

Center for Internet Security Gold Standard Benchmark for Cisco IOS

Level 1 and 2 Benchmarks
Version 2.1

<http://www.cisecurity.org>
rat-feedback@cisecurity.org

September 2, 2003

Abstract

This document defines a set of benchmarks or standards for securing Cisco IOS routers. The benchmark is an industry consensus of current best practices. It lists actions to be taken as well as reasons for those actions. It is intended to provide step-by-step guidance to front line system and network administrators. It may be used manually by itself or in conjunction with automated scoring tools.

Agreed Terms of Use

Background

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere (“Products”) as a public service to Internet users worldwide. Recommendations contained in the Products (“Recommendations”) result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a “quick fix” for anyone’s information security needs.

No representations, warranties and covenants

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations “as is” and “as available” without representations, warranties or covenants of any kind.

User agreements

By using the Products and/or the Recommendations, I and/or my organization (“we”) agree and acknowledge that:

1. No network, system, device, hardware, software or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS’s negligence or failure to perform;
4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at its sole option to do so; and
6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;
2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled “Grant of limited rights.”

Subject to the paragraph entitled “Special Rules” (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations (“CIS Parties” harmless from and against any and all liability, losses, costs and expenses (including attorneys’ fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS’s right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (<http://nsa2.www.conxion.com/cisco/notice.htm>).

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member’s own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing

grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Contents

1 Introduction	iii
1.1 How To Get Started Now	iii
1.2 Using This Document	iv
2 Audit Checklist	1
2.1 Level-1	1
2.2 Level-2	3
3 The Level-1 Benchmark	6
3.1 Actions	6
3.2 Supporting Documentation	18
4 The Level-2 Benchmark	29
4.1 Actions	29
4.2 Supporting Documentation	38
A Other Information	45
A.1 How Benchmark Items Are Determined	45
A.2 Understanding Technology, Risks and Your Organizational Goals	45
A.3 Scoring and Scoring Tools	45
A.4 Credits	46
B Example Configuration	47

1 Introduction

1.1 How To Get Started Now

There are three ways to use this benchmark:

1. Dive in

If you are well-versed in Cisco IOS, and fit the other assumptions listed in the next section, and you are a highly skilled security professional confident in your knowledge of the functional/performance consequences of implementing the actions, then you may proceed directly to sections 3.1 and 4.1.

2. Slow and steady

All others are strongly urged to complete the Audit Checklist in Section 2 and study the warnings and explanations in sections 3.2 and 4.2 before implementing any of the actions in sections 3.1 and 4.1. Many security actions can disable or otherwise interfere with the function or performance of software on your system, particularly applications. Note also that many of the actions in sections 3.1 and 4.1 are conditional. They only apply in certain situations.

3. Use a scoring tool

The third option is to use a scoring tool. See section A.3 for availability.

1.2 Using This Document

1.2.1 Read This First

Read this section in its entirety. It tells you how to get started quickly using the benchmark to improve the security of your systems. It lists important information and assumptions. Failure to read this section could result in incomplete or incorrect application of the recommendations.

1.2.2 Prerequisites

This benchmark does not assume that any other benchmarks have been previously applied.

1.2.3 Assumptions About The System Environment

This benchmark assumes that you are running IOS 11 or later.

1.2.4 Assumptions About The Reader

This benchmark assumes that the person applying the recommendations

- May or may not be an IOS/network expert.
- Is able to log in to the router and enable.
- Is able to enter basic IOS commands.
- Understands the business critical functions of the routers being secured.
- Understands local policies.
- Is capable of evaluating the potential impact of recommended changes on both function and policy.

1.2.5 Benchmark Format

The body of this document consists of the “Audit Checklist” followed by the level-1 and level-2 benchmarks. Each benchmark is divided into “Actions” and “Supporting Documentation.”

The “Audit Checklist” lays out the rough structure of the benchmarks, and includes questions about specific configuration choices and settings that must be answered each time a router is audited to judge a router’s compliance with the benchmarks. If you are following the “Slow and Steady” approach to using this benchmark, you should read over the checklist carefully and record the expected answers for the questions.

As a convenience an “Expanded Audit Checklist” is available at <http://www.cisecurity.org/> If you intend to audit more than one router or intend to audit the same device several times, you are encouraged to print and copy this document.

The “Actions” section is intended to contain the minimum information necessary to allow you to implement the recommendations quickly. Each item will contain a brief description of the action to be taken, a list of the OS versions and contexts in which the action applies, a list of the information needed to complete the action (the “question”), and the action to be taken.

The “Supporting Documentation” section contains, for each item, a corresponding description, a “Security Impact” section describing the reason for the action, an “Importance” value reflecting the importance of the item on a 1-10 scale as assigned by the CIS consensus process, and a “For more information” section listing references to further information.

See A.1 for information on how levels are determined.

1.2.6 Special Notation

This benchmark uses the following typographical conventions.

