that contain the "deny" statement.

Background/Risk:
Having logging enabled on both performance and access lists is essential to being able to track activities that are occurring both on the routers and the traffic that is travelling from the segregated network to the PCC network. Without logging being done on the access lists it is impossible for the network team to have any knowledge of any unauthorised access attempts to the PCC network.

Given the amount of traffic that is travelling to the PCC network, the logs on the routers will fill up and overwrite quite quickly. Without sending this information to a separate system it is not possible to identify any intrusion attempts, performance issues, unauthorised attempts to access other systems not in the access lists or conduct investigation into any suspicious activity. This means that anything could potentially be happening between LBaP and PCC and there is no way of picking up unauthorised activity. There is also the issue that no proactive monitoring for performance issues are occurring which could impact the level of service being provided to customers.

Audit Recommendations:
Logging needs to be enabled for the access lists to ensure that any unauthorised access attempts are identified. As a priority, at least the access lists with the "deny" statement should be logged. A server should be identified as a possible system for the router logs to be stored. Monitoring of the logs should be implemented to ensure that critical issues are being identified and actioned. At a minimum, this should be set up for pccear1 as it is controlling the access from the segregated network to the PCC network and is the most critical to be monitored. This needs to be included in the standard configuration documentation for business partner routers to ensure future routers are configured in the same manner.

Costs:
The time taken to configure logging for the access lists with the "deny" statements at a minimum would only require approximately half an hour. Time for change management procedures also needs to be allowed for. In general it would take approximately half an hour to raise a change request and a minimum 3-day lead-time before the change can be implemented.

After discussions with the network engineer, a server has been identified that could be utilised for storage of the log files. Therefore the cost associated with this would be to setup the logging and testing to ensure the log files are being written to the server. This would take approximately half a day. It was also identified that monitoring scripts were

already in use with other equipment and could be leveraged off. Hence, implementation of the monitoring scripts will take approximately half a day including testing.

Compensating Controls:
There are no compensating controls for this finding.

Audit Finding #5: LBaP PC Configuration
Priority: Medium
Reference: Checklist item 3, page 31
Checklist item 4, page 32

Observation:
An onsite inspection of the PCs that are in use by LBaP on the segregated network found that the screen saver configuration did not meet the mitigating action required of LBaP in that it was not enabled to use password protection once the screen saver came on. It was also found that the PCs were not meeting the LBaP corporate password standard configuration.

Background/Risk:
As part of the business partner proposal, LBaP were required to implement a number of mitigating actions. One of these was to ensure that all the PCs in use were configured so that a password was required to unlock the PC once the screen saver comes on. The lack of this setting makes it easier for an attacker to walk up to any of the PCs and access any of the PCC systems that happen to be connected to at the time. LBaP's password practices were found to be adequate in securing the PCs, however it was found that the LBaP password standard had not been implemented on the PCs. This means that it is possible for all the PCs to be configured with blank passwords thus making access to the PCs a lot easier for an attacker. In both situations, access to PCC's systems is a lot easier and could result in the disclosure of confidential information, an attacker could launch an attack on the PCC systems and the brand images of PCC and LBaP could be damaged.

Audit Recommendation:
The PCC business sponsor needs to ensure that these items are addressed by LBaP as soon as possible to reduce the risk to PCC's systems and network.

Cost:
There is no cost to PCC, as LBaP will handle these configuration items.

Compensating Controls:
There are no compensating controls for this finding.

Audit Finding #6: Patch Management
Priority: Medium
Reference: Checklist item 15, page 52

Observation:
All three routers – lbapmelgw1, lbapmelgw2 and pccear1 – were all found to be running old versions of the IOS.

