



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Auditing Networks, Perimeters and Systems



Practical Assignment

Version 3.1 Option 1

Auditing a Cisco 1710

Dave Weir

June 23, 2004

Abstract

The following paper is comprised of a security assessment of a small engineering firm that implemented a Cisco 1710 as their primary firewall and VPN device. The paper looks at the threats and vulnerabilities faced by the firm as well as the risks they pose. It then continues to discuss the state of practice today including useful references before tackling a checklist that details the items that should be assessed as well as the procedure to perform the tests. Finally the paper performs the ten most critical test items showing evidence of the results and uses these to produce a security assessment that includes the findings and recommendations to the firm.

While this paper deals with an assessment of a Cisco 1710 for a small office a similar procedure could be used to assess any firewall device.



Table of Contents

1. PART #1 - RESEARCH IN AUDIT, MEASUREMENT PRACTICE, AND CONTROL	4
1.1. System to be Audited	4
1.2. The Most Significant Risks to the System	6
1.2.1. Threats and their Capacity to Inflict Damage	6
1.2.2. Major Information Asset	7
1.2.3. Major Vulnerabilities of the Assessment	7
1.3. The Current State of Practice	9
2. PART #2 - AUDIT CHECKLIST	11
2.1. Item 1 Scan Router for Open Ports	11
2.2. Item 2 Scan Network Inbound for Open Ports (Ingress)	12
2.3. Item 3 Scan Network Outbound for Open Ports (Egress)	12
2.4. Item 4 Insure Java is Blocked	13
2.5. Item 5 Check Physical Security	13
2.6. Item 6 Test Stateful Inspection	14
2.7. Item 7 Test for Known Exploits	14
2.8. Item 8 Determine Business Requirements	20
2.9. Item 9 Compare ACL's to Business Requirements	21
2.10. Item 10 Compare Current Router Config with Best Practices	21
2.11. Item 11 Compare Current Router Config with Cisco Recommendations	22
2.12. Item 12 Compare ACL's to Firewall Best Practices	22
2.13. Item 13 Check for Logon Banner	23
2.14. Item 14 Check Change Control	23
3. PART #3 - AUDIT TESTING, EVIDENCE, AND FINDINGS	24
3.1. Evidence and Findings from Test Item 1	25
3.2. Evidence and Findings from Test Item 2	26
3.3. Evidence and Findings from Test Item 3	28
3.4. Evidence and Findings from Test Item 4	29
3.5. Evidence and Findings from Test Item 5	30
3.6. Evidence and Findings from Test Item 6	31
3.7. Evidence and Findings from Test Item 7	31
3.8. Evidence and Findings from Test Item 8	34
3.9. Evidence and Findings from Test Item 9	37
3.10. Evidence and Findings from Test Item 10	41
4. PART #4 - RISK ASSESSMENT	48
4.1. Executive Summary	48
4.2. Assessment Findings	48
4.3. Assessment Recommendations	52
REFERENCES	56
APPENDIXES	58
Appendix A- Config File from Audited Cisco 1710	59
Appendix B- Network Diagram DML Engineering (Current)	67
Appendix C- Recommended Network Design for DML Engineering	68

1. Part #1 - Research in Audit, Measurement Practice, and Control

1.1. System to be Audited

DLM Engineering Inc. are a small engineering firm that specialize in hull design and testing for both pleasure crafts and vessels for offshore work in harsh environments. They have a staff of approximately 40 people of which about 30 are located in their primary office and the other 10 are located at a testing site.

They currently rely on a Cisco 1710 as their primary firewall and VPN device at the central office. While they do not have a formal written security policy they are security aware and have tried to limit exposure as much as possible using ingress and egress filtering to limit traffic to legitimate business requirements.

Yesterday they were awarded a lucrative contract, for hull design and testing of a contender in the Americas Cup. Since the Americas Cup is so prestigious and competition is fierce they now have some concerns as to whether their security is sufficient or not. The CEO has determined they now require a security assessment of their firewall.

The focus of the Audit will be on their edge device, which is currently a Cisco 1710 running IOS version 12.3(1a). The router is currently the primary firewall running Context Based Access Control (CBAC) as well as terminating their remote VPN tunnels.

In order to fully understand the device to be audited the following show version gives us the operating system version and image as well as other useful information such as processor type, flash, DRAM, installed modules, and serial number.

Figure 1 Results from Show Version

```
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1710-K9O3SY-M), Version 12.3(1a), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Fri 06-Jun-03 19:50 by dchih
Image text-base: 0x80008120, data-base: 0x80F0625C
```

```
ROM: System Bootstrap, Version 12.2(1r)XE1, RELEASE SOFTWARE (fc1)
```

```
DLM_Eng uptime is 1 week, 48 minutes
```



System returned to ROM by power-on
System restarted at 09:58:06 NDT Wed Jun 16 2004
System image file is "flash:c1710-k9o3sy-mz.123-1a.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco 1710 (MPC855T) processor (revision 0x200) with 83559K/14745K bytes of memory.

Processor board ID HGF065310ME (3590106274), with hardware revision 0000

MPC855T processor: part number 5, mask 2

Bridging software.

X.25 software, Version 3.0.0.

1 Ethernet/IEEE 802.3 interface(s)

1 FastEthernet/IEEE 802.3 interface(s)

1 Virtual Private Network (VPN) Module(s)

32K bytes of non-volatile configuration memory.

16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

In order to understand what all those letters in the image name mean you can consult Cisco's web site¹. The two of most interest to us are shown below with their meanings as per the Cisco site.

k9	Greater than 64-bit encryption. On Cisco IOS Software Release 12.2 and up.
----	--

¹http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a00801ab747.shtml



o3	Firewall with Intrusion Detection (Firewall Phase II).
----	--

1.2. The Most Significant Risks to the System

In order to understand risk the first thing that needs to be done is to define both threats and vulnerabilities.

Threats, in an information security sense, are any activities that represent possible danger to your information or operation.² As a result not all threats are attacks they can be natural disasters like floods or mechanical breakdowns such as a hard drive failure. As you can see threats come in many shapes and forms.

Next we need to look at vulnerabilities. In security terms, a vulnerability is a weakness in your systems or processes that allow a threat to occur.³

Now that we have defined both threats and vulnerabilities lets take a look at risk, which turns out is actually the combination of threats and vulnerabilities. As a simple formula: $\text{Risk} = \text{Threat} \times \text{Vulnerability}$.⁴ In other words risk is the likelihood that a threat and vulnerability will both exist at the same time.

Finally exposure is defined by the SANS glossary as: A threat action whereby sensitive data is directly released to an unauthorized entity.⁵ Therefore the degree of exposure would essentially be the risk or likelihood that a particular vulnerability would be exploited.

Now that we have the definitions out of the way lets take a look at the threats and vulnerabilities that face DML and the risk or exposure that they create. In order to rate the risks as high, medium, and low a value between 1-10 will be assigned to each threat and vulnerability and if the resulting product of the two falls between 0-30 we will consider it low, 31 – 70 medium and 71 – 100 as high.

1.2.1. Threats and their Capacity to Inflict Damage

Threat	Capacity to do damage
Hackers/Crackers (9)	<ul style="list-style-type: none">• Data Loss• Data Theft• Data Manipulation• Loss of Availability Denial of

² Cole, p.25

³ Cole, p.27

⁴ Cole, p.28

⁵ <http://www.sans.org/resources/glossary.php>



	Service (DoS) <ul style="list-style-type: none"> • Public Image Tarnished
Physical Threats (flood, fire, vandalism, theft, etc) (4)	<ul style="list-style-type: none"> • Hardware Theft • Hardware Destruction or Damage • Data Loss • Data Theft • Data manipulation • Loss of Availability (DoS)
Administrator Error (2)	<ul style="list-style-type: none"> • Data Loss • Data Theft • Data Manipulation • Loss of Availability (DoS) • Loss of Productivity
Malware (10)	<ul style="list-style-type: none"> • Data Loss • Data Theft • Data Manipulation • Inadvertent Disclosure of Private Information • Loss of Availability (DoS) • Loss of Productivity due to network congestion • Public Image Tarnished

1.2.2. Major Information Asset

Affected Major Information Asset	Description
Intellectual Property	As the 1710 router is the primary network defense all DLM Engineering's data is at risk of being unavailable, lost, stolen, or altered.

1.2.3. Major Vulnerabilities of the Assessment

Vulnerabilities	Degree of Exposure	Potential Impact
V1.Lack of Physical Security (10)	High	<ul style="list-style-type: none"> • Accidental or malicious damage or destruction of the router itself leading to system unavailability • Theft of the router itself leading to system unavailability as well as

		<p>financial loss of having to replace and reconfigure the router</p> <ul style="list-style-type: none"> Unauthorized access leading to Data theft, loss, alteration, and/or system unavailability
V2.Unpatched or Misconfigured Hardware (2)	Low	<ul style="list-style-type: none"> Unauthorized access leading to Data theft, loss, alteration, and/or system unavailability Introduction of malware leading to lost productivity, system unavailability, inadvertent disclosure of private information, and/or damage to reputation / image
V3.Lack of DMZ (8)	High	<ul style="list-style-type: none"> Unauthorized access leading to Data theft, loss, alteration, and/or system unavailability Introduction of malware leading to lost productivity, system unavailability, inadvertent disclosure of private information, and/or damage to reputation / image
V4.Inappropriate Access Controls (2)	Low	<ul style="list-style-type: none"> Unauthorized access leading to Data theft, loss, alteration, and/or system unavailability Introduction of malware leading to lost productivity, system unavailability, inadvertent disclosure of private information, and/or damage to reputation / image
V5.Inappropriate Means of Remote Administration (9)	High	<ul style="list-style-type: none"> Unauthorized access leading to Data theft, loss, alteration, and/or system unavailability
V6.Insufficient Router Hardening (2)	Low	<ul style="list-style-type: none"> Unauthorized access leading to Data theft, loss, alteration, and/or system unavailability
V7.Lack of Written Security Policies and Procedures (6)	Medium	<ul style="list-style-type: none"> Unauthorized access leading to Data theft, loss, alteration, and/or system unavailability Introduction of malware leading to lost productivity, system unavailability, inadvertent disclosure of private information, and/or damage to

		reputation / image
--	--	--------------------

1.3. The Current State of Practice

Information Security has come along ways over the last couple of years going from an after thought at best to an integral part of Information Systems architecture and planning. As security has garnered interest the amount of information and tools available have grown substantially as well. In today's information era not only is security extremely important the amount of useful information available on line is almost unlimited. Searches can find information and tools for almost any topic you are interested in. You no longer have to reinvent the wheel for every aspect of security that you want to address. Instead there are consensus documents of best practices, check lists, sample policies and procedures, etc. readily available online.

Some of the documents and URL's I found particularly useful are listed below:

The first one is a great resource from Cisco with information on how to make their routers more secure.

Improving Security on Cisco Routers

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

The next one also from Cisco is a white paper covering branch office network security considerations.

Securing the Branch Office Network White Paper

http://www.cisco.com/en/US/netsol/ns340/ns394/ns346/ns382/net_value_proposition09186a00801c602f.html

Also from Cisco is the firewall data sheet which covers the key benefits and firewall highlights of Cisco's IOS.

Cisco IOS Firewall Data Sheet

http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_data_sheet09186a0080117962.html

Another useful link from Cisco for both troubleshooting and checking router configurations is their output interpreter. While not meant to replace a sound security policy or security expertise it will suggest enhancements to the security of your router.

Output Interpreter

<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>



Finally another useful link from Cisco is their Security Solutions portal, which provides links to vast resources of security information including [The Cisco Secure Encyclopedia \(CSEC\)](#)

Security Solutions

<http://www.cisco.com/warp/customer/cc/so/neso/sqso/index.shtml>

SANS also provides lots of useful information including a sample router security policy, firewall checklist, and a list of ports that should be blocked at the firewall.

Router Security Policy

http://www.sans.org/resources/policies/Router_Security_Policy.pdf

Firewall Checklist

<http://www.sans.org/score/firewallchecklist.php>

Ports to Block at the Firewall

<http://www.sans.org/top20/#ports>

The National Security Agency also provides an extremely helpful guide on best practices for securing routers with specific syntax included for Cisco router configurations.

Router Security Configuration Guide

http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf

Finally Lance Spitzner also provides a useful document on auditing your firewall that covers both methodology and tools.

Auditing your Firewall Setup

<http://www.spitzner.net/audit.html>

Moving on to links to useful tools and their documentation; the following links are very valuable indeed when it comes to performing a router audit.

The first is for the Router Audit Tool (RAT) which compares your configuration to best practice.

RAT

http://www.cisecurity.org/bench_cisco.html



The next is for Nessus a very powerful vulnerability scanner. One of the advantages of Nessus is that while the server has to run on a Unix based system the client can be a Unix variant or a Windows based machine offering great flexibility in mixed operating environments.

Nessus

<http://www.nessus.org/>

Finally is nmap, one of the most common and useful scanners available.

nmap

<http://www.insecure.org/nmap/index.html>

Armed with these resources and tools we are well prepared to tackle the audit of our router.

2. Part #2 - Audit Checklist

2.1. Item 1 Scan Router for Open Ports

Reference	Spitzner, Lance. "Auditing your Firewall Setup" 12 December, 2000 URL: http://www.spitzner.net/audit.html Personal Experience Router Security Configuration Guide, p. 242 http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf
Risk	Access to the router itself could lead to exploits of running services allowing unauthorized access. This test is checking V2, V4, and V5.
Testing Procedure / Compliance Criteria	Run nmap from the Internet scanning the outside interface of the router. nmap -v -g53 -sS -sU -sR -P0-O -p1-65535 -oN firewall.txt x.x.x.x -v verbose -sS Half Open scan -sU Scan UDP as well -sR RPC Scan -P0 Do not ping before scanning -O OS fingerprinting -p1-65535 scan all 65535 ports not just the first 1023 -oN log file x.x.x.x IP address of outside interface The test should reveal that all ports are filtered unless they are specifically required for a legitimate business function.
Test Nature	Objective
Evidence	Place holder
Findings	Place Holder

2.2. Item 2 Scan Network Inbound for Open Ports (Ingress)

Reference	Spitzner, Lance. "Auditing your Firewall Setup" 12 December, 2000 URL: http://www.spitzner.net/audit.html Personal Experience "Firewall Checklist 1.0" Item 7 URL: http://www.sans.org/score/checklists/FirewallChecklist.doc
Risk	Access to open ports in the network could lead to exploits of running services allowing unauthorized access or introduction of malware. This test is checking V2, V3, and V4.
Testing Procedure / Compliance criteria	Run nmap from the Internet scanning the internal network. nmap -v -g53 -sS -sU -sR -P0-O -p1-65535 -oN network.txt x.x.x.x/28 -v verbose -sS Half Open scan -sU Scan UDP as well -sR RPC Scan -P0 Do not ping before scanning -O OS fingerprinting -p1-65535 scan all 65535 ports not just the first 1023 -oN log file x.x.x.x/28 IP address Range used by the company The test should reveal that all ports are filtered to the internal network.
Test Nature	Objective
Evidence	Place holder
Findings	Place Holder