- The **Action** section of each audit rule shows IOS commands you can use to configure IOS in compliance with the rule. The IOS prompts have been included in the command listing to give context.
- Router commands are shown in typewriter font, for example: `router(config)# aaa new-model`.
- Long router commands are wrapped so that words do not get broken on line boundaries. This is a little different from how the Cisco IOS command interface looks on a typical display. Be careful to check for wrapped lines when copying commands from this benchmark.
- Some fields and arguments to router commands must be filled in with values from the Audit Checklist (Section 2). These are shown as variables in uppercase italics, for example: `no access-list $(VTY_ACL_NUMBER)`. In these cases, you should replace the variable with the value you filled in on the Audit Checklist.
- Other fields, in which the fix script contains the word “INSTANCE” in italics, indicate that the fix must be applied one or more instances of interfaces, lines, etc. For example: `interface INSTANCE` indicates that the rule must be applied to all interfaces that match the rules conditions, such as `Ethernet0`, `Ethernet1`, etc. You will have to fill in the correct instance values to use the command.
- In the supporting documentation section you will see references that look like this: “RSCG Page 140”. These are pointers to specific pages in the Router Security Configuration Guide [1] where more details relevant to the rule may be found.

2 Audit Checklist

2.1 Level-1

- Check rules and data related to system management? (3.1.1) YES
- Use local authentication? (3.1.2) (YES/no)
- Create new AAA model using local usernames and passwords? (3.1.3) YES
- Create local usernames? (3.1.4) YES
- Username of user for local authentication? (3.1.5)(username1/_____)
- Apply standard SNMP checks? (3.1.6) YES
- Disable SNMP server? (3.1.7)(YES/no)
- Forbid SNMP read-write? (3.1.8)(YES/no)
- Forbid SNMP community string 'public'? (3.1.9) YES
- Forbid SNMP community string 'private'? (3.1.10) YES
- Require an ACL to be applied for all SNMP access? (3.1.11) (yes/NO)
- Specify ACL number to be used for filtering SNMP requests? (3.1.12) (99/_____)
- Define SNMP ACL? (3.1.13)(yes/NO)
- Address block and mask for SNMP access? (3.1.14) .. (192.168.1.0 0.0.0.255/_____)
- Apply standard checks to control access to the router? (3.1.15) (YES/no)
- Allow Telnet access for remote administration? (3.1.16) (YES/no)
- Allow only telnet access for remote login? (3.1.17) YES
- Specify maximum allowed exec timeout? (3.1.18) YES
- Exec timeout value? (3.1.19)(10 0/_____)
- Disable the aux port? (3.1.20) (YES/no)
- Use default AAA login authentication on each line? (3.1.21) (YES/no)
- Use explicit named AAA login authentication on each line? (3.1.22) (yes/NO)
- Name for login AAA list? (3.1.23) (default/_____)
- require line passwords? (3.1.24) (YES/no)
- Require an enable secret? (3.1.25) YES
- Check line password quality? (3.1.26) (YES/no)
- Check user password quality? (3.1.27) (YES/no)

- Require VTU ACL to be applied? (3.1.28) YES
- Specify ACL number to be used for telnet or ssh? (3.1.29)(182/_____)
- Define simple (one netblock + one host) VTU ACL? (3.1.30)(YES/no)
- Address block and mask for administrative hosts? (3.1.31) (192.168.1.0
 0.0.0.255/_____)
- Address for administrative host? (3.1.32) (192.168.1.254/_____)
- Disable unneeded management services? (3.1.33) (YES/no)
- Forbid finger service (on IOS 11)? (3.1.34) YES
- Forbid identd service (on IOS 11)? (3.1.35) YES
- Forbid finger service (on IOS 12)? (3.1.36) YES
- Forbid finger service (on IOS 12)? (3.1.37) YES
- Forbid http service? (3.1.38) YES
- Encrypt passwords in the configuration? (3.1.39) YES
- Check rules and data related to system control? (3.1.40) YES
- Synchronize router time via NTP? (3.1.41) (YES/no)
- Designate an NTP time server? (3.1.42) YES
- Address of first NTP server? (3.1.43) (1.2.3.4/_____)
- Designate a second NTP time server? (3.1.44) (YES/no)
- Address of second NTP server? (3.1.45) (5.6.7.8/_____)
- Designate a third NTP time server? (3.1.46) (YES/no)
- Address of third NTP server? (3.1.47)(9.10.11.12/_____)
- Apply standard logging rules? (3.1.48) (YES/no)
- Use GMT for logging instead of localtime? (3.1.49) (YES/no)
- Check timezone and offset? (3.1.50) YES
- Forbid summertime clock changes? (3.1.51) YES
- Timestamp log messages? (3.1.52) YES
- Timestamp debug messages? (3.1.53) YES
- enable logging? (3.1.54) YES
- Designate syslog server? (3.1.55) YES