Background/Risk:
A robust patch management process needs to be in place to ensure that the PCC network is protected from any vulnerabilities found in the IOS versions running on the three routers. This needs to be balanced with the cost associated with regular patch management and the risk associated with a vulnerability. After conducting research on the Cisco web site (www.cisco.com) it was found that there were a number of vulnerabilities within the IOS that is currently running on the routers:

Alert: Cisco Security Advisory: Cisco IOS ARP Table Overwrite Vulnerability
URL: http://www.cisco.com/warp/public/707/IOS-arp-overwrite-vuln-pub.shtml
Routers affected – lbapmelgw1 and lbapmelgw2

Alert: Cisco Security Advisory: Malformed SNMP Message-Handling Vulnerabilities
URL: http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml
Routers affected – lbapmelgw2

Alert: Cisco Security Advisory: IOS HTTP Authorization Vulnerability
URL: http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html
Routers affected – lbapmelgw1

Alert: Cisco Security Advisory: Data Leak with Cisco Express Forwarding Enabled
URL: http://www.cisco.com/warp/public/707/IOS-CEF-pub.shtml
Routers affected – lbapmelgw1

Alert: Cisco Security Advisory: SSH Malformed Packet Vulnerabilities
URL: http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml
Routers affected – pccear1

Alert: Cisco Security Advisory: Cisco Security Advisory: Cisco IOS Software Processing of SAA Packets
URL: http://www.cisco.com/warp/public/707/cisco-sa-20030515-saa.shtml
Routers affected – lbapmelgw2

These vulnerabilities may result in the PCC network being breached in some way and confidential information being obtained. This could have the flow on effect of impacting PCC's brand image. LBaP's brand image and ability to meet SLA may also be affected if the router connecting LBaP to the PCC network is rendered unavailable. This would also result in customer satisfaction issues for PCC.

Audit Recommendations:
PCC needs to review each alert and determine the level of risk associated with not implementing the recommended IOS upgrades. There may be little to no risks

associated with these vulnerabilities in this situation or there may be mitigating actions that can be put in place to render them insignificant.

A formalised patch management process needs to be put in place. This process needs to be documented and communicated to all network engineers working on the PCC network to ensure there is no single point of failure. The network engineers need to ensure they are being notified of any vulnerabilities so that appropriate action can be taken to ensure the PCC network is protected.

Cost:
A review of each alert for applicability needs to be conducted by the network engineer. This would take approximately 2 hours for the 3 routers. If any alerts are found to place the PCC network at high risk for which there are no mitigating actions that can be applied then hardware requirements need to be reviewed. Upgrading the IOS may need additional RAM or Flash.

Compensating Controls:
If any of the alerts have mitigating actions, these may be implemented if they do not impact the ability of LBaP to deliver the required services rather than investing a large amount of money in upgrading hardware.

References

1. BobbyRite. Cisco Pass the Password. 1997 - 1999
   URL: www.alcrypto.co.uk/cisco (June 2003)

2. BP Consultant. LBaP Proposal 125. 12 March 2003.

3. Centre for Internet Security Benchmark and Audit Tool for Cisco IOS Routers. Version 2.0 March 2003.
   URL: http://www.cisecurity.org/ (May 2003)

4. Cisco Systems Inc. Copyright 1992 – 2003
   URL: http://www.cisco.com

5. Cisco Systems Inc. Improving Security on Cisco Routers. 25 June 2003
   URL: http://www.cisco.com/warp/public/707/21.html#intro (June 2003)

6. Combs, Gerald. Ethereal. Version 0.9.11
   URL: http://www.ethereal.com/ (February 2003)

7. Khaw, Penny. Business Partner Network Security Checklist. Version 1.0 5 May 2003.

8. National Security Agency. Router Security Configuration Guide. Version 1.1 27 September 2002.
   URL: http://www.nsa.gov/snac/cisco/guides/cis-2.pdf (May 2003)

9. Stewart, Brian. Router Audit Tool: Securing Cisco Routers Made Easy! 29 March 2002
   URL: http://www.sans.org/rr/papers/38/238.pdf (June 2003)

Appendix A: LBaP Proposal 125

LBaP Project Proposal

Project Number: AUS0125	**Date:** 09-Aug-2000, 22-March-2002
Project: Business Partner (LB and P Pty. Ltd.)	
IT Contact:	**Contact Phone:**
PCC Business Contact:	**Contact Phone:**
Project Sponsor: Back up contact:	**Sponsor Phone:**
Project Coordinator:	**Project Coordinator Phone:**
EA Consultant:	**Consultant Phone:**