2.3. Item 3 Scan Network Outbound for Open Ports (Egress)

Reference	Spitzner, Lance. "Auditing your Firewall Setup" 12 December, 2000 URL: http://www.spitzner.net/audit.html Personal Experience "Firewall Checklist 1.0" Item 7 URL: http://www.sans.org/score/checklists/FirewallChecklist.doc
Risk	Access to ports beyond those required for business functions may allow users to run applications with security implications such as p2p applications which often allow firewall rule sets to be bypassed possibly leading to unauthorized access or introduction of malware. This test is checking V2, and V4
Testing Procedure / Compliance Criteria	Run nmap from the inside scanning a known external host with no firewall. Repeat test twice once from a machine on VLAN 10 and once from a machine on VLAN 20. nmap -v -g53 -sS -sU -sR -P0-O -p1-65535 -oN fromvlan10.txt x.x.x.x nmap -v -g53 -sS -sU -sR -P0-O -p1-65535 -oN fromvlan20.txt x.x.x.x -v verbose -sS Half Open scan -sU Scan UDP as well -sR RPC Scan -P0 Do not ping before scanning -O OS fingerprinting -p1-65535 scan all 65535 ports not just the first 1023 -oN log file x.x.x.xIP address Range used by the company The test should reveal that all ports are filtered unless they are specifically required for

	a legitimate business function.
Test Nature	Objective
Evidence	Place holder
Findings	Place Holder

2.4. Item 4 Insure Java is Blocked

Reference	Personal Experience “Firewall Checklist 1.0” Item 3 URL: http://www.sans.org/score/checklists/FirewallChecklist.doc
Risk	Allowing java code to be downloaded and ran on client PC’s could introduce malware into the network. This test checks V4
Testing Procedure / Compliance Criteria	Go to http://java.com/en/download/help/testvm.jsp . The test should reveal an empty grey box. If you see the dancing Duke logo™ java is not blocked.
Test Nature	Objective
Evidence	Place holder
Findings	Place Holder

2.5. Item 5 Check Physical Security

Reference	Spitzner, Lance. “Auditing your Firewall Setup” 12 December, 2000 URL: http://www.spitzner.net/audit.html Personal Experience Router Security Configuration Guide, p. 33 http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf
Risk	Lack of physical security: <ul style="list-style-type: none"> • Could lead to damage and/or destruction of the router either accidentally or from malicious activity resulting in loss of availability of service. • Financial loss from theft of the hardware and replacement costs and configuration charges of a new router. • Financial loss from environmental damage of the hardware and replacement costs and configuration charges of a new router. • Data theft, loss or alteration from unauthorized access. • Lost productivity from system unavailability (DoS) This test checks V1.
Testing Procedure / Compliance Criteria	Locate the router and inspect the physical security of the room. <ul style="list-style-type: none"> • Is the room environmentally controlled and monitored? • Is the room locked? • Is access to the room controlled? • Is the room monitored? The test should reveal that the answer to all questions is yes.
Test Nature	Subjective
Evidence	Place holder
Findings	Place Holder

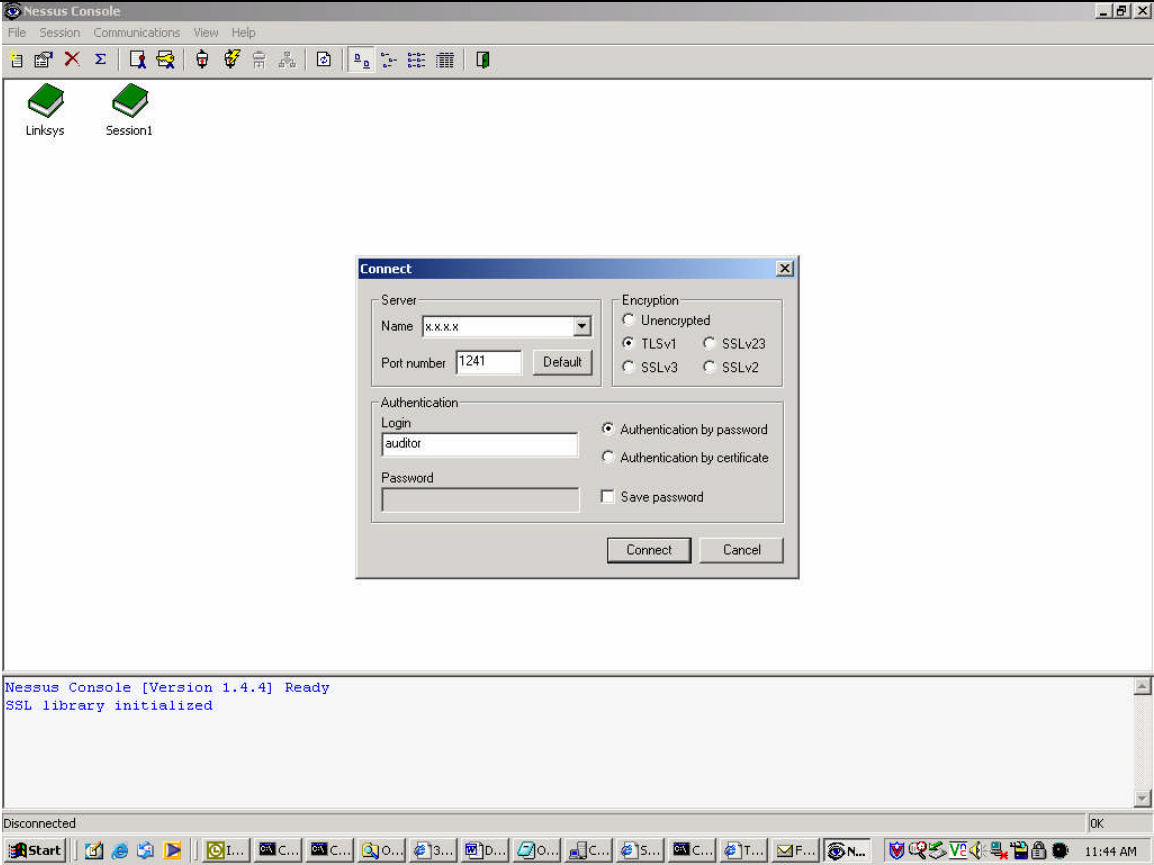


2.6. Item 6 Test Stateful Inspection

Reference	Personal Experience “Firewall Checklist 1.0” Items 2 and 3 URL: http://www.sans.org/score/checklists/FirewallChecklist.doc
Risk	If stateful Inspection is not working properly people may be able to fool the firewall into allowing malicious traffic into the network over well known ports as the firewall will assume it to be whatever type of traffic is normally on that port. This again could lead to unauthorized access or introduction of malware. This test checks V4.
Testing Procedure / Compliance Criteria	Run netcat listening on port 25 and handing out a command prompt on connection. Set netcat listening on port 25 nc -l -p 25 -t -e cmd.exe -l listen -p port -t answer telnet negotiation -e inbound program to execute From outside the firewall connect to the listening machine Nc x.x.x.x 25 If stateful inspection is working the connection should be dropped as it will be recognized that it is not valid smtp traffic even though it is on port 25. If you receive a command prompt and can continue to enter commands stateful inspection is not functioning.
Test Nature	Objective
Evidence	Place holder
Findings	Place Holder

2.7. Item 7 Test for Known Exploits

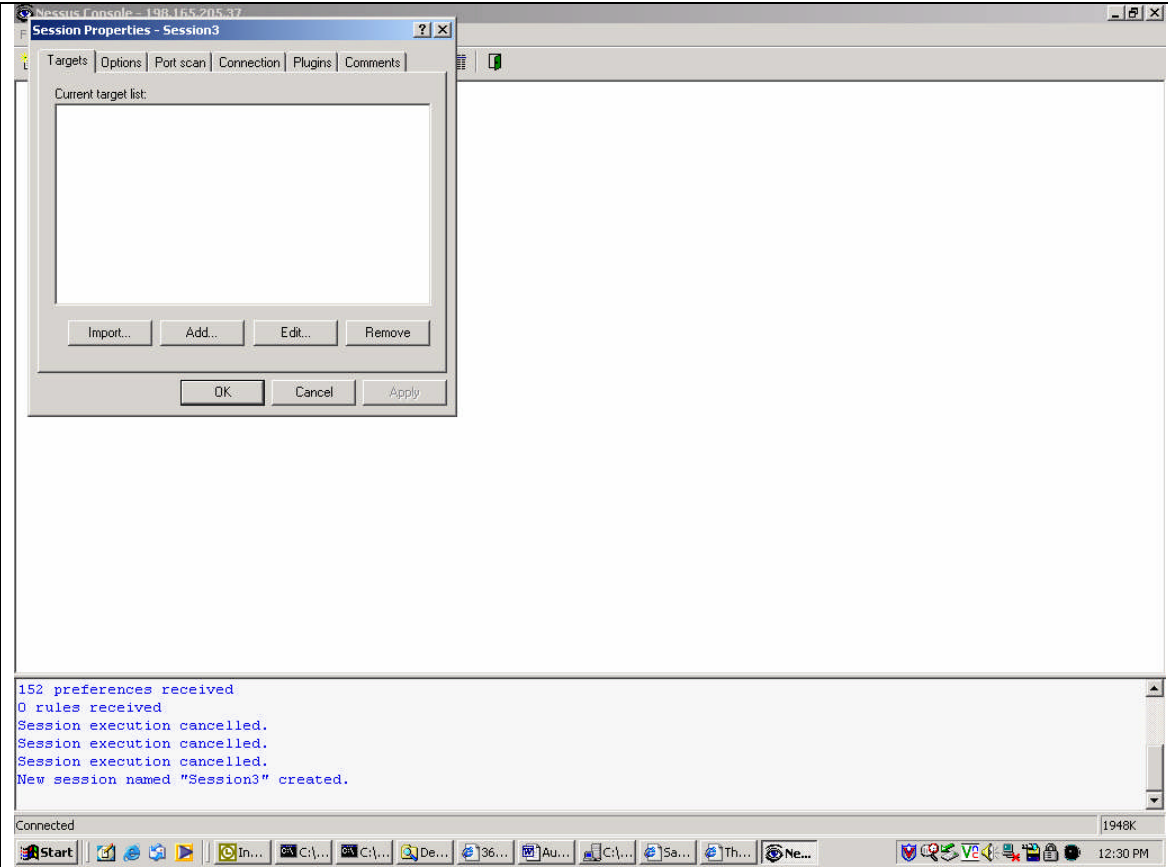
Reference	Spitzner, Lance. “Auditing your Firewall Setup” 12 December, 2000 URL: http://www.spitzner.net/audit.html Personal Experience “Firewall Checklist 1.0” Item 5 URL: http://www.sans.org/score/checklists/FirewallChecklist.doc Router Security Configuration Guide, p. 246 http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf
Risk	Known exploits from unpatched code could allow for unauthorized access or introduction of malware. Test checks V2
Testing Procedure / Compliance Criteria	Run nessus from the Internet scanning the outside interface of the router for known exploits. Start Nessuswx from Start Menu > Programs > NessusWx Connect to Nessus server by entering the IP address and login ID. Then enter password when prompted.



Nessus Console [Version 1.4.4] Ready
SSL library initialized

Disconnected

Create a new session by selecting new from the session menu and enter a description when prompted.
Add host to be scanned on the targets tab of the session properties window by clicking add.

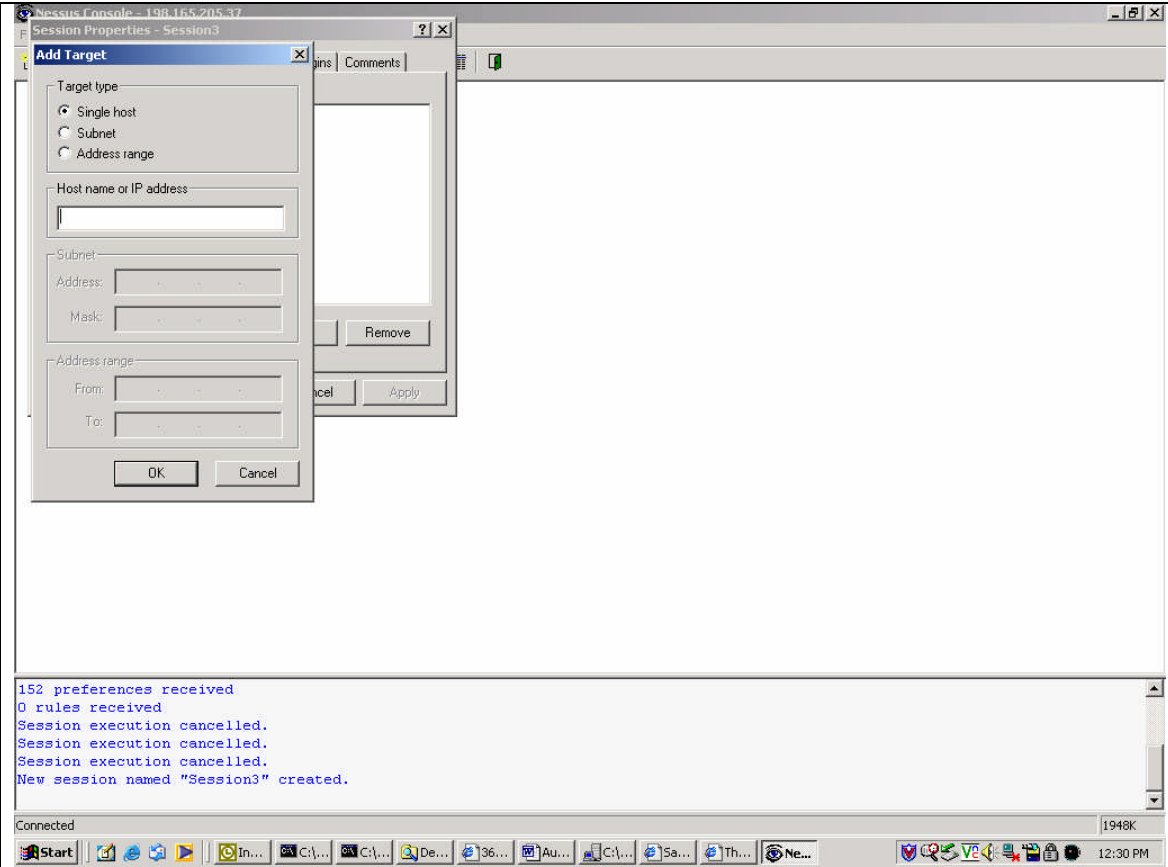


The screenshot shows the Nessus Console interface. A 'Session Properties - Session3' dialog box is open, displaying the 'Targets' tab. The 'Current target list' is empty, and buttons for 'Import...', 'Add...', 'Edit...', and 'Remove' are visible. Below the dialog box, the console output shows the following text:

```
152 preferences received  
0 rules received  
Session execution cancelled.  
Session execution cancelled.  
Session execution cancelled.  
New session named "Session3" created.
```

The console status bar at the bottom indicates 'Connected' and '1948K'. The Windows taskbar at the bottom shows the Start button and several open applications, including Internet Explorer, Outlook, and Nessus.