- Address of syslog server? (3.1.56)(13.14.15.16/_____)
- Designate local logging buffer size? (3.1.57) YES
- Local log buffer size? (3.1.58)(16000/_____)
- Require console logging of critical messages? (3.1.59) YES
- Require remote logging of level info or higher? (3.1.60) YES
- Disable unneeded control services? (3.1.61) (YES/no)
- Forbid small TCP services (on IOS 11)? (3.1.62) YES
- Forbid small UDP services (on IOS 11)? (3.1.63) YES
- Forbid small TCP services (on IOS 12)? (3.1.64) YES
- Forbid small UDP services (on IOS 12)? (3.1.65) YES
- Forbid bootp service? (3.1.66) YES
- Disable CDP service? (3.1.67) (YES/no)
- Forbid config service? (3.1.68) (YES/no)
- Use tcp-keepalive-in service to kill stale connections? (3.1.69) YES
- Forbid tftp service? (3.1.70) (YES/no)
- Check rules and data related to data flow? (3.1.71) YES
- Apply standard routing protections? (3.1.72) (YES/no)
- Forbid directed broadcasts (on IOS 11)? (3.1.73) YES
- Forbid directed broadcasts (on IOS 12)? (3.1.74) YES
- Forbid IP source routing? (3.1.75) YES

2.2 Level-2

- Check rules and data related to system management? (4.1.1)(yes/NO)
- Use TACACS Plus authentication? (4.1.2) (yes/NO)
- Create emergency account? (4.1.3) YES
- Check for AAA new-model? (4.1.4) (yes/NO)
- Require tacacs authentication for login? (4.1.5) (yes/NO)
- Require tacacs authentication for enable? (4.1.6) (yes/NO)

- Check for aaa accounting for exec? (4.1.7)(yes/NO)
- Check for aaa accounting for commands? (4.1.8)(yes/NO)
- Check for aaa accounting for network events? (4.1.9)(yes/NO)
- Check for aaa accounting for connections? (4.1.10)(yes/NO)
- Check for aaa accounting for system events? (4.1.11)(yes/NO)
- Use loopback address as source for TACACS? (4.1.12) (yes/NO)
- What is the local loopback interface number? (4.1.13)(0/_____)
- Check the existence of the defined loopback interface? (4.1.14)(yes/NO)
- What is the local loopback address? (4.1.15) (192.168.1.3/_____)
- Apply level 2 checks to control access to the router? (4.1.16) YES
- Require use of SSH for remote administration? (4.1.17) (YES/no)
- Check for SSH transport only on VTYs? (4.1.18) (YES/no)
- Require VTY ACL to be applied? (4.1.19) YES
- Define VTY ACL? (4.1.20) (YES/no)
- Check rules and data related to system control? (4.1.21)(yes/NO)
- Apply non-standard logging rules? (4.1.22)(YES/no)
- Use localtime for logging instead of GMT? (4.1.23) (yes/NO)
- Local timezone name? (4.1.24) (GMT/_____)
- Local timezone offset from GMT? (4.1.25)(0/_____)
- Check timezone and offset? (4.1.26) (yes/NO)
- Require summertime clock changes? (4.1.27)(yes/NO)
- Apply loopback checks? (4.1.28) (yes/NO)
- Use primary loopback as source address for NTP? (4.1.29)(yes/NO)
- Forbid all non-standard loopbacks? (4.1.30) (yes/NO)
- Use loopback for tftp source interface? (4.1.31) (yes/NO)
- Disable unneeded services? (4.1.32) (yes/NO)
- Check rules and data related to data flow? (4.1.33)(yes/NO)
- Apply border router filtering rules? (4.1.34)(yes/NO)
- What is the primary external interface? (4.1.35)(Ethernet0/_____)

- Does this border router have a second external interface? (4.1.36)(yes/NO)
- What is the secondary external interface? (4.1.37)(Ethernet1/_____)
- Apply ingress filter to second external interface? (4.1.38) (yes/NO)
- What ACL number (100-199) should be used for ingress filtering? (4.1.39)
(180/_____)
- Apply egress filter to second external interface? (4.1.40)(yes/NO)
- What ACL number (100-199) should be used for egress filtering? (4.1.41)
(181/_____)
- Test for existence of 2nd external interface? (4.1.42)(yes/NO)
- Define egress filter? (4.1.43) (yes/NO)
- What is the the internal netblock and mask? (4.1.44) .. (192.168.1.0 0.0.0.255/_____)
- Apply ingress filter to external interface? (4.1.45) (yes/NO)
- Define ingress filter? (4.1.46)(yes/NO)
- Apply egress filter to first external interface? (4.1.47)(yes/NO)
- Test for existence of external interface? (4.1.48)(yes/NO)
- Apply extra routing protections? (4.1.49) (yes/NO)
- Use Unicast RPF for filtering? (4.1.50)(yes/NO)
- Forbid proxy arp? (4.1.52)(YES/no)
- Forbid tunnel interfaces? (4.1.53)(yes/NO)

3 The Level-1 Benchmark

3.1 Actions

3.1.1 Management Plane Level 1

Description Services, settings, and data streams related to setting up and examining the static configuration of the router, and the authentication and authorization of router administrators. Examples of management plane services include: administrative telnet or ssh, SNMP, TFTP for image file upload, and security protocols like RADIUS and TACACS+.