Overview:

PCC has outsourced the phone support on all commercial desktop PC products. In order for LB and P Pty. Ltd. to provide phone support on all commercial desktop PC products access is required to the PCC Parts and Inventory Management Systems, Hardware Call Management system, PCC External web, Knowledge Management System, Customer Call Management System and PCC contact information. In addition email access is also required to allow for communication with PCC. Access to Workflow Manager will be required when available in the near future, prior to August 2002. In consideration to the access between the Business Partner and the PCC network, there are risks associated with the PCC network connectivity. Precautions have been made to minimize these risks, however total elimination of these risks cannot be guaranteed.

For further details on PCC contact information, please refer to project AUS0075.

The sponsor will have to understand and accept these risks before this project may proceed.

Revision History:

Date	By	Major Changes
14th Aug, 2000	BP Consultant	Initial creation
10 Jan 2002	BP Consultant	Updated access
19 Mar 2002	BP Consultant	Added sub-project AUS0075
22 Mar 2002	BP Consultant	Added network diagram
22 Mar 2002	BP Consultant	Removed Knowledge Management 8081
22 Mar 2002	BP Consultant	Revision history updated. Added Appendix B. Responsibilities and Liabilities of PCC and PCC Customer Change proposal tagging as PCC Confidential in the footnote portion of the document
2 April 2002	BP Consultant	Integrated changes in IT & Business Contact

Date	By	Major Changes
12 March 2003	BP Consultant	Added Parts Inventory and Management system v-observer.hp.com

Requirements:

1. Allow LBaP employees access to PCC facilities in order for them to meet their contractual agreement to provide telephone support to PCC customers.
2. The business partner will need to have email accounts created as their primary means of communication with PCC. The business partner will need to purchase an off the shelf copy of the Outlook client for the license.
3. There will be an NT domain controller server on the business partner network to administer user accounts and host future network printers.
4. Provisioning for a network printer as the business partner size grows
5. There will be a call center set up at CPM office to receive PCC external customer phone calls
6. Monitor of ISDN data link between CPM and the PCC site is required to ensure adequate performance is maintained
7. Provide sponsor with the security requirements to be adhered to by CPM.
8. One month's clear notice to be provided for renewals.
9. PCC approved dual network access established for access to both PCC and CPM's network from the same PC.

Port Access Requirements:

Source Address	Destination Address	Port Number / Application
10.88.32.0/25	10.68.1.29	TCP 1570 / Hardware call tracking & parts ordering.
10.88.32.0/25	192.168.13.70	TCP 8081, 8087 / Knowledge Management System
10.88.32.0/25	192.168.40.101	TCP 8081, 8087 Knowledge Management System
10.88.32.0/25	192.168.43.4	TCP 80 / PCC contact information
10.88.32.0/25	10.73.170.149	TCP 5012, 5102 / Customer Call Management System
~~10.88.32.0/25~~	~~10.88.40.100~~	~~TCP 80 / Proxy~~
10.88.32.0/25	10.85.49.5	TCP 5729 / Email
10.88.32.0/25	10.56.8.57	TCP 5729 / Email
10.88.32.0/25	172.26.66.72	TCP 80, 443 / Product Warranty System
10.88.32.0/25	10.68.1.8	TCP 1570 / Parts Inventory System Parts Inventory system
10.88.32.0/25	172.26.77.91	TCP 80, 443 / Parts ID and dispatch System
10.88.32.0/25	172.20.164.84	TCP 80, 443 / Parts Inventory System
10.88.32.0/25	172.16.64.56	TCP 443 / HTTPS

Considerations/Risks:

Risks to PCC IT Infrastructure

The risk to PCC IT infrastructure is minimal due to the following measures:

- The access to the PCC infrastructure shall be restricted to applications as detailed in the Business Control Checklist by placing access lists on the router at the LBaP office.
- Screen Saver Passwords shall be installed on all the PC's located at the Business Partner's premises.
- The Communications Equipment Rack shall be located in a secure area to minimise the Risk of any unauthorised person in obtaining access. Access will only be provided by the onsite Manager.
- Authorised personnel have access to the PCC system and the building is secured with a Burglar Alarm System.