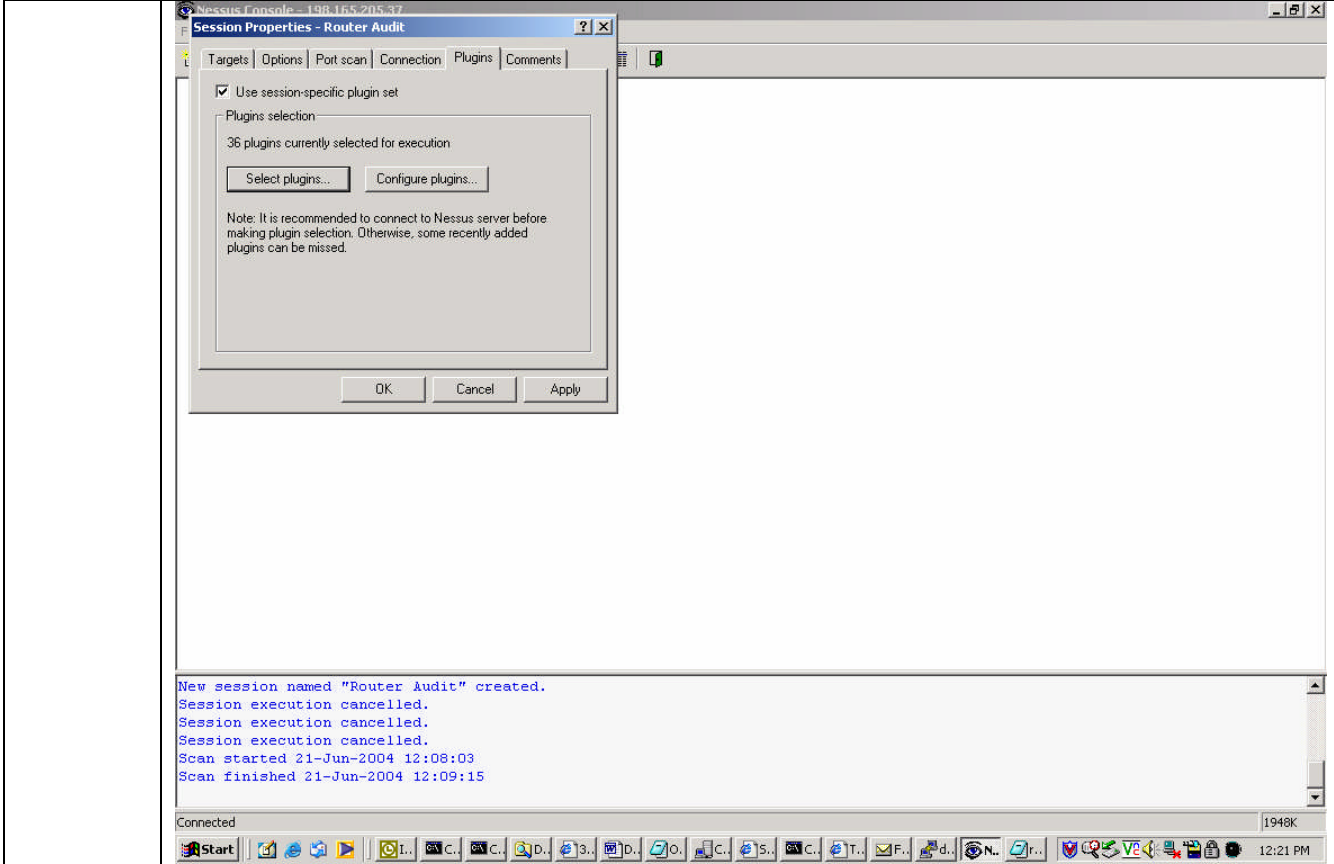
Add Host to be scanned by selecting single host radio button and entering the IP address of the router.



152 preferences received
0 rules received
Session execution cancelled.
Session execution cancelled.
Session execution cancelled.
New session named "Session3" created.

Connected 1948K 12:30 PM

Select plugins to use in testing by pushing the select plugins button on the plugins tab



Session Properties - Router Audit

Targets | Options | Port scan | Connection | Plugins | Comments

☒ Use session-specific plugin set

Plugins selection

36 plugins currently selected for execution

Select plugins... Configure plugins...

Note: It is recommended to connect to Nessus server before making plugin selection. Otherwise, some recently added plugins can be missed.

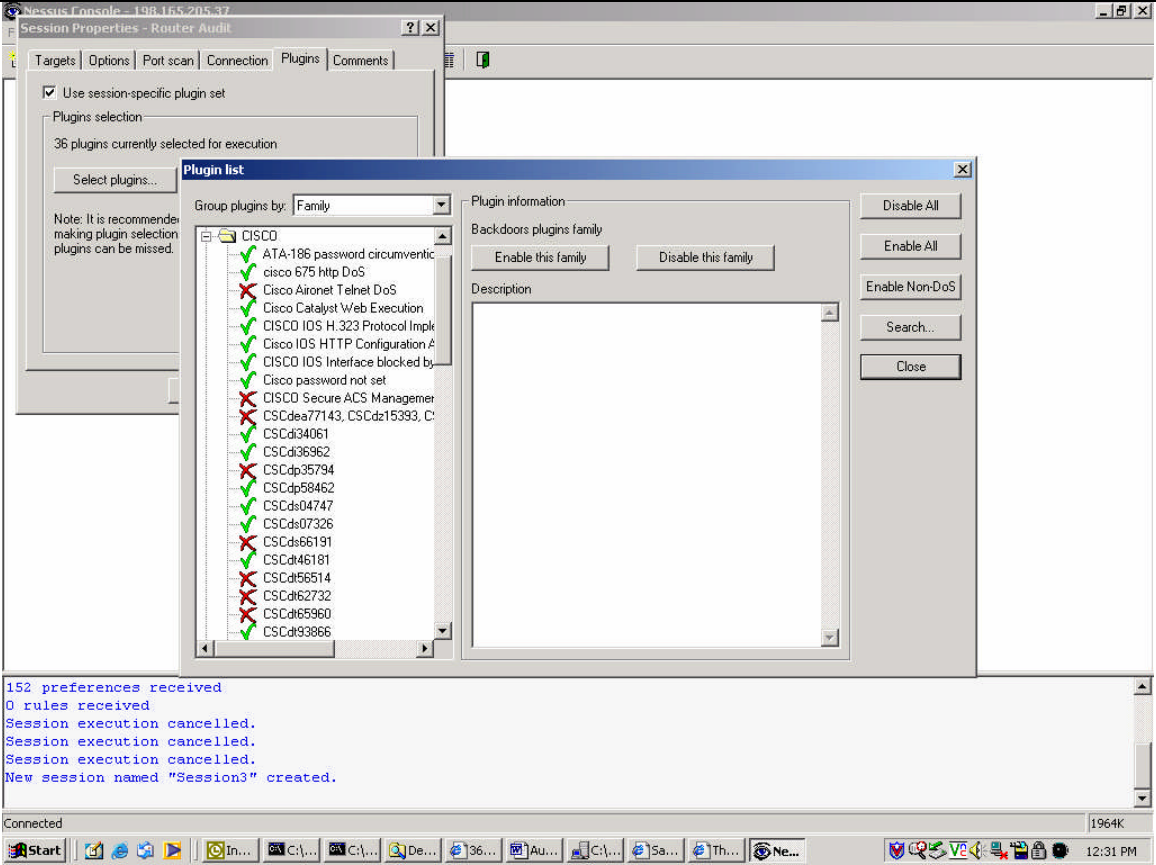
OK Cancel Apply

New session named "Router Audit" created.
Session execution cancelled.
Session execution cancelled.
Session execution cancelled.
Scan started 21-Jun-2004 12:08:03
Scan finished 21-Jun-2004 12:09:15

Connected 1948K

12:21 PM

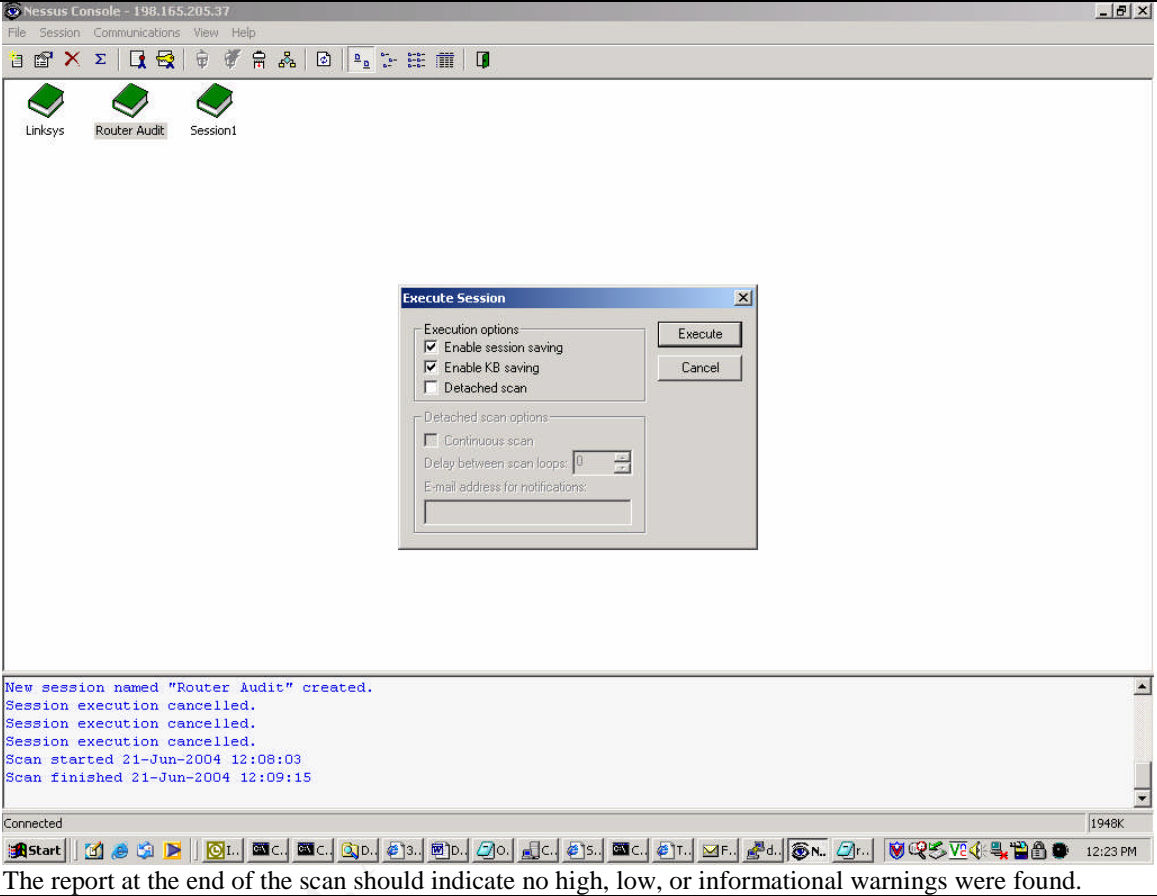
Enable the desired plugins from the Cisco family



152 preferences received
0 rules received
Session execution cancelled.
Session execution cancelled.
Session execution cancelled.
New session named "Session3" created.

Connected

Select ok to save session.
Double click on the saved session and execute Scan

	 <p>New session named "Router Audit" created. Session execution cancelled. Session execution cancelled. Session execution cancelled. Scan started 21-Jun-2004 12:08:03 Scan finished 21-Jun-2004 12:09:15</p> <p>The report at the end of the scan should indicate no high, low, or informational warnings were found.</p>
Test Nature	Objective
Evidence	Place holder
Findings	Place Holder

2.8. Item 8 Determine Business Requirements

Reference	Spitzner, Lance. "Auditing your Firewall Setup" 12 December, 2000 URL: http://www.spitzner.net/audit.html Personal Experience "Firewall Checklist 1.0" Item 8 URL: http://www.sans.org/score/checklists/FirewallChecklist.doc
Risk	In the absence of a security policy the only way to determine appropriate rule sets is to determine what the business requirements are. If the business requirements are not understood least privilege and deny all and permit only what is required can not be implemented. Resulting in too much access which could lead to unauthorized access or introduction of malware. This test checks V7, V2, and V4.
Testing Procedure / Compliance Criteria	Interview IT manager and CEO to determine business requirements for day to day operations. <ul style="list-style-type: none"> • Ask what tools/applications are required to perform various job functions • Ask what applications need to be accessed by the general public • Ask what applications need to be accessed by remote users • Ask what applications need to be accessed by business partners Test will result in a complete list of all inbound and outbound access required to operate

	business.
Test Nature	Subjective
Evidence	Place holder
Findings	Place Holder

2.9. Item 9 Compare ACL's to Business Requirements

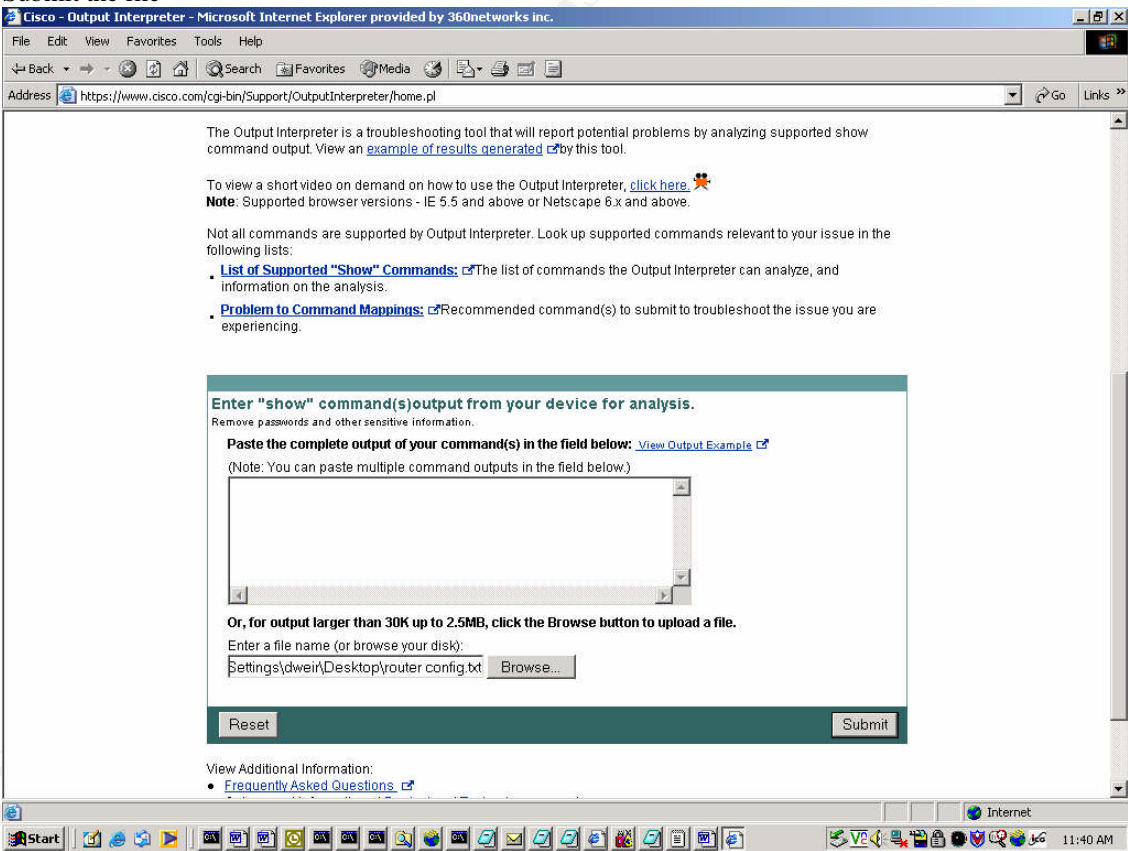
Reference	Spitzner, Lance. "Auditing your Firewall Setup" 12 December, 2000 URL: http://www.spitzner.net/audit.html Personal Experience "Firewall Checklist 1.0" Item 8 URL: http://www.sans.org/score/checklists/FirewallChecklist.doc
Risk	If access is not restricted to only what is required, unnecessary services and or applications may lead to unauthorized access or introduction of malware. This test checks V2 and V4.
Testing Procedure / Compliance Criteria	Compare compiled list of ports required inbound and outbound from questions above to the actual Ingress and Egress ACL's applied to the interfaces. Connect to the console of the router using Procomm plus set to use 9600 baud, no parity 8 data bits and 1 stop bit and login using the console password. Put the router in enable mode and then config mode by typing enable followed by the enable password and then typing config t. Examine the running configuration by typing show running-config and determine what ACL is applied to the interfaces and in which direction. Then compare the appropriate ACL's with the list of ports compiled from the business requirements to determine if they match. Test should reveal only ports with business requirements as defined by IT director and CEO should be allowed inbound or outbound.
Test Nature	Objective
Evidence	Place holder
Findings	Place Holder