3.1.2 Local AAA Rules

Description Rules in the Local AAA Rules Configuration class implement local authentication. Only one set of authentication rules (local, TACACS+) may be selected.

3.1.3 IOS - Use local authentication

Description Establish a new authentication model that requires local login
Applicability 10.0+ IOSGlobal configuration mode
Rule Type Management Plane Level 1⇒Local AAA Rules
Documentation See section 3.2.1.
Action

```
router(config)# aaa new-model
router(config)# aaa authentication login $(AAA_LIST_NAME) local
router(config)# aaa authentication enable default enable
```

3.1.4 IOS - Create local users

Description Create at least one local user with password.
Applicability 10.0+ IOSGlobal configuration mode
Rule Type Management Plane Level 1⇒Local AAA Rules
Documentation See section 3.2.2.
Action

```
!
! 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".
!
!router(config)# username $(LOCAL_USERNAME) password LOCAL_PASSWORD
```

3.1.5 LOCAL_USERNAME

Info Needed Username for local authentication.
Default Value username1
How To Obtain Choose a local username

3.1.6 SNMP Rules

Description Disable SNMP and check for common mis-configurations.

3.1.7 IOS - no snmp-server

Description	Disable SNMP if not in use.
Applicability	10.0+ IOSGlobal configuration mode
Rule Type	Management Plane Level 1⇒SNMP Rules
Documentation	See section 3.2.3.
Action	<code>router(config)# no snmp-server</code>

3.1.8 IOS - forbid SNMP read-write

Description	Forbid SNMP read-write community strings.
Applicability	11+ IOSSNMPCommunity
Rule Type	Management Plane Level 1⇒SNMP Rules
Documentation	See section 3.2.4.
Action	<code>router(config)# no snmp-server community INSTANCE</code>

3.1.9 IOS - forbid SNMP community public

Description	Don't use default SNMP community strings.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 1⇒SNMP Rules
Documentation	See section 3.2.5.
Action	<code>router(config)# no snmp-server community public</code>

3.1.10 IOS - forbid SNMP community private

Description	Don't use default SNMP community strings.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 1⇒SNMP Rules
Documentation	See section 3.2.6.
Action	<code>router(config)# no snmp-server community private</code>

3.1.11 IOS - forbid SNMP without ACLs

Description	Require SNMP to use ACLs.
Applicability	11+ IOSSNMPCommunity
Rule Type	Management Plane Level 1⇒SNMP Rules
Documentation	See section 3.2.7.
Action	<code>router(config)# no snmp-server community INSTANCE</code>

3.1.12 SNMP_ACL_NUMBER

Info Needed	The number of the IP access list used to protect the SNMP access.
Default Value	99
How To Obtain	Choose an ACL number between 1 and 99

3.1.13 IOS - Define SNMP ACL

Description	Define SNMP ACL.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 1⇒SNMP Rules
Documentation	See section 3.2.8.
Action	<pre>router(config)# access-list \$(SNMP_ACL_NUMBER) permit \$(SNMP_ACL_BLOCK_WITH_MASK) router(config)# access-list \$(SNMP_ACL_NUMBER) deny any log</pre>

3.1.14 SNMP_ACL_BLOCK_WITH_MASK

Info Needed	The IP address and netmask for the hosts permitted to connect via SNMP.
Default Value	192.168.1.0 0.0.0.255
How To Obtain	Choose an address block in which all permitted SNMP monitoring systems exist.

3.1.15 Access Rules

Description Apply standard checks to control access to the router.

3.1.16 Access Allow Telnet

Description Answer Yes if Telnet remote access is permitted for the router. Answer No if SSH will be used exclusively.

3.1.17 IOS - VTY transport telnet

Description	Permit only Telnet for incoming VTY login
Applicability	10.0+ IOSLine configuration mode
Rule Type	Management Plane Level 1⇒Access Rules⇒Access Allow Telnet
Documentation	See section 3.2.9.
Action	<pre>router(config)# line INSTANCE ! router(config-line)# transport input telnet router(config-line)# exit</pre>

3.1.18 IOS - exec-timeout

Description	Disconnect sessions after a fixed idle time.
Applicability	10.0+ IOSLine configuration mode
Rule Type	Management Plane Level 1⇒Access Rules
Documentation	See section 3.2.10.
Action	<pre>router(config)# line INSTANCE router(config-line)# exec-timeout \$(EXEC_TIMEOUT) router(config-line)# exit</pre>

3.1.19 EXEC_TIMEOUT

Info Needed	Timeout values (minutes and seconds) for interactive sessions.
Default Value	10 0
How To Obtain	Choose timeout values (minutes and seconds).