Business Partner Risks:

- As the Site is a Business Partner Site, the PC's are not secured and may be accessible to unauthorised personnel. Screen Saver passwords are a must in order to minimise the risk of unauthorised personnel easily gaining access to the PC's.
- Security of the Communications equipment is necessary. This is to minimize the risk of unauthorized personnel easily gaining access to the PCC Communication equipment.
- The security of the Data outlets at the desk will not be extremely secure, as they shall be accessible to unauthorised Staff. This will allow for capturing of packets on the Business Partner Network. As a result, IP information may be obtained and unauthorised PCs will be able to masquerade on the Business Partner LAN as business Partner PC. However restriction will be placed on the Router to minimise the access to only the applications the Business Partner is authorised to access.
- Password non-disclosure is also necessary. However the Business Partner practices offer password protection that is substantial which shall ensure that passwords will not be disclosed to unauthorised personnel.

The risk involved is low because:

- The applications that the Business Partner personnel are using are dead-ended. This means that it would be difficult for normal users to break out of the application to access other information that they are not supposed to access.
- The PCC hosts appear to meet the requirements for stringent host security as defined in the current checklists extracted from the relevant host security standards.

Risks to PCC Information

The information on the PCC Machines is classified as PCC Confidential and as such will need to be secured for Confidentiality and Integrity:

The risk to PCC information is minimised due to the following measures:

- Screen Saver Passwords shall be installed on all the PCC PCs located at the Business Partner premises. This shall minimise the risk of unauthorised persons gaining access to the PCC Network and manipulating and viewing the data.

- The applications being accessed are designed and administered using stringent security practices, which should minimize the risks of unauthorised access to PCC information.

- At the Business Partner site passwords are being used to authenticate the identity of the Business Partner users who are accessing PCC Information. Passwords can be compromised through a variety of methods including deliberate disclosure, accidental disclosure and guessing attacks. The Business Partner practices do offer password protection that is substantial to protect against unauthorised disclosure of passwords.

- The PCC Communication Equipment (including Hub, Router etc) will need to be physically located in a 19-inch rack located in a secure area.

- Network wiring between the Desks and 19-inch rack will need to terminate within the 19-inch rack.

- Patching from the Hub to the Data outlets will also be confined within the 19-inch rack.

- The Telecom termination of the ISDN line will also terminate within the 19-inch rack.

- An audit of the network, connections and operation shall be performed by PCC every 12 months and a report on the shortcomings provided to the sponsor with the required actions to secure the network.