2.10. Item 10 Compare Current Router Config with Best Practices

Reference	Router Security Configuration Guide, p. 249 http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf Personal Experience Improving Security on Cisco Routers http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
Risk	A misconfigured or inappropriately hardened router could lead to unauthorized access or introduction of malware. This test checks V6
Testing Procedure / Compliance Criteria	Use RAT to determine if the router is configured as per best practice rat --snarf --user=dweir --userpw=password --enablepw=EnabL3 x.x.x.x --user username --userpw password for username --enablepw enable password x.x.x.x IP address of router interface Test should reveal no major deviations from best practice.
Test Nature	Objective
Evidence	Place holder

Findings	Place Holder
----------	--------------

2.11. Item 11 Compare Current Router Config with Cisco Recommendations

Reference	<p>Router Security Configuration Guide http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf Personal Experience Improving Security on Cisco Routers http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml</p>
Risk	A misconfigured or inappropriately hardened router could lead to unauthorized access or introduction of malware. This test checks V6
Testing Procedure / Compliance Criteria	<p>Use Cisco output interpreter to see if router is configured as per Cisco's recommendations Go to https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl Login using Cisco cco account and password Browse to the config file you saved using a show running-config Submit the file</p>  <p>Test should reveal no warnings or errors about your configuration</p>
Test Nature	Objective
Evidence	Place holder
Findings	Place Holder

2.12. Item 12 Compare ACL's to Firewall Best Practices



Reference	<p>“Ports to Block at the Firewall” http://www.sans.org/top20/#ports Personal Experience “Firewall Checklist 1.0” Items 1,9 and 11 URL: http://www.sans.org/score/checklists/FirewallChecklist.doc</p>
Risk	Access to open ports in the network could lead to exploits of running services allowing unauthorized access or introduction of malware. Test checks for V4
Testing Procedure / Compliance Criteria	<p>Compare applied ACL’s to firewall best practice. Again using the ACL’s gathered in Item 9 compare these to the firewall checklist 1.0 and ports to block at the firewall from SANS to insure that the recommended ports are blocked and anti-spoofing rules are in place.</p> <p>Test should reveal firewall is configured as per checklist and the appropriate ports are blocked.</p>
Test Nature	Objective
Evidence	Place holder
Findings	Place Holder

2.13. Item 13 Check for Logon Banner

Reference	<p>Router Security Configuration Guide p. 57-58 http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf Personal Experience Improving Security on Cisco Routers http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml</p>
Risk	Without a logon banner it may be difficult to prosecute breaches of their network. This tests checks V6
Testing Procedure / Compliance Criteria	<p>Connect to router and see if logon banner is displayed. Telnet to the outside interface of the router and observe if a warning banner is displayed advising people that the device is monitored and unauthorized uses are prohibited prior to the login prompt.</p> <p>telnet x.x.x.78</p> <p>When you connect banner should be displayed prior to receiving logon prompt</p>
Test Nature	Objective
Evidence	Place holder
Findings	Place Holder

2.14. Item 14 Check Change Control

Reference	Personal Experience
Risk	If proper change control is not followed it may be possible using social engineering to gain unauthorized access to the network. This test checks V4
Testing Procedure / Compliance Criteria	<p>Call consultant who manages the router and see if he follows correct change control process or if he makes changes or provides information without verifying the request is legitimate and authorized.</p> <p>Call consultant and advise him you are calling to have a change made to the DML router and ask to have an ACL modified to permit access from a host to DML’s network.</p> <p>Consultant should deny request until it can be authenticated to insure it is a valid request. If he makes the change without validating the request with DML</p>

	change control is not being implemented properly.
Test Nature	Subjective
Evidence	Place holder
Findings	Place Holder

3. Part #3 - Audit Testing, Evidence, and Findings

Security is really a balancing act between required security and cost. Since nothing can ever be 100% secure it comes down to what is considered a satisfactory level of security based on cost of implementation. There is no point in spending \$10, 000 on security to protect a \$500 asset so it is always a juggling act between risk, impact, and cost to mitigate the various risks.

It is also a juggling act between time to implement required changes and risk of not implementing change. Since time is such a critical factor we have to prioritize even the items in our check list for this audit. It has been decided that time will only permit the 10 most critical checks to be performed at this time with the others to be completed at a later date.

Therefore we have decided that items 11 – 14 are to be left off the audit for now.

Item 11 has been determined to be low risk since it evaluates our router configuration against Cisco's recommended configuration, which should not be substantially different from Item 10, which evaluates our configuration against industry best practice for Cisco routers.

Item 12 has been determined to be low risk as well since we are implementing a deny all except for specific permits to meet business requirements. While there may be some risk from missing anti-spoofing rules etc. the only ports that will be open for attack will be those required in order to operate.

Item 13 has been determined to be low risk as well since the logon banner does nothing to improve security as it is only required for legal reasons. It may not be possible to admit evidence in court or to prosecute without a warning banner advising that the device is monitored and unauthorized uses are prohibited. So while there is a risk that there may be no recourse if the network is breached the primary reason for the audit was to insure that the network was as secure as possible.

Finally Item 14 has been determined to be low risk as well since the consultant looking after the router is a security consultant it should be fair to assume that he will take the appropriate precautions when a change request is made. When time permits though this test should be performed to insure the consultant is following proper procedures.

Now that we have determined which 10 tests are most critical to insuring the network is as secure as possible lets take a look at the evidence and findings from those tests.

3.1. Evidence and Findings from Test Item 1

Evidence:

```
# nmap 3.50 scan initiated Mon Jun 28 10:08:22 2004 as: nmap -v -g53 -sS -sU -sR -P0-O -p1-65535 -oN firewall.txt x.x.x.78
```

Interesting ports on hx-x-x-x.cust.domain.com (x.x.x.78):

(The 131066 ports scanned but not shown below are in state: filtered)

PORT	STATE	SERVICE	VERSION
23/tcp	open	telnet	
500/udp	open	isakmp	
515/tcp	open	printer	
4500/udp	open	sae-urn	

```
# Nmap run completed at Mon Jun 28 17:57:09 2004 -- 1 IP address (1 host up) scanned in 28130.025 seconds
```

Findings:

The only four ports opened are telnet, isakmp, non500-isakmp and line printer.

The printer service is port forwarded internally to a printer to allow for printing from an external partner. The risk of this is **low** as someone could waste a lot of paper by sending the dictionary etc. to the printer or possibly cause a DoS attack on the printer. Both of these would have very little financial or operating impact on DML. To minimize risk access to port 515 could be limited to the partners IP range.

The telnet service running on the router is to allow remote administration of the router. The risk of this is **high** as someone could gain remote access to the router allowing for unauthorized access, which could have large financial and operating impact on DML. If someone gains control of the router they have full control to DML's network allowing for DoS and/or unauthorized access. Remote administration should be changed to use SSH or be via the IPSEC tunnel that is already configured.

Both isakmp and non500-isakmp are required in support of the IPSEC tunnels. Since IPSEC itself is considered secure the risk to having these ports open is **low** and they are required for the VPN access which is a business requirement of the operation.

3.2. Evidence and Findings from Test Item 2

Evidence:

```
# nmap 3.50 scan initiated Tue Jun 29 08:55:16 2004 as: nmap -v -g53 -sS -sU -sR -P0-O -p1-65535 -oN network.txt x.x.x.192/28
```

All 131070 scanned ports on x.x.x.192 are: filtered

All 131070 scanned ports on n033h193.testdomain.com (x.x.x.193) are: filtered

All 131070 scanned ports on n033h194.testdomain.com (x.x.x.194) are: filtered

Interesting ports on n033h195.testdomain.com (x.x.x.195):

(The 131067 ports scanned but not shown below are in state: filtered)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

25/tcp	open	smtp	
--------	------	------	--

80/tcp	open	http	
--------	------	------	--

443/tcp	open	https	
---------	------	-------	--

Interesting ports on n033h196.testdomain.com (x.x.x.196):

(The 131063 ports scanned but not shown below are in state: filtered)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

20/tcp	closed	ftp-data	
--------	--------	----------	--

21/tcp	open	ftp	
--------	------	-----	--

25/tcp	closed	smtp	
--------	--------	------	--

80/tcp	open	http	
--------	------	------	--

110/tcp	closed	pop3	
---------	--------	------	--

123/tcp	closed	ntp	
---------	--------	-----	--

443/tcp	open	https	
---------	------	-------	--

All 131070 scanned ports on n033h197.testdomain.com (x.x.x.197) are: filtered

All 131070 scanned ports on n033h198.testdomain.com (x.x.x.198) are: filtered

All 131070 scanned ports on n033h199.testdomain.com (x.x.x.199) are: filtered

All 131070 scanned ports on n033h200.testdomain.com (x.x.x.200) are: filtered

All 131070 scanned ports on n033h201.testdomain.com (x.x.x.201) are: filtered

All 131070 scanned ports on n033h202.testdomain.com (x.x.x.202) are: filtered

All 131070 scanned ports on n033h203.testdomain.com (x.x.x.203) are: filtered

Interesting ports on n033h204.testdomain.com (x.x.x.204):

(The 131068 ports scanned but not shown below are in state: filtered)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------



20/tcp closed ftp-data
21/tcp open ftp

All 131070 scanned ports on n033h205.testdomain.com (x.x.x.205) are: filtered

All 131070 scanned ports on n033h206.testdomain.com (x.x.x.206) are: filtered

All 131070 scanned ports on x.x.x.207 are: filtered

Nmap run completed at Tue Jun 29 14:43:09 2004 -- 16 IP addresses (16 hosts up) scanned in
20873.806 seconds

Findings:

Three machines were determined to have ports that were accessible from the Internet.

The first machine x.x.x.195 has three accessible ports 25, 80 and 443. It was determined through discussions with the system administrator that this machine was the corporate mail server and provided web access to mail. All three of these ports are required to provide business requirements however the risk from having these three ports open is **high** as the server resides in the private network as opposed to in a DMZ and these services have continued to have frequent security flaws that could lead to exploits. If these services are exploited and someone gains access to the box they will then have full access to other devices in the internal network as they will be past the firewall. To minimize risk a DMZ should be created and a front-end exchange server should be put in the DMZ to act as a mail relay and to provide web access to mail. Once these services are relocated to a DMZ if the box is breached it still does not provide access to the other internal devices as they are still separated by the firewall.

The second machine x.x.x.196 has seven accessible ports 20,21, 25, 80, 110, 123, and 443. It was determined through discussions with the system administrator that this machine is an ftp server but also use to be the mail server before the new exchange server was installed. Of these seven ports the only one that is still required for business operations is 21 and the risk to having these ports accessible is **high**. To minimize risks the six unneeded ports should be blocked as they provide extra services to try and exploit and serve no business function. Also to minimize risk the ftp service should be relocated to the newly created DMZ so if the box is breached it still does not provide access to the other internal devices as they are still separated by the firewall.

The third machine x.x.x.204 has two accessible ports 20 and 21. It was determined through discussions with the system administrator that this machine was also an ftp server. Again the risk is **high** as there is an unneeded port accessible and the ftp service while required should be in the DMZ as per above.

3.3. Evidence and Findings from Test Item 3

Evidence:

From vlan 10

```
# nmap 3.50 scan initiated Wed Jun 30 10:53:40 2004 as: nmap -v -g53 -sS -sR -P0-O -p1-65535 -oN fromvlan10.txt x.x.x.23
```

Interesting ports on test.testdomain.com (x.x.x.23):

(The 66542 ports scanned but not shown below are in state: filtered)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

21/tcp	open	ftp	
--------	------	-----	--

23/tcp	open	telnet	
--------	------	--------	--

25/tcp	open	smtp	
--------	------	------	--

53/tcp	closed	domain	
--------	--------	--------	--

53/udp	closed	domain	
--------	--------	--------	--

80/tcp	open	http	
--------	------	------	--

110/tcp	open	pop3	
---------	------	------	--

119/tcp	closed	nntp	
---------	--------	------	--

123/tcp	closed	ntp	
---------	--------	-----	--

443/tcp	open	https	
---------	------	-------	--

554/tcp	closed	rtsp	
---------	--------	------	--

1720/tcp	closed	H.323/Q.931	
----------	--------	-------------	--

1755/tcp	closed	wms	
----------	--------	-----	--

8000/tcp	closed	http-alt	
----------	--------	----------	--

8080/tcp	open	http-proxy	
----------	------	------------	--

8554/tcp	open	unknown	
----------	------	---------	--

1024-65535/udp open (grouped together for simplicity would all be listed out individually in actual results)

```
# Nmap run completed at Wed Jun 30 11:01:15 2004 -- 1 IP address (1 host up) scanned in 456.173 seconds
```

From vlan 20

```
# nmap 3.50 scan initiated Wed Jun 30 10:53:40 2004 as: nmap -v -g53 -sS -sR -P0-O -p1-65535 -oN fromvlan10.txt x.x.x.23
```

Interesting ports on test.testdomain.com (x.x.x.23):

(The 66541 ports scanned but not shown below are in state: filtered)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

21/tcp	open	ftp	
--------	------	-----	--

25/tcp	open	smtp	
--------	------	------	--

53/tcp	closed	domain	
--------	--------	--------	--

53/udp	closed	domain	
--------	--------	--------	--

80/tcp	open	http	
--------	------	------	--

110/tcp	open	pop3	
---------	------	------	--

119/tcp	closed	nntp	
---------	--------	------	--

123/tcp	closed	ntp	
---------	--------	-----	--

443/tcp	open	https	
---------	------	-------	--

554/tcp	closed	rtsp	
---------	--------	------	--

1720/tcp	closed	H.323/Q.931	
----------	--------	-------------	--

1755/tcp	closed	wms	
----------	--------	-----	--

8000/tcp	closed	http-alt	
----------	--------	----------	--

8080/tcp	open	http-proxy	
----------	------	------------	--



8554/tcp open unknown

1024-65535/udp open (grouped together for simplicity would all be listed out individually in actual results)

Nmap run completed at Wed Jun 30 11:01:15 2004 -- 1 IP address (1 host up) scanned in 456.173 seconds

Findings:

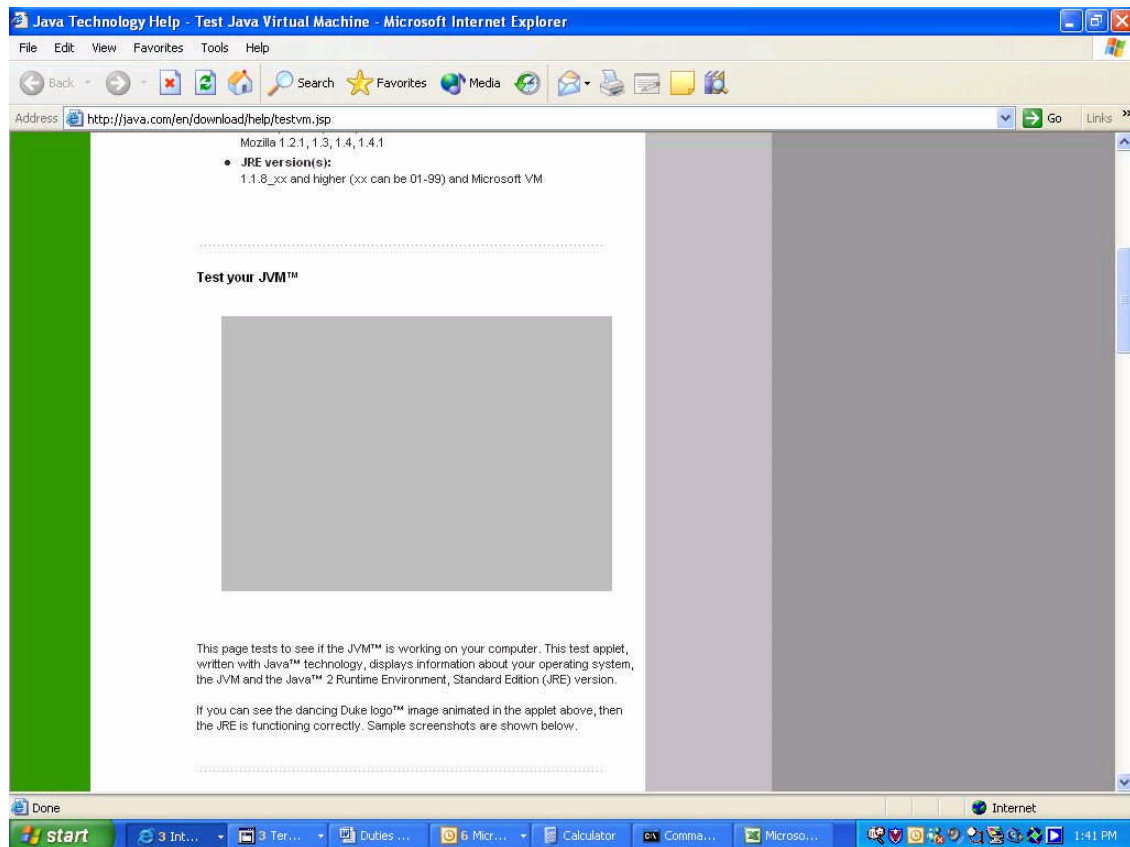
It was determined that access from both VLAN's were essentially the same with the only difference being that VLAN 10 also permitted telnet access outbound.