3.1.20 IOS - disable aux

Description	Disable exec on aux.
Applicability	10.0+ IOSLine configuration mode
Rule Type	Management Plane Level 1⇒Access Rules
Documentation	See section 3.2.11.
Action	<pre>router(config)# line aux 0 router(config-line)# no exec router(config-line)# transport input none router(config-line)# exit</pre>

3.1.21 IOS - login default

Description	Configure VTY lines to require login using the default AAA authentication list
Applicability	10.0+ IOSLine configuration mode
Rule Type	Management Plane Level 1⇒Access Rules
Documentation	See section 3.2.12.
Action	<pre>router(config)# line INSTANCE router(config-line)# login authentication default router(config-line)# exit</pre>

3.1.22 IOS - login named list

Description	Configure VTY lines to require login using a particular named AAA authentication list (Note: if you applied the IOS 12.3 auto_secure feature, you should probably answer 'yes' to this question)
Applicability	10.0+ IOSLine configuration mode
Rule Type	Management Plane Level 1⇒Access Rules
Documentation	See section 3.2.13.
Action	<pre>router(config)# line INSTANCE router(config-line)# login authentication \$(AAA_LIST_NAME) router(config-line)# exit</pre>

3.1.23 AAA_LIST_NAME

Info Needed	This is the name of AAA method list that will be used for login authentication and other purposes. Choose 'default' if you want to use the default AAA list, otherwise choose another name, like 'local_auth'. (Note: if you applied the IOS 12.3 auto_secure feature, then 'local_auth' is the name to use.)
Default Value	default
How To Obtain	Select a AAA list name

3.1.24 IOS - require line passwords

Description Set a login password on all lines/VTYs
Applicability 10.0+ IOSLine configuration mode
Rule Type Management Plane Level 1⇒Access Rules
Documentation See section 3.2.14.
Action

```
!
! 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".
!
!router(config)# line INSTANCE
!router(config-line)# password LINE_PASSWORD
!router(config-line)# exit
```

3.1.25 IOS - enable secret

Description Set an enable secret
Applicability 11+ IOSGlobal configuration mode
Rule Type Management Plane Level 1⇒Access Rules
Documentation See section 3.2.15.
Action

```
!
! 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 "ENABLE_SECRET" with the value you have chosen.
! Do not use "ENABLE_SECRET".
!
!router(config)# enable secret ENABLE_SECRET
```

3.1.26 IOS - line password quality

Description Use high quality line passwords.
Applicability 11+ IOSLine configuration mode
Rule Type Management Plane Level 1⇒Access Rules
Documentation See section 3.2.16.
Action

```
!
! 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.
!
!router(config)# line INSTANCE
!router(config-line)# password LINE_PASSWORD
!router(config-line)# exit
```

3.1.27 IOS - user password quality

Description	Use high quality user passwords.
Applicability	11+ IOSLocalUser
Rule Type	Management Plane Level 1⇒Access Rules
Documentation	See section 3.2.17.
Action	<pre> ! ! 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. ! !router(config)# username \$(LOCAL_USERNAME) password LOCAL_PASSWORD </pre>

3.1.28 IOS - apply VTY ACL

Description	Apply VTY access control list to all VTY lines
Applicability	11+ IOSLine configuration mode
Rule Type	Management Plane Level 1⇒Access Rules
Documentation	See section 3.2.18.
Action	<pre> router(config)# line INSTANCE router(config-line)# access-class \$(VTY_ACL_NUMBER) in router(config-line)# exit </pre>

3.1.29 VTY_ACL_NUMBER

Info Needed	The number of the IP access list used to protect the VTY lines (telnet or ssh).
Default Value	182
How To Obtain	Choose an ACL number between 100 and 199.

3.1.30 IOS - Define VTY ACL

Description	Define VTY ACL.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 1⇒Access Rules
Documentation	See section 3.2.19.
Action	<pre> router(config)# no access-list \$(VTY_ACL_NUMBER) router(config)# access-list \$(VTY_ACL_NUMBER) permit tcp \$(VTY_ACL_BLOCK_WITH_MASK) any router(config)# access-list \$(VTY_ACL_NUMBER) permit tcp host \$(VTY_ACL_HOST) any router(config)# access-list \$(VTY_ACL_NUMBER) deny ip any any log </pre>

3.1.31 VTY_ACL_BLOCK_WITH_MASK

Info Needed	The IP address and netmask for the hosts permitted to connect via telnet or ssh to the router.
Default Value	192.168.1.0 0.0.0.255
How To Obtain	Choose an address block that is allowed to access the router.

3.1.32 VTY_ACL_HOST

Info Needed	The IP address of the host permitted to connect via telnet or ssh to the router.
Default Value	192.168.1.254
How To Obtain	Choose a host that is allowed to access the router.