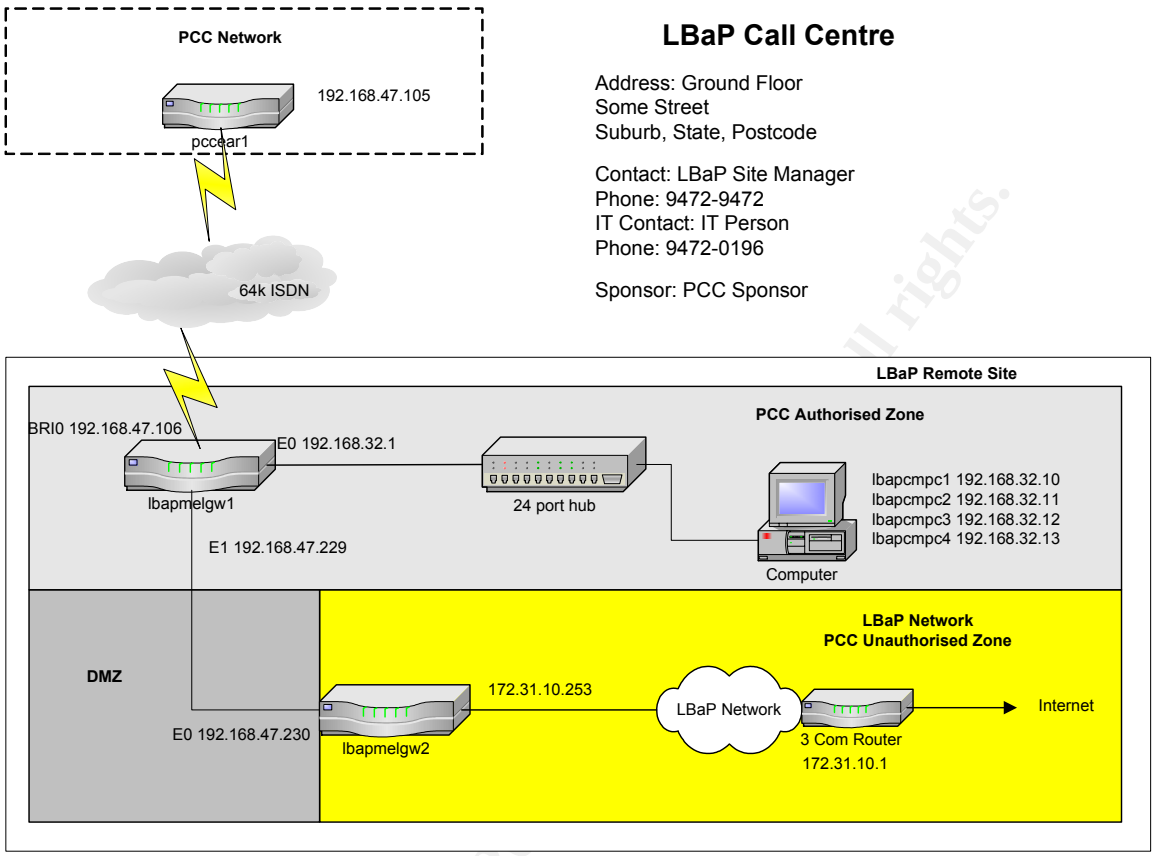
- The security of the Data outlets at the desk will not be extremely secured, as they shall be easily accessible to unauthorised Staff. This will allow for capturing of packets on the PCC- Business Partner Network. This exposes PCC as the unauthorised person may easily find out IP information and masquerade as a Business Partner PC on the PCC-Business Partner Network. However restriction will be placed on the Router to minimise the access to only the application the Business Partner is authorised to do access.

Bottom line

The risks in this setup are mainly on the protection of the PCC Infrastructure, the PCC information on the PCC systems located in regional headquarters, the PCC system and NT Server located in the local country, and in the protection of any unauthorised person gaining access to PCC facilities or PCC Communication equipment that will be located at the Business Partner Site. This also assumes that no PCC data shall be stored on the Desktop PC's. Measures such as ensuring that the communication equipment is placed in a secure area, ensuring that Screensaver passwords are used on all desktop PCs must be put in place to reduce the risk of unauthorised personnel gaining access to the PCC Infrastructure and PCC Information.

It is the decision of the project sponsor, to accept these risks in giving the go-ahead to this project.

Proposed setup:



Responsibilities and Liabilities of PCC and PCC Customer

PCC Responsibilities:

- All BPC Modules are compliant with IT Risk Management (ITRM) standards for securing the access to the PCC Internet.
- All standard BPC Modules are pre-approved by the ITRM approval process.
- In particular, BPC must provide the firewall options, which should be used to communicate between the Business Partner and PCC. If the firewall option to be used is not pre approved, BPC will escalate it into the security approval chain.
- If a security problem is detected which might endanger the security of the Business Partner's network, the Business Partner and/or PCC sponsor will be notified immediately with suggestions for handling this situation.
- Request forms are kept according to the General Retention Schedule.
- BPC is responsible for evaluating host and application security.