Outbound access was restricted to select ports resulting in a **low** risk to DML. However it was determined that five ports were allowed access while they were not required to accomplish the desired business functions. These five ports were: tcp/udp 53 for DNS while machines should in fact be using internal DNS servers, tcp 25 for outbound mail while mail should be being sent to the internal mail server only, tcp 110 for POP3 while machines should be only popping mail from the internal mail server, and tcp 123 for NTP when machines should be synching time with an internal NTP server.

3.4. Evidence and Findings from Test Item 4

Evidence:





Findings:

Java is being stripped out at the router as illustrated by the fact that we get a blank grey box as opposed to the dancing Duke logo. Java is **no longer a risk** of introducing malware.

3.5. Evidence and Findings from Test Item 5

Evidence:

A physical inspection reveals the router is mounted on the wall of a supply closet.

Is the room environmentally controlled and monitored? The room has no environmental control (HVAC) or monitoring systems.

Is the room locked? The room while inside of their corporate office space is accessible to all staff and/or visitors once they are past the receptionist and into DML's office space.

Is access to the room controlled? Access to the room is not controlled and people are in and out for supplies etc. with no logging or authentication.

Is the room monitored? There is no monitoring of who is coming and going from the room



Findings:

The room is inadequately secured and exposes DML to **high** risk. It is recommended that the router be relocated to a locked secure room where access is controlled to mitigate risk. Ideally the room would also be environmentally controlled and monitored but the cost of such systems is substantial for a small business and the risk of water, heat, fire, etc. damage is relatively low. They are better off mitigating financial loss from such an event by making sure they have appropriate levels and types of insurance in place.

3.6. Evidence and Findings from Test Item 6

Evidence:

C:\net>nc x.x.x.78 25

Microsoft(R) Windows NT(TM)

(C) Copyright 1985-1996 Microsoft Corp.

C:\net>

Findings:

The connection is immediately dropped as soon as non-smtp traffic is seen on port 25 so the stateful inspection is working. Stateful Inspection reduces the risk to **low** of having accessible ports since it limits traffic to a safer subset of commands and insures that traffic is of the type that it should be on that port.

3.7. Evidence and Findings from Test Item 7

Evidence:

NESSUS SECURITY SCAN REPORT

Created 21.06.2004

Sorted by host names

Session Name : Router Audit

Start Time : 21.06.2004 14:22:01

Finish Time : 21.06.2004 14:23:07

Elapsed Time : 0 day(s) 00:01:06

Plugins used in this scan:



Id Name

10982 CSCdt93866
11791 CISCO IOS Interface blocked by IPv4 Packet
10046 Cisco DoS
10973 CSCdi34061
10969 Obtain Cisco type via SNMP
10974 CSCdi36962
12039 CSCdy15598 and CSCeb56052
11383 CSCdz60229, CSCdy87221, CSCdu75477
12199 CSCed30113
10545 Cisco Catalyst Web Execution
11283 CSCdp58462
10045 Cisco 675 passwordless router
10970 GSR ACL pub
10976 CSCds04747
11380 CSCdz39284, CSCdz41124
10700 Cisco IOS HTTP Configuration Arbitrary Administrative Access
11056 CSCdy03429
10983 CSCdu20643
10561 cisco 675 http DoS
10972 Multiple SSH vulnerabilities
12023 CISCO IOS H.323 Protocol Implementation Flaws
10977 CSCds07326
11632 CSCdx17916, CSCdx61997
11012 ATA-186 password circumvention / recovery
10264 Default community names of the SNMP Agent
10754 Cisco password not set
10387 cisco http DoS
10971 GSR ICMP unreachable
10985 CSCdv48261
10979 CSCdt46181
11379 CSCdx92043
10265 An SNMP Agent is running



10987 CSCdw67458

11381 CSCdw33027

10551 Obtain network interfaces list via SNMP

10984 CSCdu81936

Preferences settings for this scan:

max_hosts = 16
max_checks = 40
log_whole_attack = yes
cgi_path = /cgi-bin
port_range = 1-1024
optimize_test = yes
language = english
checks_read_timeout = 5
non_simult_ports = 139, 445
plugins_timeout = 320
safe_checks = no
auto_enable_dependencies = no
use_mac_addr = no
save_knowledge_base = yes
kb_restore = no
only_test_hosts_whose_kb_we_dont_have = no
only_test_hosts_whose_kb_we_have = no
kb_dont_replay_scanners = no
kb_dont_replay_info_gathering = no
kb_dont_replay_attacks = no
kb_dont_replay_denials = no
kb_max_age = 864000
plugin_upload = no
plugin_upload_suffixes = .nasl, .inc
slice_network_addresses = no
ntp_save_sessions = yes
ntp_detached_sessions = yes
server_info_nessusd_version = 2.0.7



server_info_libnasl_version = 2.0.7
server_info_libnessus_version = 2.0.7
server_info_thread_manager = fork
server_info_os = Linux
server_info_os_version = 2.4.7-10
reverse_lookup = no
ntp_keep_communication_alive = yes
ntp_opt_show_end = yes
save_session = yes
detached_scan = no
continuous_scan = no

Total security holes found : 0

high severity : 0

low severity : 0

informational : 0

Scanned hosts:

Name	High	Low	Info
x.x.x.78	0	0	0

Findings:

The router IOS is not vulnerable to any of the known Cisco exploits as Nessus turned up no high, low, or informational warnings when the router was scanned. The risk to DML of exploits against the router is **low** as the router IOS is up to date and protected from the known exploits; however that still leaves any exploits that have not been discovered or made public yet.

3.8. Evidence and Findings from Test Item 8

Evidence:

After discussion with the Director of IT and the CEO it was determined that:



Egress:

VLAN 10 users require ability to ftp, telnet, send and receive mail, do dns queries, read news, browse the web via http and ssl, and have access to http on port 8000 and 8080. They also require access to tcp 1755, 554, 8554, 1720, and udp greater than 1023 to support streaming audio and training resources they access via the Internet.

Full IP access and GRE access to a partner network.

Full IP access to remote clients and remote test site via IPSEC tunnel is also required.

Full IP access to VLAN 20.

Selected hosts on VLAN 10 require additional access as documented below:

Host x.x.x.195 requires the ability to respond on tcp ports greater than 1023 in order to respond to requests from the Internet.

Host x.x.x.196 requires the ability to respond on tcp ports greater than 1023 in order to respond to requests from the Internet.

Host x.x.x.199 requires the ability to have a PPTP tunnel with host x.x.x.223 via the Internet.

Host x.x.x.203 requires the ability to have a PPTP tunnel with host x.x.x.120 via the Internet.

Host x.x.x.204 requires the ability to respond on tcp ports greater than 1023 in order to respond to requests from the Internet.

Host x.x.x.206 requires the ability to have a PPTP tunnel with host x.x.x.120 via the Internet.

VLAN 20 users require ability to ftp, send and receive mail, do dns queries, read news, browse the web via http and ssl, and have access to http on port 8000 and 8080. They also require access to tcp 1755, 554, 8554, 1720, and udp greater than 1023 to support streaming audio and training resources they access via the Internet.

Full IP access and GRE access to a partner network.

Full IP access to remote clients and remote test site via IPSEC tunnel is also required.



Full IP access to VLAN 10.

Selected hosts on VLAN 20 require additional access as documented below:

All hosts need to be able to telnet to x.x.x.83 via the Internet.

All hosts need to be able to have udp 554 and tcp/udp 5078 to x.x.x.50 via the Internet.

Host x.x.x.27 requires the ability to have full IP access with host x.x.x.223 via the Internet.

Host x.x.x.244 requires the ability to have full IP access with any host via the Internet.

Ingress:

Consultant requires remote access to the router for management purposes.

ESP, ISAKMP and non500-isakmp are required to the outside interface from anywhere to allow IPSEC VPN functionality.

GRE access is required from anywhere to anywhere.

HTTP, HTTPS, and SMTP access is required from anywhere to x.x.x.195.

FTP access is required from anywhere to x.x.x.196 and x.x.x.204.

DNS access between x.x.x.196 and two ISP DNS servers x.x.x.65 and x.x.x.129.

SQL access from x.x.x.245 to internal SQL server x.x.x.196 is required.

NTP responses from x.x.x.2, x.x.x.252, and x.x.x.53 to the outside router interface.

Full IP access to all hosts from remote VPN clients as well as from the site-to-site VPN to the test site.

Access to lpd and tcp 9100 from the partner network to the outside interface of the router is required.

Access to x-windows return traffic from partner network to machines on VLAN 10 is required.



Access to TCP 3000-3999 from the partner network to machines on VLAN 10 is required.

Full IP access from partner machine x.x.x.118 to internal host x.x.x.4

Full IP access from partner machine x.x.x.118 to internal host x.x.x.102

Full IP access from partner machine x.x.x.50 to internal host x.x.x.197.

Findings:

DML have a good understanding of what is required for them to do business and have tried to limit traffic to the bare minimum required to still function. The risk to DML of someone exploiting an unnecessary service is **low** since DML have a good understanding of what they need to allow and intend to block all other access.

3.9. Evidence and Findings from Test Item 9

Evidence:

The following lines in the Ingress and Egress ACL's should be removed or modified.

Egress:

```
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq smtp
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq domain
access-list 122 permit udp x.x.x.192 0.0.0.15 any eq domain
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq pop3
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq 123
access-list 122 permit ip x.x.x.192 0.0.0.15 192.168.90.0 0.0.0.255
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq smtp
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq domain
access-list 122 permit udp 10.0.0.0 0.0.0.255 any eq domain
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq pop3
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq 123
access-list 122 permit ip 10.0.0.0 0.0.0.255 192.168.90.0 0.0.0.255
access-list 122 permit esp any any
access-list 122 permit tcp x.x.x.192 0.0.0.15 host x.x.x.193
access-list 122 permit tcp 10.0.0.0 0.0.0.255 host x.x.x.100 eq 1723
access-list 122 permit tcp x.x.x.192 0.0.0.15 host x.x.x.100 eq 1723
access-list 122 permit udp 10.0.0.0 0.0.0.255 any eq 1755
access-list 122 permit udp x.x.x.192 0.0.0.15 any eq 1755
access-list 122 permit udp host x.x.x.203 host x.x.x.223 eq isakmp
access-list 122 permit udp host x.x.x.199 host x.x.x.223 eq isakmp
```

```
access-list 122 permit tcp host 10.0.0.27 host x.x.x.120 eq 1723
access-list 122 permit gre host 10.0.0.27 host x.x.x.120
access-list 122 permit tcp host 10.0.0.28 host x.x.x.120 eq 1723
access-list 122 permit gre host 10.0.0.28 host x.x.x.120
access-list 122 permit udp host x.x.x.195 any gt 1023
access-list 122 permit udp host x.x.x.196 any gt 1023
access-list 122 permit ip host 10.0.0.44 host x.x.x.118
access-list 122 permit ip 10.0.0.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 122 permit ip 10.0.0.0 0.0.0.255 10.1.2.0 0.0.0.255
access-list 122 permit udp host x.x.x.204 any gt 1023
```

Ingress

```
access-list 125 permit tcp any host x.x.x.189 eq telnet
access-list 125 permit ip 192.168.90.0 0.0.0.255 x.x.x.192 0.0.0.15
access-list 125 permit ip 192.168.90.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 125 permit tcp x.x.x.0 0.0.0.255 x.x.x.192 0.0.0.15 range 6000 7000
access-list 125 permit udp x.x.x.0 0.0.0.255 x.x.x.192 0.0.0.15 range 6000 7000
access-list 125 permit tcp any host x.x.x.196 eq smtp
access-list 125 permit tcp any host x.x.x.196 eq ftp-data
access-list 125 permit tcp any host x.x.x.196 eq www
access-list 125 permit tcp any host x.x.x.196 eq pop3
access-list 125 permit tcp any host x.x.x.196 eq 123
access-list 125 permit tcp any host x.x.x.196 eq 443
access-list 125 permit udp any any eq isakmp
access-list 125 permit tcp any host x.x.x.78 eq telnet
access-list 125 permit ip host x.x.x.223 host 10.0.0.27
access-list 125 permit ip 10.1.1.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 125 permit ip 10.1.2.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 125 permit ip x.x.x.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 125 permit tcp any host x.x.x.204 eq ftp-data
access-list 125 permit udp host x.x.x.41 host x.x.x.78 eq ntp
```

Findings:

DML has done a good job of trying to limit traffic to only what is required both inbound and outbound however unfortunately as requirements changed it appears they have not been as diligent in updating their filter lists. Also it has been determined in some instances while the access-list does provide the required access there are ways that it could have been configured more securely while still allowing the same functionality. Finally in some instances it appears there may have been some errors in creating the lists themselves, which would have been caught if there had been an audit procedure in place.



Since the ACL's do have some unnecessary holes in them it poses a **medium** risk to DML. It is recommended that the access lists be modified so as they accurately reflect the true "current" business requirements as well as take advantage of some architecture changes that would allow for more secure configuration.

The following suggested changes should be considered:

SMTP outbound should be restricted to the mail server only as opposed to everybody being able to send mail out. The current set-up allows for mail to be sent out bypassing the corporate mail server, which could cause confidentiality issues as well as provide a path for documents to be removed from site without being logged, scanned, etc. It also provides a mechanism for infected machines to act as a mail relay etc. possibly leading to inadvertent disclosure of private information and reduced productivity from network congestion.

DNS queries should be restricted to the DNS server with all clients querying the internal DNS server(s). There also should be a secondary DNS server internal to help prevent DoS or outages caused by issues with the single internal DNS server. Currently any PC can query any DNS server they choose which may again cause issues such as cache poisoning etc and may lead to additional trouble shooting problems. Finally it is possible for someone to run something else over udp 53 as it is an unnecessary hole in the filter list.

Both tcp 110 and 123 should be removed as they appear to have been added in error. While some users pop mail internally there is no instance of an external user popping mail from the internal server. As for tcp 123 it is assumed it should have been udp 123 for ntp however this as well is not required; as devices internally should synch to an internal ntp server as opposed to every machine synching with an external ntp server. There are already holes added to allow internal ntp servers to synch to external ntp servers. Both of these services again are unnecessary and offer extra points of exploitation.