3.1.33 Management Service Rules

Description	Disable unneeded management services.
--------------------	---------------------------------------

3.1.34 IOS 11 - no finger service

Description	Disable finger server.
Applicability	11.0+ IOSGlobal configuration mode
Rule Type	Management Plane Level 1⇒Management Service Rules
Documentation	See section 3.2.20.
Action	<code>router(config)# no service finger</code>

3.1.35 IOS 11 - no identd service

Description	Disable ident server.
Applicability	11.0+ IOSGlobal configuration mode
Rule Type	Management Plane Level 1⇒Management Service Rules
Documentation	See section 3.2.21.
Action	<code>router(config)# no ip identd</code>

3.1.36 IOS 12.1,2,3 - no finger service

Description	Disable finger server.
Applicability	version 12.[123] IOSGlobal configuration mode
Rule Type	Management Plane Level 1⇒Management Service Rules
Documentation	See section 3.2.22.
Action	<code>router(config)# no ip finger</code>

3.1.37 IOS 12.0 - no finger service

Description	Disable finger server. For IOS 12.0, this rule is designed to "fail" every time. This forces the fix to be applied with each run of RAT. The reason for this behavior is that it appears that the default for finger changed in some versions of 12.0 but not others. This makes it impossible, by looking at the configuration, to determine if finger has been turned off. Because of this, it is always assumed to be turned on and the fix to turn it off is applied every time. The score for this rule has been set to "0", so it will be possible to get a "perfect" score.
Applicability	version 12.0 IOSGlobal configuration mode
Rule Type	Management Plane Level 1⇒Management Service Rules
Documentation	See section 3.2.23.
Action	<code>router(config)# no ip finger</code>

3.1.38 IOS - no ip http server

Description	Disable http server.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 1⇒Management Service Rules
Documentation	See section 3.2.24.
Action	<code>router(config)# no ip http server</code>

3.1.39 IOS - encrypt passwords

Description	encrypt passwords in configs.
Applicability	10.0+ IOSGlobal configuration mode
Rule Type	Management Plane Level 1⇒Management Service Rules
Documentation	See section 3.2.25.
Action	<code>router(config)# service password-encryption</code>

3.1.40 Control Plane Level 1

Description	Services, settings, and data streams that support and document the operation, traffic handling, and dynamic status of the router. Examples of control plane services include: logging (e.g. Syslog), routing protocols, status protocols like CDP and HSRP, network topology protocols like STP, and traffic security control protocols like IKE. Network control protocols like ICMP, NTP, ARP, and IGMP directed to or sent by the router itself also fall into this area.
--------------------	--

3.1.41 NTP Rules

Description	Apply standard NTP checks.
--------------------	----------------------------

3.1.42 IOS - ntp server

Description	Designate an NTP time server
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒NTP Rules
Documentation	See section 3.2.26.
Action	<code>router(config)# ntp server \$(NTP_HOST)</code>

3.1.43 NTP_HOST

Info Needed	The IP address of this router's main NTP server.
Default Value	1.2.3.4
How To Obtain	Choose an external NTP server. See http://www.eecis.udel.edu/~mills/ntp/servers.html

3.1.44 IOS - ntp server 2

Description	Designate a second NTP time server
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒NTP Rules
Documentation	See section 3.2.27.
Action	<code>router(config)# ntp server \$(NTP_HOST_2)</code>

3.1.45 NTP_HOST_2

Info Needed	The IP address of this router's 2nd NTP server.
Default Value	5.6.7.8
How To Obtain	Choose an external NTP server. See http://www.eecis.udel.edu/~mills/ntp/servers.html

3.1.46 IOS - ntp server 3

Description	Designate a third NTP time server
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒NTP Rules
Documentation	See section 3.2.28.
Action	<code>router(config)# ntp server \$(NTP_HOST_3)</code>

3.1.47 NTP_HOST_3

Info Needed	The IP address of this router's 3rd NTP server.
Default Value	9.10.11.12
How To Obtain	Choose an external NTP server. See http://www.eecis.udel.edu/~mills/ntp/servers.html

3.1.48 Logging Rules Level 1

Description	Apply standard logging rules.
--------------------	-------------------------------

3.1.49 GMT Rules

Description	Use GMT for logging, etc. Not compatible with localtime. This should be selected if you manage devices in several timezones
--------------------	---

3.1.50 IOS - clock timezone - GMT

Description	Set timezone explicitly
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Logging Rules Level 1⇒GMT Rules
Documentation	See section 3.2.29.
Action	<code>router(config)# clock timezone GMT 0</code>

3.1.51 IOS - forbid clock summer-time - GMT

Description	Don't adjust for summer time.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Logging Rules Level 1⇒GMT Rules
Documentation	See section 3.2.30.
Action	<code>router(config)# no clock summer-time</code>

3.1.52 IOS - service timestamps logging

Description	Configure logging to include message timestamps
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Logging Rules Level 1
Documentation	See section 3.2.31.
Action	<code>router(config)# service timestamps log datetime show-timezone msec</code>

3.1.53 IOS - service timestamps debug

Description	Configure debug messages to include timestamps
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Logging Rules Level 1
Documentation	See section 3.2.32.
Action	<code>router(config)# service timestamps debug datetime show-timezone msec</code>

3.1.54 IOS - enable logging

Description	enable logging.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Logging Rules Level 1
Documentation	See section 3.2.33.
Action	<code>router(config)# logging on</code>

3.1.55 IOS - set syslog server

Description	Designate one or more syslog logging servers
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Logging Rules Level 1
Documentation	See section 3.2.34.
Action	<code>router(config)# logging \$(SYSLOG_HOST)</code>