- BPC is responsible for educating the Sponsor on all aspects of risk and how they relate to ITRM standards. BPC will inform the businesses about their responsibilities & liabilities and about the responsibilities & liabilities they have to explain to the Business Partner.
- BPC may close a connection if security problems are suspected.
- Perform an audit of the network, connections and operation every 12 months and provide a report on the shortcomings to the sponsor with the required actions to secure the network.
- Provide the sponsor with a set of security requirements that can be used for training of Business Partner's personnel.

PCC Business (Customer) Responsibilities & Liabilities

- The sponsor is responsible for including all legal requirements relevant for the BPC solution in the business agreement with the Business Partner.
- The Sponsor is responsible for maintaining business process security, and the documentation describing that security. The Sponsor is responsible for providing all the information needed for documenting the security measures on hosts, applications and network.
- The Sponsor and the Business Partner are responsible for implementing these measures on their hosts, applications and network and must confirm the inclusions.
- The Business will ensure that the Business Partner understands and agrees in writing to the following points:
  - Should a security problem occur due to neglect of the Business Partner, the Business Partner is liable for any damages to PCC
  - The configuration of one of these services must not be changed in any way whatsoever by the Business Partner
  - The Business Partner must safeguard the routers properly. Once the end-to-end tests have been completed, it should be put in a locked place.
  - The Business Partner is held responsible for any damages to the equipment at his site
  - The equipment provided by PCC to the BP must only be used for access to the PCC network
  - The Business must provide the username and PIN to the Business Partner end user in a secure way and will ensure that the Business Partner end user understands and agrees in writing that he:
    - is responsible for keeping his/her username and PIN secret as he/she does for his credit card
    - is responsible that his/her token card is used only by himself/herself. (No token card sharing)
- For incoming firewall options the Business will ensure that the Business Partner end user understands and agrees that he/she should open the connection only if the business need is well defined and documented and that the connection has to be closed right after the incoming access is terminated
- The LBaP Business users should close their outgoing connections once the BP transactions have terminated

Appendix B: Business Partner Network Security Checklist

Network Compliance	Rating G Y R	Reason for Yellow or Red
1. The security configuration of the network equipment (such as ACLs) corresponds to the approved application/server access as documented in the project proposal.		
2. Documentation/diagrams exist for supplier connections. These need to be current, and appropriately labeled (such as "PCC Confidential" or "PCC Restricted").		
3. The solution description accurately reflects the on-site configuration/setup.		
4. a) All documentation of any PCC managed network components and/or topology is complete and accurate. b) List any undocumented equipment that was identified.		
5. All equipment at the supplier site is compliant with the physical access policies of PCC		
6. No unauthorized access of the following types could be established back in to HP's network: a.) Telnet b.) VT3K c.) FTP d.) HTTP e.) Rexec, rlogin, Remote Shell f.) Netbios g.) SMTP		
7. Where the supplier has their own local network, access between that and HP's networks (net-15 and on site at the supplier) is not available, unless specified within the project proposal.		
8. All network equipment (such as routers and hubs) is physically secured from unauthorised access.		
9. Access to the network equipment is available only to authorized PCC and supplier staff.		
10. Appropriate AntiVirus software is installed on all PCs accessing PCC equipment and virus definition files are regularly updated.		
11. All network equipment (routers, firewalls, etc), and network configuration files are securely password protected.		
12. A process exists for the archival and storage of all audit logs.		
13. Backup and recovery procedures have been designed; backups are performed daily and compared to reference data.		

14. Appropriate banner information is displayed at login, indicating that system is to be used by authorized personnel only.		
15. Sensitive configuration information such as type and firmware version is hidden until full user authentication.		
16. Relevant host based or network security monitoring tools are installed and utilized. The monitoring of such tools is able to identify and report security incidents.		
17. A systematic review process exists to resolve, validate and respond to log file exceptions.		
18. A process exists to review all patches, Service Pack and Hot Fixes.		
19. Major System Patch bundles / Updates and Service Packs are reviewed and applied in a timely manner.		
20. Network engineers are alert to potential hardware/software security issues, and apply critical security patches, as they are made available.		