Access to 192.68.90.0/24 should be removed this was another site-to-site VPN to New Orleans but that office has been closed down for a couple of months. Again it is unnecessary access, which could be exploited.

ESP from anywhere to anywhere also should be removed; as it is unnecessary. It was added in anticipation of having VPN access to outside companies using IPSEC but it turned out that the companies used PPTP instead for their VPN's. Having said this once these companies support IPSEC the VPN connections should be switched to this from PPTP as it offers more security.

Allowing all access to the inside router interface is not required and in fact should never be allowed this line should be removed.

Allowing access to TCP 1723 to a host on the partner network is not required since all traffic is permitted outbound to the partner network. While it does not provide any additional threat since all ports are already allowed it is just unnecessary and an extra line to be processed, for efficiency it should be removed.

Allowing access to UDP 1755 to any host is not required since all udp greater than 1024 is permitted outbound. While it does not provide any additional threat since all ports are already allowed it is just unnecessary and an extra line to be processed, for efficiency it should be removed. Also noteworthy is the line that allows all UDP access should be greater than 1023 not the current 1024.

Allowing ISAKMP access to two hosts is also unnecessary again as these VPN's ended up being PPTP as opposed to IPSEC.

Allowing PPTP connections from 10.0.0.27 and 10.0.0.28 was also a temporary requirement that is no longer needed and should be removed.

Allowing access to UDP greater than 1023 to any host from x.x.x.195, x.x.x.196, and x.x.x.204 is not required since all udp greater than 1024 is permitted outbound. While it does not provide any additional threat since all ports are already allowed it is just unnecessary and an extra line to be processed, for efficiency it should be removed. Also noteworthy is the line that allows all UDP access should be greater than 1023 not the current 1024.

Allowing access from host x.x.x.44 to a host on the partner network is not required since all traffic is permitted outbound to the partner network. While it does not provide any additional threat since all ports are already allowed it is just unnecessary and an extra line to be processed, for efficiency it should be removed.

Finally permitting traffic to 10.1.1.0/24 and 10.1.2.0/24 was for a failed project with the partner that is also no longer required.

Similarly on the Ingress side:

Telnet access to x.x.x.189 is not required it was the old outside interface of the router.

Access from 192.168.90.0/24 is not required anymore either as it was an old site-to-site tunnel connection from a closed office in New Orleans.

Access for tcp/udp 6000-7000 should be changed as well. It should have only been tcp for x-windows access but both should be removed and x-windows

should be tunneled through ssh instead. It currently allows a large number of ports that could be exploited.

Access to SMTP, WWW, POP3, HTTPS, ftp-data, and TCP 123 to host x.x.x.196 should all be removed; as this server now is only an ftp server. In the past it was a mail server that required the extra ports opened. Both tcp 20 and 123 were most likely opened in error, as they were never required even on the old server.

Access to ISAKMP to anywhere is also not required and should be removed.

Telnet access to the outside interface should be changed while it is required to administer the router remotely this should be done over the existing IPSEC tunnel as an added layer of security.

Access to tcp 20 on host x.x.x.204 should be removed as it is not required it appears this was opened in error as well. It appears someone opened it believing they needed it for active ftp.

Finally permitting traffic from 10.1.1.0/24 and 10.1.2.0/24 was for a failed project with the partner that is also no longer required.

3.10. Evidence and Findings from Test Item 10

Evidence:

Router Audit Tool report for

x.x.x.78

Audit Date: Tue Jun 22 12:07:53 2004 GMT

Sort Order: importance,passfail,rule,device,instance,line

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number.

10	pass	IOS - require line passwords	x.x.x.78		
10	pass	IOS - no snmp-server	x.x.x.78		
10	pass	IOS - no ip http server	x.x.x.78		
10	pass	IOS - login default	x.x.x.78		
10	pass	IOS - forbid SNMP community public	x.x.x.78		
10	pass	IOS - forbid SNMP community private	x.x.x.78		



10	pass	IOS - enable secret	x.x.x.78		
10	pass	IOS - Create local users	x.x.x.78		
10	FAIL	IOS - apply VTY ACL	x.x.x.78	vtty 5 15	414
10	FAIL	IOS - apply VTY ACL	x.x.x.78	vtty 0 4	410
10	FAIL	IOS - Use local authentication	x.x.x.78	n/a	2
10	FAIL	IOS - Define VTY ACL	x.x.x.78	n/a	2
7	pass	IOS 12 - no udp-small-servers	x.x.x.78		
7	pass	IOS 12 - no tcp-small-servers	x.x.x.78		
7	pass	IOS 12 - no directed broadcast	x.x.x.78		
7	pass	IOS - no service config	x.x.x.78		
7	pass	IOS - no ip source-route	x.x.x.78		
7	pass	IOS - no cdp run	x.x.x.78		
7	pass	IOS - exec-timeout	x.x.x.78		
7	pass	IOS - encrypt passwords	x.x.x.78		
5	pass	IOS 12.1.2.3 - no finger service	x.x.x.78		
5	pass	IOS - tcp keepalive service	x.x.x.78		
5	pass	IOS - service timestamps logging	x.x.x.78		
5	pass	IOS - no ip bootp server	x.x.x.78		
5	pass	IOS - enable logging	x.x.x.78		
5	pass	IOS - VTY transport telnet	x.x.x.78		
5	FAIL	IOS - user password quality	x.x.x.78	sfinn	66
5	FAIL	IOS - user password quality	x.x.x.78	dweir	67
5	FAIL	IOS - set syslog server	x.x.x.78	n/a	2
5	FAIL	IOS - service timestamps debug	x.x.x.78	n/a	2
5	FAIL	IOS - ntp server 3	x.x.x.78	n/a	2
5	FAIL	IOS - ntp server 2	x.x.x.78	n/a	2
5	FAIL	IOS - ntp server	x.x.x.78	n/a	2
5	FAIL	IOS - logging buffered	x.x.x.78	n/a	52
5	FAIL	IOS - line password quality	x.x.x.78	vtty 5 15	416
5	FAIL	IOS - line password quality	x.x.x.78	vtty 0 4	412
5	FAIL	IOS - line password quality	x.x.x.78	con 0	404
5	FAIL	IOS - forbid clock summer-time - GMT	x.x.x.78	n/a	73
3	pass	IOS - logging trap info or higher	x.x.x.78		
3	pass	IOS - logging console critical	x.x.x.78		
3	pass	IOS - disable aux	x.x.x.78		
3	FAIL	IOS - clock timezone - GMT	x.x.x.78	n/a	2

Summary for x.x.x.78



#Checks	#Passed	#Failed	%Passed
42	25	17	59
Perfect Weighted Score	Actual Weighted Score	%Weighted Score	
278	175	62	

Overall Score (0-10)
6.2

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.

Fix Script for x.x.x.78

! The following commands may be entered into the router to fix
! problems found. They must be entered in config mode (IOS). Fixes
! which require specific information (such as uplink interface device
! name) are listed but commented out. Examine them, edit and uncomment.
!
! THESE CHANGES ARE ONLY RECOMMENDATIONS.
!
! CHECK THESE COMMANDS BY HAND BEFORE EXECUTING. THEY MAY BE WRONG.
! THEY MAY BREAK YOUR ROUTER. YOU ASSUME FULL RESPONSIBILITY FOR THE
! APPLICATION OF THESE CHANGES.

! enter configuration mode
configure terminal

! RULE: IOS - apply VTY ACL
line vty 5 15
access-class 182 in
exit

! RULE: IOS - apply VTY ACL
line vty 0 4
access-class 182 in



exit

! RULE: IOS - Use local authentication

aaa new-model

aaa authentication login default local

aaa authentication enable default enable

! RULE: IOS - Define VTY ACL

no access-list 182

access-list 182 permit tcp 192.168.1.0 0.0.0.255 any

access-list 182 permit tcp host 192.168.1.254 any

access-list 182 deny ip any any log

! RULE: IOS - user password quality

!

! This fix is commented out because you have to supply a sensitive value.

! To apply this rule, uncomment (remove the leading "!" on the commands below)

! and replace "LOCAL_PASSWORD" with the value you have chosen.

! Do not use "LOCAL_PASSWORD". Instead, choose a value that is longer

! than seven characters, and contains upper- and lower-case letters,

! digits, and punctuation.

!

!username username1 password LOCAL_PASSWORD

! RULE: IOS - user password quality

!

! This fix is commented out because you have to supply a sensitive value.

! To apply this rule, uncomment (remove the leading "!" on the commands below)

! and replace "LOCAL_PASSWORD" with the value you have chosen.

! Do not use "LOCAL_PASSWORD". Instead, choose a value that is longer



! than seven characters, and contains upper- and lower-case letters,
! digits, and punctuation.

!

!username username1 password LOCAL_PASSWORD

! RULE: IOS - set syslog server
logging 13.14.15.16

! RULE: IOS - service timestamps debug
service timestamps debug datetime show-timezone msec

! RULE: IOS - ntp server 3
ntp server 9.10.11.12

! RULE: IOS - ntp server 2
ntp server 5.6.7.8

! RULE: IOS - ntp server
ntp server 1.2.3.4

! RULE: IOS - logging buffered
logging buffered 16000

! RULE: IOS - line password quality

!

! This fix is commented out because you have to supply a sensitive value.
! To apply this rule, uncomment (remove the leading "!" on the commands below)
! and replace "LINE_PASSWORD" with the value you have chosen.
! Do not use "LINE_PASSWORD". Instead, choose a value that is longer
! than seven characters, and contains upper- and lower-case letters,
! digits, and punctuation.

!

!line vty 5 15

!password LINE_PASSWORD



!exit

! RULE: IOS - line password quality

!

! This fix is commented out because you have to supply a sensitive value.

! To apply this rule, uncomment (remove the leading "!" on the commands below)

! and replace "LINE_PASSWORD" with the value you have chosen.

! Do not use "LINE_PASSWORD". Instead, choose a value that is longer

! than seven characters, and contains upper- and lower-case letters,

! digits, and punctuation.

!

!line vty 0 4

!password LINE_PASSWORD

!exit

! RULE: IOS - line password quality

!

! This fix is commented out because you have to supply a sensitive value.

! To apply this rule, uncomment (remove the leading "!" on the commands below)

! and replace "LINE_PASSWORD" with the value you have chosen.

! Do not use "LINE_PASSWORD". Instead, choose a value that is longer

! than seven characters, and contains upper- and lower-case letters,

! digits, and punctuation.

!

!line con 0

!password LINE_PASSWORD

!exit

! RULE: IOS - forbid clock summer-time - GMT

no clock summer-time

! RULE: IOS - clock timezone - GMT



clock timezone GMT 0

! Save running configuration so that it will be used each time
! the router is reset/powercycled. Only do this after you are
! SURE everything is correct
!
! copy running-config startup-config

Findings:

According to best practice there are a few minor changes to be considered for DML's router. These discrepancies constitute a **low** risk to DML.

First of all VTY (telnet) access to the router itself is not ACL'ed. It should be added in order to incorporate defense in depth but we have suggested limiting access via the remote tunnels for remote administration, which will limit telnet access as well.

RAT also suggested they are not using local authentication. However this is a false positive as local authentication is enabled on DML's router.

Of the user and password combinations it was discovered that two users have weak passwords. These two users passwords should be changed to be more complex making them harder to brute force. In addition it is recommended that they move to RADIUS authentication as opposed to local authentication to allow for more controlled password management following generally accepted best practice such as password aging, length, etc.

Also there is currently no syslog server defined. As a result there are no logs only the brief history in the buffers. The router should be configured to log to a syslog server allowing for log history to be maintained and parsed for signs of trouble.

It also was discovered that timestamps not being applied to debug information. This is a minor issue but should be addressed to make it easier to trouble shoot.

RAT also reports that NTP servers are not defined but again this appears to be a false positive as there are three NTP servers defined.



RAT also reports that logging to buffers is not set which also is a false positive as logging buffered is set to 4096.

It also was determined that the passwords for vty and console access are of poor quality. These passwords should be changed to something more complex to help prevent password guessing or brute force password attacks.

Finally according to best practice summertime Clock Setting should not be used and the time zone should be set to GMT. Both of these conditions are intended to prevent confusion over time differences when consolidating logs. However since all of DML's devices are located in the Newfoundland time zone and are set for Daylight savings time this is not really an issue for them.

4. Part #4 - Risk Assessment

4.1. Executive Summary

The purpose of the security assessment was to determine if the current level of security was sufficient now that DML has been awarded some high profile projects. The assessment was successful because it highlighted both the areas that were secured properly as well as the area that could be modified for additional security. It also took into account the level of risk presented by each deficiency to allow DML to prioritize which changes they wanted to tackle first from both a monetary aspect as well as risk reduction.

The assessment clearly demonstrated that while DML had taken reasonable precautions to secure their network, there are some places where improvements can be made. It also clearly demonstrated that security is an ongoing cycle and that work is required to maintain security just as much or more as the work required to initially secure the network. Many of the deficiencies are a result of changes since the network was originally configured as opposed to things that were not secured appropriately in the beginning. Also as DML has grown it makes sense now to take a fresh look at their architecture and determine if changes are required.

The deficiencies will be addressed in the following sections as well as recommendations on which changes should be made and in which priority.

4.2. Assessment Findings

Lets begin by looking at the items that were discovered that are categorized as high risk as these are the items that DML should try to mitigate first. Available funds and time should be exhausted on the items that cause the most concern and then work their way down through the list as far as possible until time and/or money is depleted or all risks have been mitigated.

The first item discovered that poses a high risk to DML is that telnet access is allowed to the outside interface of the router to permit an external consultant to perform remote management. This was discovered when nmap was used to scan the outside interface of the router for accessible ports as per Test Item 1. The following snippet from the nmap scan indicates that the telnet port is open: 23/tcp open telnet. While it is a business requirement for the security consultant to be able to manage the router remotely telnet is not a secure means of doing so. Telnet passes logon information in the clear so it may be possible to capture the traffic and determine the logon id and password. Also it may be possible to brute force access to the router since it is accessible from the Internet. If access to the router is gained via any means the game is over as the person with access to the router then has full access to the protected network and/or the ability to disrupt service to DML.

The next item that was discovered that poses a high risk to DML is that they have publicly accessible services in their Internal network as opposed to having them located in a DMZ or screened subnet. This was discovered during Test Item 2 when the Internal network was scanned using nmap to search for open ports. The following snippet from the nmap scan shows that there are in fact open ports in the internal network: 25/tcp open smtp. Open ports in the internal network if exploited will then provide access to other devices in the protected network. Basically if a service is exploited that resides in the protected network the attacker or malicious code is past the firewall and has full access to all other devices. Essentially they can then use the exploited device as a launching pad for attacks deeper into the network.

Finally there is a high risk to DML from the fact that the router is located in an insecure area. During Test Item 5 it was determined that the room the router is located in is a supply closet that is freely accessible. As a result the router could easily be damaged or destroyed through malicious or accidental means resulting in lost productivity from down time as well as financial loss to procure and configure a replacement router. Of even deeper concern is if someone has physical access to the router they can easily gain administrative access to it, which would give them full access to the protected network and/or the ability to cause service interruptions.