3.1.56 SYSLOG_HOST

Info Needed	The IP address of this system that will receive syslog messages.
Default Value	13.14.15.16
How To Obtain	Choose a system to receive syslog messages

3.1.57 IOS - logging buffered

Description	Configure buffered logging (with minimum size)
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Logging Rules Level 1
Documentation	See section 3.2.35.
Action	<code>router(config)# logging buffered \$(LOG_BUFFER_SIZE)</code>

3.1.58 LOG_BUFFER_SIZE

Info Needed	This is the size of the local buffer for storing log messages.
Default Value	16000
How To Obtain	Select a local log buffer size

3.1.59 IOS - logging console critical

Description	set console logging level.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Logging Rules Level 1
Documentation	See section 3.2.36.
Action	<code>router(config)# logging console critical</code>

3.1.60 IOS - logging trap info or higher

Description	set SNMP trap and syslog logging level.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Logging Rules Level 1
Documentation	See section 3.2.37.
Action	<code>router(config)# logging trap informational</code>

3.1.61 Control Service Rules

Description	Disable unneeded control services.
--------------------	------------------------------------

3.1.62 IOS 11 - no tcp-small-servers

Description	Disable unnecessary services such as echo, discard, chargen, etc.
Applicability	11.0-2 IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Control Service Rules
Documentation	See section 3.2.38.
Action	<code>router(config)# no service tcp-small-servers</code>

3.1.63 IOS 11 - no udp-small-servers

Description	Disable unnecessary services such as echo, discard, chargen, etc.
Applicability	11.0-2 IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Control Service Rules
Documentation	See section 3.2.39.
Action	<code>router(config)# no service udp-small-servers</code>

3.1.64 IOS 12 - no tcp-small-servers

Description	Disable unnecessary services such as echo, discard, chargen, etc.
Applicability	11.3+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Control Service Rules
Documentation	See section 3.2.40.
Action	<code>router(config)# no service tcp-small-servers</code>

3.1.65 IOS 12 - no udp-small-servers

Description	Disable unnecessary services such as echo, discard, chargen, etc.
Applicability	11.3+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Control Service Rules
Documentation	See section 3.2.41.
Action	<code>router(config)# no service udp-small-servers</code>

3.1.66 IOS - no ip bootp server

Description	Disable bootp server.
Applicability	11.2+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Control Service Rules
Documentation	See section 3.2.42.
Action	<code>router(config)# no ip bootp server</code>

3.1.67 IOS - no cdp run

Description	Disable Cisco Discovery Protocol (CDP) service
Applicability	10.0+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Control Service Rules
Documentation	See section 3.2.43.
Action	<code>router(config)# no cdp run</code>

3.1.68 IOS - no service config

Description	Disable loading of remote configs.
Applicability	10.0+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Control Service Rules
Documentation	See section 3.2.44.
Action	<code>router(config)# no service config</code>

3.1.69 IOS - tcp keepalive service

Description	Use tcp keepalives to kill sessions where the remote side has died.
Applicability	10.0+ IOSGlobal configuration mode
Rule Type	Control Plane Level 1⇒Control Service Rules
Documentation	See section 3.2.45.
Action	<code>router(config)# service tcp-keepalives-in</code>

3.1.70 IOS - no tftp-server

Description	Disable tftp server.
Applicability	11+ IOS TFTP Server
Rule Type	Control Plane Level 1⇒Control Service Rules
Documentation	See section 3.2.46.
Action	<code>router(config)# no tftp-server INSTANCE</code>

3.1.71 Data Plane Level 1

Description	Services and settings related to the data passing through the router (as opposed to directed to it). Basically, the data plane is for everything not in control or management planes. Settings on a router concerned with the data plane include interface access lists, firewall functionality (e.g. CBAC), NAT, and IPSec. Settings for traffic-affecting services like unicast RPF verification and CAR/QoS also fall into this area.
--------------------	--

3.1.72 Routing Rules

Description	Unneeded services should be disabled.
--------------------	---------------------------------------

3.1.73 IOS 11 - no directed broadcast

Description	Explicitly disallow IP directed broadcast on each interface
Applicability	11.0+ IOSInterface configuration mode
Rule Type	Data Plane Level 1⇒Routing Rules
Documentation	See section 3.2.47.
Action	<pre>router(config)# interface INSTANCE router(config-if)# no ip directed-broadcast router(config-if)# exit</pre>

3.1.74 IOS 12 - no directed broadcast

Description	Disallow IP directed broadcast on each interface
Applicability	12.0+ IOSInterface configuration mode
Rule Type	Data Plane Level 1⇒Routing Rules
Documentation	See section 3.2.48.
Action	<pre>router(config)# interface INSTANCE router(config-if)# no ip directed-broadcast router(config-if)# exit</pre>

3.1.75 IOS - no ip source-route

Description	Disable source routing.
Applicability	10.0+ IOSGlobal configuration mode
Rule Type	Data Plane Level 1⇒Routing Rules
Documentation	See section 3.2.49.
Action	<pre>router(config)# no ip source-route</pre>