Now that we have covered off the most pressing issues we will move along to the only medium risk item. It was discovered through both a nmap scan of outbound traffic (Test Items 3) and a comparison of permitted traffic versus business requirements (Test item 9) that lack of documented security policy and procedures has lead to some unnecessary ports being accessible both inbound and outbound. The tests show that there are ports opened that are not required in order to achieve the desired results, ports opened that are no longer required as requirements have changed, and ports opened do to configuration

errors or lack of understanding of how some services actually work. Some examples of these are:

- 1) the fact that all internal machines are permitted to send mail (tcp 25) outbound when in reality it should only be the mail server that is permitted to send mail out, as all other devices should be sending mail to the mail server for delivery, as shown by this snippet of nmap scan: 25/tcp open smtp
- 2) the fact that telnet access is still permitted to an old IP address that use to be on the outside interface as shown by this snippet of ACL: access-list 125 permit tcp any host x.x.x.189 eq telnet;
- 3) and the fact that ftp-data (tcp 20) was permitted inbound to the ftp server even though it would not be required in order to grant outside users ftp access to the server as shown by this snippet of ACL: access-list 125 permit tcp any host x.x.x.196 eq ftp-data.

Allowing access to unnecessary services gives hackers and/or malicious code other services to try and exploit and other possible entry points into the network. Well documented procedures and policies would help prevent these kind of configuration issues by stipulating exactly what steps must be taken when a requirement changes, what exactly the corporate policy is in regards to a particular subject, and finally provide procedures for checking to insure things are as they should be.

Finally there were several low risk items uncovered which can be mitigated to reduce risk even more.

First of all the nmap scan of the router itself in test item 1 showed that lpd was open from anywhere even though the business requirement later showed it was only required from the partner network. By allowing access to tcp 515 from anywhere it allows people to use this as a potential vulnerability.

Next Test Item 3 used an nmap scan outbound to determine the egress filtering that was in place permitted 5 outbound ports that were not required. The following snippet from the nmap scan shows that SMTP was allowed out while it should only be the Exchange server that has the ability to send mail out: 25/tcp open smtp.

Finally RAT was used to compare the current router configuration with best practice in Test Item 10. This test turned up several discrepancies from best practice as demonstrated by the summary below:

Overall Score (0-10)

6.2

However all of the discrepancies constitute a low risk to DML. The items discovered by RAT that should be addressed were: no ACL for VTY access, two users had weak passwords, currently no logging server in place,

timestamps are not being applied to debug information, and finally both vty and console access have weak passwords.

Now that we have discussed the issues that should be addressed there were also many positives that came out of the assessment.

The first three tests which all relied on nmap scans to determine access to the router itself, access inbound, and access outbound all determined that considerable effort was taken to restrict access to what was required. Rules were in place to limit traffic in all directions to reduce the risk of unnecessary access.

Test Item 4, which was designed to insure that java was being stripped out of http code accessed via the Internet, tested successfully. As a result DML has removed any chance of malicious java code entering their network.

Results also determined that Stateful Inspection was enabled and functioning properly when Test Item 6 dropped a connection that tried to pass other traffic over the SMTP port.

In Test Item 7 Nessus was used to scan for any known exploits in the running software of the router. Again this test determined that the code was up to date and not vulnerable to any known exploits.

It also became clear from the interviews conducted with the Director of IT and CEO in Test Item 8 that considerable thought and effort has gone into understanding business requirements. This enables DML to restrict access as much as possible without impeding their ability to operate as normal.

Test Item 9 compared the existing ACL's to the business requirements as defined by the CEO and IT director. While this test showed some discrepancies it also showed that for the most part the ACL's were defined to limit access to that required to perform business functions.

Finally Test Item 10 used RAT to compare the router configuration to best practice. Again while this test turned up some discrepancies it clearly showed that the router was configured pretty close to the consensus on best practice.

Overall while there is room for improvement the current security stance of DML was found to be in pretty good shape.



4.3. Assessment Recommendations

The greatest risk currently facing DML is the fact that the current network layout does not incorporate the use of a DMZ to isolate publicly accessible services from the Internal network. Our first recommendation is the creation of a DMZ to house any devices that require public access such as a mail relay and the ftp servers. As it happens during the assessment we discovered that a small remote office in New Orleans was closed down and therefore a spare 1710 that use to be located in the New Orleans office to terminate the site-to-site VPN is available.

We recommend placing this 1710 in front of the existing 1710 so as its outside interface faces the ISP and the internal interface plugs into a switch which will create the new DMZ network segment. The existing 1710's outside interface will then plug into this new DMZ segment firewalling the internal network from the newly created DMZ. Since the 1710 from New Orleans is currently surplus equipment this allows DML to remove the risk of having publicly accessible devices inside the internal network at very little cost.

Once the DMZ is created the two ftp servers can be moved out to this new segment isolating them from the internal network. DML will require the purchase of another Exchange server so as it can be located in the DMZ as a front-end Exchange server allowing the current Exchange server to remain in the internal network functioning as a back-end Exchange server. This will allow the frond-end Exchange server to accept mail from the general public and relay the mail to the internal mail server as well as providing Outlook Web Access to DML's staff.

So for the relatively low costs of another Exchange license and some professional service fees to reconfigure both the 1710's they can isolate all services that are publicly accessible from the Internet to a separate network segment. By doing this they insure that if any of these devices are breached the internal network is still protected from them by the firewall.

This set-up will also allow the new 1710 to do the anti-spoofing filtering etc. removing that burden from the firewall. This is the one single item that can increase DML's security stance the most and ironically carries very little capital expenditure.

The next recommendation would be to relocate the supplies etc. out of the room that currently houses the servers, switches, and routers. This would allow for that room then to be locked and insure that there is no unauthorized access to this room and equipment. The other option is to divide the room in half adding a locked door between the half used to store supplies and the half housing the infrastructure equipment. Relocating the servers, routers, and

switches would not be feasible as the entire offices would have to be rewired as all cabling currently terminates in this supply closet.

It also would be beneficial to have the room environmentally controlled and monitored to protect against physical threats such as fire and flood. However the cost of constructing a data center room with raised floors, UPS, fire suppression, HVAC units, etc. is well out of reach of a company DML's size. Since the cost is prohibitive we recommend that DML makes sure it has adequate insurance to cover both the actual costs as well as lost revenue from service interruption in the case of such an event. This will allow DML to mitigate the risk of such an event without the huge expenditure to protect against it.

The third and final recommended change that absolutely must be performed is to change the process for remote administration. Since telnet is not secure and DML are currently already running IPSEC on their router it is recommended that immediately telnet access be blocked from the outside and the security consultant connect using the remote VPN client so as the session is encrypted. The recommended process for this would be to create another vpn group for individuals who need to have administrative access to the router. This group could be handed out a different IP pool then regular users so as vty access can also be acl'd to this pool only, providing defense in depth. Again the only cost to DML of implementing these changes is the professional services charges to make the changes on the firewall.

Once these three changes have been implemented DML should tackle the lack of formal written security policies and procedures. This is by far the most time consuming and costly endeavor that DML should undertake to improve their security stance. The lack of written procedures and policies has led to many of the issues that this assessment turned up.

A written policy and procedure would outline the proper steps to be taken for all circumstances as well as provide a means to audit the current position to make sure it is in agreement with the policy. It will take some time and effort as well as possible costs if they enlist consultants to assist with the documentation, but the documentation should pay for itself over time. Having this documentation at your fingertips would reduce the risk from the current medium rating to low and eliminate many of the vulnerabilities that occur from configuration errors, requirement changes, and/or misconceptions over what is required.

Next there are several minor changes that can be done to improve security as resources allow. These involve some changes to the way the business is currently operating to allow the functions to be performed in a more secure manner.



First it is recommended that all internal hosts use the internal DNS server for all lookups as opposed to the current situation of using the ISP's DNS servers. In order to accommodate this it is required to set-up a secondary DNS server to avoid lost productivity if there is an issue with a DNS server. This will allow the egress filter to be locked down tighter limiting tcp/udp 53 requests to the two internal DNS servers.

Similarly the egress filter also should be changed to only allow smtp access outbound from the mail server and ntp access only from the internal ntp servers. DML then should only allow internal devices to send mail via the corporate server and synch time to the internal ntp servers.

In addition the Ingress and Egress filters should be redefined removing all the discovered discrepancies so that the only access allowed is the current business requirements and the ACL's are as tightly defined as possible. In addition to correcting the ACL's now there has to be a procedure in place to insure they stay up to date.

Finally there are a couple of recommendations based on best practice that were discovered by RAT. These changes should be made as well but again the root cause stems back to the lack of policy and procedures and will rely on these policies and procedures being created in order to truly address these concerns.

First of all vty access is not acl'ed and while the ingress and egress filtering will limit telnet access to the device, the ports themselves also should have an acl to limit access. This is in line with defense in depth and will still protect the ports if the Ingress / Egress filters fail or are modified.

Also it was discovered that two users have weak passwords and it is recommended that these be changed to something more complex. However to truly get to the root cause of this issue it is recommended that DML move to RADIUS authentication as opposed to local to allow for strong password checking to be enforced. This will insure that best practice for passwords are followed such as requiring passwords to expire, meet complexity guidelines, etc.

Next it was determined that they are not currently logging to a syslog server. The router should be configured to log to a syslog server and again the security policies and procedures should define what has to be logged, how long logs are kept, how and when they are reviewed, etc. So while enabling logging will remove the deficiency it still needs the policies and procedures to get to the real issue.



The final deficiency from RAT was that the vty and console passwords were also weak. Again these passwords should be changed but DML should implement RADIUS authentication to get to the root cause of the problem, which is no mechanism to insure strong passwords.

These recommendations cover all the deficiencies that were determined in the assessment but as part of the policies and procedures to be implemented there should be a procedure and policy for future audits. This will insure that DML stays current and any discrepancies that turn up can be addressed in a timely manner. The one other thing that was noticed during the assessment was that while the router has built in IDS functionality it is not enabled. Since there is no cost to take advantage of this functionality in closing we would recommend that DML enable IDS on their router as well.

DML's security stance will be considerably improved if they put in place a project plan to implement the recommendations of this assessment. For a relatively small expenditure they can sleep easier at night knowing that they have taken reasonable precautions to protect their data. As they grow they should continue to redefine their security requirements to insure that they stay in line with the value of the assets being protected. The most important thing to remember is that security is a continuing battle that requires constant maintenance and care to keep it up to date.



References

- “Improving Security on Cisco Routers.” 13608. May 3, 2004. URL:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
- “Securing the Branch Office Network White Paper.” URL:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns346/ns382/net_value_proposition09186a00801c602f.html
- “Cisco IOS Firewall Data Sheet.” URL:
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_data_sheet09186a0080117962.html
- “White Paper: Cisco IOS Reference Guide.” 15169. May 4, 2004. URL:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a00801ab747.shtml
- “Output Interpreter.” URL:
<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>
- “Router Security Policy.” URL:
http://www.sans.org/resources/policies/Router_Security_Policy.pdf
- Naidu, Krishni. “Firewall Checklist 1.0.” URL:
<http://www.sans.org/score/firewallchecklist.php>
- “Ports to Block at the Firewall.” The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus. Version 4.0. October 8, 2003. URL: <http://www.sans.org/top20/ports>
- Antoine, Vanessa, Bongiorno, Raymond et. All. “Router Security Configuration Guide” Version 1.1b. December 5, 2003. URL:
http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf
- Spitzner, Lance. “Auditing your Firewall Setup.” March 26, 2000 URL:
<http://www.spitzner.net/audit.html>
- Akin, Thomas. Hardening Cisco Routers. Published by O'Reilly & Associates, Inc. 2002



Lundrigan, Russell, Steudier, Oliver, Allison, Jacques. Managing Cisco Network Security: Building Rock-Solid Networks. Syngress publishing Inc. 2000

Rudenko, Innokenty. Cisco Routers for IP Networking Black Book. The Coriolis Group. 2000

Cole, Eric, Fossen, Jasson, Northcutt, Stephen, Pomeranz, Hal. SANS Security Essentials Book 2 Defense in Depth. The SANS Institute. 2004

Hoelzer, David. Advanced System and Network Auditing Course Books. The SANS Institute. 2003

"SANS Glossary of Terms Used in Security and Intrusion Detection." May 2003.
URL: <http://www.sans.org/resources/glossary.php>



Appendixes

© SANS Institute 2004, Author retains full rights.



Appendix A- Config File from Audited Cisco 1710

Building configuration...

Current configuration : 16321 bytes

```
!  
! Last configuration change at 09:18:23 NDT Tue Jun 22 2004 by dweir  
! NVRAM config last updated at 09:18:41 NDT Tue Jun 22 2004 by dweir  
!  
version 12.3  
no parser cache  
service nagle  
no service pad  
service tcp-keepalives-in  
service timestamps debug uptime  
service timestamps log datetime msec show-timezone  
service password-encryption  
!  
hostname DML_ENG  
!  
logging buffered 4096 debugging  
logging console critical  
enable secret 5 $1$67JKN567MK2R7WMnAitNH6HslOLt.  
!  
username sfinn password 7 020SCRAMBLED41F151C  
username dweir password 7 000307SCRAMBLED818  
username tshoot password 7 09SCRAMBLED80B1E11595D547B79747860  
username adillon password 7 0828414A5B4855SCRAMBLEDC57  
username rmcdonald password 7 110BSCRAMBLED103F39217A62657341574650  
username mbrocklehurst password 7 08324SCRAMBLED65C567B7A76786366  
username dhatcher password 7 13111800040210SCRAMBLED7724354  
username jstinson password 7 0SCRAMBLED49574643595C5479  
username bpenney password 7 094747071E16SCRAMBLED7B747B  
username amahon password 7 141SCRAMBLED387B76796267724354  
username testing password 7 08711A1E504SCRAMBLED13C2436  
username rrice password 7 15SCRAMBLED67D717C67742818  
username gbennett password 7 000E06080SCRAMBLED4645  
username kjenkins password 7 011SCRAMBLED3555B604A5A  
username ochaytor password 7 11031D00144ASCRAMBLED33E  
memory-size iomem 15  
clock timezone NST -3 30  
clock summer-time NDT recurring  
aaa new-model  
!  
!  
aaa authentication login default local  
aaa authentication login userauthen local  
aaa authentication enable default enable  
aaa authorization network groupauthen local  
aaa session-id common  
ip subnet-zero  
no ip source-route  
!  
!
```



```
ip name-server x.x.x.x
ip name-server x.x.x.x
!
no ip bootp server
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 3600
ip inspect name myfw tcp timeout 3600
ip inspect name myfw http java-list 51 urlfilter timeout 3600
ip urlfilter max-request 500
ip urlfilter max-resp-pak 150
ip urlfilter allow-mode on
ip urlfilter cache 4500
ip urlfilter audit-trail
ip urlfilter urlf-server-log
ip urlfilter server vendor websense 10.0.0.102
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
!
crypto isakmp policy 3
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp policy 10
  authentication pre-share
  group 2
crypto isakmp key cryptokey1 address x.x.x.x no-xauth
crypto isakmp key cryptokey2 address x.x.x.x no-xauth
!
crypto isakmp client configuration group dlmclientvpn
  key cryptokey3
  pool remotepool
  acl 160
!
!
crypto ipsec transform-set dave esp-des esp-sha-hmac
crypto ipsec transform-set remote esp-3des esp-md5-hmac
!
crypto dynamic-map dyna 90
```



```
set transform-set remote
!
!
crypto map stjgan client authentication list userauth
crypto map stjgan isakmp authorization list groupauthor
crypto map stjgan client configuration address respond
crypto map stjgan 10 ipsec-isakmp
set peer 192.75.14.118
set transform-set dave
match address 181
crypto map stjgan 50 ipsec-isakmp
set peer 64.132.30.131
set transform-set dave
match address 190
crypto map stjgan 90 ipsec-isakmp dynamic dyna
!
!
!
interface Ethernet0
description LAN
ip address x.x.x.x 255.255.255.240
ip access-group 122 in
no ip proxy-arp
ip nat inside
no ip route-cache
no ip mroute-cache
half-duplex
no cdp enable
hold-queue 32 in
!
interface FastEthernet0
description Internet
ip address x.x.x.x 255.255.255.252
ip access-group 125 in
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat outside
ip inspect myfw out
no ip route-cache
no ip mroute-cache
speed 10
half-duplex
no cdp enable
crypto map stjgan
!
ip local pool remotepool 192.168.60.100 192.168.60.200
ip nat inside source route-map nonat interface FastEthernet0 overload
ip nat inside source static tcp 10.0.0.244 515 interface FastEthernet0 515
ip nat inside source static tcp 10.0.0.244 9100 interface FastEthernet0 9100
ip classless
ip route 0.0.0.0 0.0.0.0 x.x.x.x
ip route 10.0.0.0 255.255.255.0 x.x.x.x
```



```
ip route 10.1.1.0 255.255.255.0 x.x.x.x
ip route 10.1.2.0 255.255.255.0 x.x.x.x
ip route x.x.x.x 255.255.255.255 x.x.x.x
no ip http server
no ip http secure-server
!
!
access-list 51 permit 134.153.184.170
access-list 51 permit 134.153.184.154
access-list 51 permit 128.255.27.53
access-list 51 permit 134.153.184.5
access-list 51 permit 198.165.33.245
access-list 51 permit 209.184.81.223
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq ftp
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq telnet
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq smtp
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq domain
access-list 122 permit udp x.x.x.192 0.0.0.15 any eq domain
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq www
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq pop3
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq nntp
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq 123
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq 443
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq 8000
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq 8080
access-list 122 permit ip x.x.x.192 0.0.0.15 x.x.x.0 0.0.0.255
access-list 122 permit ip x.x.x.192 0.0.0.15 192.168.60.0 0.0.0.255
access-list 122 permit ip x.x.x.192 0.0.0.15 192.168.80.0 0.0.0.255
access-list 122 permit ip x.x.x.192 0.0.0.15 192.168.90.0 0.0.0.255
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq ftp
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq smtp
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq domain
access-list 122 permit udp 10.0.0.0 0.0.0.255 any eq domain
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq www
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq pop3
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq nntp
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq 123
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq 443
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq 8000
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq 8080
access-list 122 permit tcp 10.0.0.0 0.0.0.255 host x.x.x.83 eq telnet
access-list 122 permit ip 10.0.0.0 0.0.0.255 192.168.60.0 0.0.0.255
access-list 122 permit ip 10.0.0.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 122 permit ip 10.0.0.0 0.0.0.255 192.168.90.0 0.0.0.255
access-list 122 permit tcp host x.x.x.196 any eq ftp-data
access-list 122 permit tcp host x.x.x.196 any gt 1023
access-list 122 permit udp host x.x.x.196 any gt 1023
access-list 122 permit esp any any
access-list 122 permit tcp x.x.x.192 0.0.0.15 host x.x.x.193
access-list 122 permit ip x.x.x.192 0.0.0.15 10.0.0.0 0.0.0.255
access-list 122 permit ip 10.0.0.0 0.0.0.255 x.x.x.0 0.0.0.255
access-list 122 permit tcp 10.0.0.0 0.0.0.255 host x.x.x.100 eq 1723
access-list 122 permit gre 10.0.0.0 0.0.0.255 host x.x.x.100
access-list 122 permit tcp x.x.x.192 0.0.0.15 host x.x.x.100 eq 1723
```



```
access-list 122 permit gre x.x.x.192 0.0.0.15 host x.x.x.100
access-list 122 permit tcp 10.0.0.0 0.0.0.255 host x.x.x.223 eq 1723
access-list 122 permit gre host x.x.x.198 host x.x.x.223
access-list 122 permit ip 10.0.0.0 0.0.0.255 x.x.x.192 0.0.0.15
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq 1755
access-list 122 permit udp 10.0.0.0 0.0.0.255 any eq 1755
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq 1755
access-list 122 permit udp x.x.x.192 0.0.0.15 any eq 1755
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq 554
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq 8554
access-list 122 permit tcp 10.0.0.0 0.0.0.255 any eq 1720
access-list 122 permit udp 10.0.0.0 0.0.0.255 any gt 1024
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq 554
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq 8554
access-list 122 permit tcp x.x.x.192 0.0.0.15 any eq 1720
access-list 122 permit udp x.x.x.192 0.0.0.15 any gt 1024
access-list 122 permit ip host 10.0.0.27 host x.x.x.223
access-list 122 permit udp host x.x.x.203 host x.x.x.223 eq isakmp
access-list 122 permit udp host x.x.x.199 host x.x.x.223 eq isakmp
access-list 122 permit tcp host x.x.x.199 host x.x.x.223 eq 1723
access-list 122 permit gre host x.x.x.199 host x.x.x.223
access-list 122 permit tcp host x.x.x.203 host x.x.x.120 eq 1723
access-list 122 permit gre host x.x.x.203 host x.x.x.120
access-list 122 permit tcp host x.x.x.206 host x.x.x.120 eq 1723
access-list 122 permit gre host x.x.x.206 host x.x.x.120
access-list 122 permit tcp host 10.0.0.27 host x.x.x.120 eq 1723
access-list 122 permit gre host 10.0.0.27 host x.x.x.120
access-list 122 permit tcp host 10.0.0.28 host x.x.x.120 eq 1723
access-list 122 permit gre host 10.0.0.28 host x.x.x.120
access-list 122 permit ip host 10.0.0.244 any
access-list 122 permit tcp host x.x.x.195 any eq ftp-data
access-list 122 permit tcp host x.x.x.195 any gt 1023
access-list 122 permit udp host x.x.x.195 any gt 1023
access-list 122 permit ip host 10.0.0.44 host x.x.x.118
access-list 122 permit ip 10.0.0.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 122 permit ip 10.0.0.0 0.0.0.255 10.1.2.0 0.0.0.255
access-list 122 permit tcp host x.x.x.204 any eq ftp-data
access-list 122 permit tcp host x.x.x.204 any gt 1023
access-list 122 permit udp host x.x.x.204 any gt 1023
access-list 122 permit tcp 10.0.0.0 0.0.0.255 host x.x.x.50 eq 554
access-list 122 permit udp 10.0.0.0 0.0.0.255 host x.x.x.50 eq 554
access-list 122 permit tcp 10.0.0.0 0.0.0.255 host x.x.x.50 eq 5078
access-list 122 permit udp 10.0.0.0 0.0.0.255 host x.x.x.50 eq 5078
access-list 122 permit ip x.x.x.192 0.0.0.15 host x.x.x.211
access-list 122 permit ip 10.0.0.0 0.0.0.255 host x.x.x.211
access-list 122 permit udp host x.x.x.196 host x.x.x.41 eq ntp
access-list 122 permit udp host x.x.x.195 host x.x.x.41 eq ntp
access-list 122 permit udp host 10.0.0.45 host x.x.x.41 eq ntp
access-list 125 permit tcp any host x.x.x.189 eq telnet
access-list 125 permit tcp host x.x.x.65 eq domain host x.x.x.196
access-list 125 permit tcp host x.x.x.129 eq domain host x.x.x.196
access-list 125 permit udp host x.x.x.65 eq domain host x.x.x.196
access-list 125 permit udp host x.x.x.129 eq domain host x.x.x.196
access-list 125 permit ip 192.168.60.0 0.0.0.255 x.x.x.192 0.0.0.15
```



```
access-list 125 permit ip 192.168.60.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 125 permit ip 192.168.80.0 0.0.0.255 x.x.x.192 0.0.0.15
access-list 125 permit ip 192.168.80.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 125 permit ip 192.168.90.0 0.0.0.255 x.x.x.192 0.0.0.15
access-list 125 permit ip 192.168.90.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 125 permit tcp x.x.x.0 0.0.0.255 x.x.x.192 0.0.0.15 range 6000 7000
access-list 125 permit udp x.x.x.0 0.0.0.255 x.x.x.192 0.0.0.15 range 6000 7000
access-list 125 permit tcp any host x.x.x.196 eq ftp-data
access-list 125 permit tcp any host x.x.x.196 eq ftp
access-list 125 permit tcp any host x.x.x.196 eq smtp
access-list 125 permit tcp any host x.x.x.196 eq www
access-list 125 permit tcp any host x.x.x.196 eq pop3
access-list 125 permit tcp any host x.x.x.196 eq 123
access-list 125 permit tcp any host x.x.x.196 eq 443
access-list 125 permit udp any any eq isakmp
access-list 125 permit gre any any
access-list 125 permit tcp x.x.x.0 0.0.0.255 x.x.x.192 0.0.0.15 range 3000 3999
access-list 125 permit ip host x.x.x.50 host x.x.x.197
access-list 125 permit ip 192.168.130.0 0.0.0.255 x.x.x.192 0.0.0.15
access-list 125 permit ip 192.168.130.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 125 permit tcp any host x.x.x.78 eq telnet
access-list 125 permit ip host x.x.x.223 host 10.0.0.27
access-list 125 permit tcp host x.x.x.50 host x.x.x.78 eq lpd
access-list 125 permit tcp host x.x.x.50 host x.x.x.78 eq 9100
access-list 125 permit tcp any host x.x.x.78 eq lpd
access-list 125 permit tcp any host x.x.x.195 eq 443
access-list 125 permit tcp any host x.x.x.195 eq www
access-list 125 permit tcp any host x.x.x.195 eq smtp
access-list 125 permit ip host x.x.x.118 host 10.0.0.102
access-list 125 permit ip 10.1.1.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 125 permit ip 10.1.2.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 125 permit ip x.x.x.0 0.0.0.255 10.0.0.0 0.0.0.255
access-list 125 permit udp any host x.x.x.78 eq isakmp
access-list 125 permit esp any host x.x.x.78
access-list 125 permit udp any host x.x.x.78 eq non500-isakmp
access-list 125 permit tcp any host x.x.x.204 eq ftp
access-list 125 permit tcp any host x.x.x.204 eq ftp-data
access-list 125 permit udp host x.x.x.41 host x.x.x.78 eq ntp
access-list 125 permit tcp host x.x.x.245 host x.x.x.196 eq 1433
access-list 125 permit udp host x.x.x.2 eq ntp host x.x.x.78
access-list 125 permit udp host x.x.x.252 eq ntp host x.x.x.78
access-list 125 permit udp host x.x.x.53 eq ntp host x.x.x.78
access-list 130 deny ip 10.0.0.0 0.0.0.255 192.168.60.0 0.0.0.255
access-list 130 deny ip 10.0.0.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 130 deny ip 10.0.0.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 130 deny ip 10.0.0.0 0.0.0.255 10.1.2.0 0.0.0.255
access-list 130 deny ip host 10.0.0.44 host x.x.x.118
access-list 130 deny ip 10.0.0.0 0.0.0.255 192.168.90.0 0.0.0.255
access-list 130 deny ip x.x.x.192 0.0.0.15 any
access-list 130 permit ip 10.0.0.0 0.0.0.255 any
access-list 140 permit ip 10.0.0.0 0.0.0.255 x.x.x.0 0.0.0.255
access-list 160 permit ip x.x.x.192 0.0.0.15 192.168.60.0 0.0.0.255
access-list 160 permit ip 10.0.0.0 0.0.0.255 192.168.60.0 0.0.0.255
access-list 180 permit ip x.x.x.192 0.0.0.15 192.168.80.0 0.0.0.255
```



```
access-list 180 permit ip 10.0.0.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 180 permit ip host 10.0.0.102 host x.x.x.118
access-list 180 permit ip 10.0.0.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 180 permit ip 10.0.0.0 0.0.0.255 10.1.2.0 0.0.0.255
access-list 180 permit ip 10.0.0.0 0.0.0.255 x.x.x.0 0.0.0.255
access-list 181 permit ip x.x.x.192 0.0.0.15 192.168.80.0 0.0.0.255
access-list 181 permit ip 10.0.0.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 181 permit ip host 10.0.0.102 host x.x.x.118
access-list 181 permit ip 10.0.0.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 181 permit ip 10.0.0.0 0.0.0.255 10.1.2.0 0.0.0.255
access-list 190 permit ip x.x.x.192 0.0.0.15 192.168.90.0 0.0.0.255
access-list 190 permit ip 10.0.0.0 0.0.0.255 192.168.90.0 0.0.0.255
no cdp run
!
route-map imd permit 10
  match ip address 140
  set ip next-hop 192.168.80.1
!
route-map nonat permit 10
  match ip address 130
!
radius-server authorization permit missing Service-Type
banner motd ^CCCCCCCCCCCC
-----
STOP: Authorized access only!
-----
```

This system is available only to authorized personnel of DML Engineering
Please disconnect immediately unless you have been specifically authorized to
connect to this terminal by DML Engineering

```
All connection attempts are logged
^C
!
line con 0
  exec-timeout 5 0
  password 7 070SCRAMBLEDA1A0A
  stopbits 1
line aux 0
  exec-timeout 5 0
  password 7 12370ASCRAMBLEDD24362C
  no exec
line vty 0 4
  exec-timeout 5 0
  password 7 0SCRAMBLED585D1A
  transport input telnet
line vty 5 15
  exec-timeout 5 0
  password 7 07083SCRAMBLED0A
  transport input telnet
!
scheduler max-task-time 5000
ntp clock-period 17168902
ntp server 192.5.41.41
```

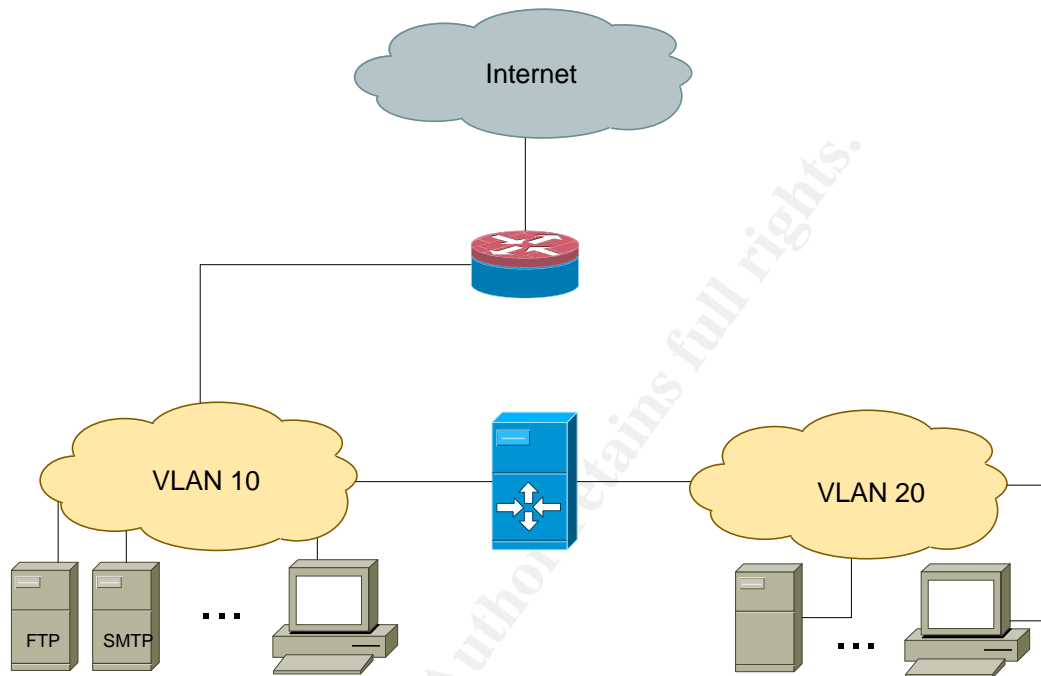


```
ntp server 136.159.2.2  
ntp server 128.100.103.252  
ntp server 209.87.233.53  
!  
end
```

© SANS Institute 2004, Author retains full rights.



Appendix B- Network Diagram DML Engineering (Current)



Appendix C- Recommended Network Design for DML Engineering