3.2 Supporting Documentation**3.2.1 IOS - Use local authentication**

Security Impact	Default IOS configurations do not require any user authentication.
Warning	Be sure that local users are created and an enable secret is set before applying this rule.
Importance	10
Rule Actions	See section 3.1.3.
Rule Match	<pre>aaa new-model aaa authentication login \$(AAA_LIST_NAME) local aaa authentication enable \S+</pre>

3.2.2 IOS - Create local users

Security Impact	Default IOS configurations do not require any user authentication.
Warning	If passwords are written, be sure to properly secure the written copies. Be sure an enable secret is set before applying these lines. Be sure to choose non-trivial passwords that are in accord with local policy.
Importance	10
Rule Actions	See section 3.1.4.
Rule Match	<pre>username \S+ password \d \S+</pre>

3.2.3 IOS - no snmp-server

Security Impact	SNMP allows remote monitoring and management of the router. Older version of the protocol do not use any encryption for the community strings (passwords). SNMP should be disabled unless you absolutely require it for network management purposes. If you require SNMP, be sure to select SNMP community strings that are strong passwords, and are not the same as other passwords used for the enable password, line password, BGP key or other authentication credentials. Consider utilizing SNMPv3 which utilizes authentication and data privatization (encryption), when available.
Warning	Disabling SNMP may disrupt system monitoring.
Importance	10
For More Info	See RSCG page 76 for more information.
Rule Actions	See section 3.1.7.
Rule Match	<code>^snmp-server</code>

3.2.4 IOS - forbid SNMP read-write

Security Impact	Enabling SNMP read-write enables remote (mis)management. It presents a possible avenue of attack. Disabling it removes the potential for such abuse.
Importance	10
For More Info	See RSCG page 138 for more information.
Rule Actions	See section 3.1.8.
Rule Match	<code>snmp-server community.*RW</code>

3.2.5 IOS - forbid SNMP community public

Security Impact	SNMP allows management and monitoring of networked devices. "public" is a well known default community string. Its use allows unauthorized individuals to easily obtain information from the router. SNMP should be disabled unless you absolutely require it for network management purposes. If you require SNMP, be sure to select SNMP community strings that are strong passwords, and are not the same as other passwords used for the enable password, line password, BGP key or other authentication credentials. Consider utilizing SNMPv3 which utilizes authentication and data privatization (encryption), when available.
Importance	10
For More Info	See RSCG page 138 for more information.
Rule Actions	See section 3.1.9.
Rule Match	<code>snmp-server community public</code>

3.2.6 IOS - forbid SNMP community private

Security Impact	SNMP allows management and monitoring of networked devices. "private" is a well known default community string. Its use allows unauthorized individuals to easily (mis)manage the router. SNMP should be disabled unless you absolutely require it for network management purposes. If you require SNMP, be sure to select SNMP community strings that are strong passwords, and are not the same as other passwords used for the enable password, line password, BGP key or other authentication credentials. Consider utilizing SNMPv3 which utilizes authentication and data privatization (encryption), when available.
Importance	10
For More Info	See RSCG page 138 for more information.
Rule Actions	See section 3.1.10.
Rule Match	<code>snmp-server community private</code>

3.2.7 IOS - forbid SNMP without ACLs

Security Impact	If ACLs are not applied, then anyone with a valid SNMP community string may monitor and manage the router. An ACL should be defined and applied for all SNMP community strings to limit access to a small number of authorized management stations.
Importance	10
For More Info	See RSCG page 85 and RSCG page 142 for more information.
Rule Actions	See section 3.1.11.
Rule Match	<code>snmp-server community.*(RW RO)\$</code>

3.2.8 IOS - Define SNMP ACL

Security Impact	SNMP ACLs control what addresses are authorized to manage and monitor your router via SNMP
Importance	10
For More Info	See RSCG page 85 for more information.
Rule Actions	See section 3.1.13.
Rule Match	<code>access-list \$(SNMP_ACL_NUMBER) permit \$(SNMP_ACL_BLOCK_WITH_MASK)</code> <code>access-list \$(SNMP_ACL_NUMBER) deny any log</code>

3.2.9 IOS - VTY transport telnet

Security Impact	Only permit protocols you intend to use. This prevents the other protocols from being mis-used.
Warning	Telnet protocol sends passwords in the clear. Use SSH instead, if the router supports it.
Importance	5
For More Info	Note that many newer versions of IOS support SSH. SSH should be used in in place of Telnet wherever possible. See RSCG page 64 and RSCG page 214 for more information.
Rule Actions	See section 3.1.17.
Rule Match	<code>transport input telnet</code>

3.2.10 IOS - exec-timeout

Security Impact	This prevents unauthorized users from misusing abandoned sessions (for instance if the network administrator went on vacation and left an enabled login session active on his desktop system). There is a trade-off here between security (shorter timeouts) and usability (longer timeouts). Check your local policies and operational needs to determine the best value. In most cases, this should be no more than 10 minutes.
Importance	7
For More Info	See RSCG page 58 for more information.
Rule Actions	See section 3.1.18.
Rule Match	

3.2.11 IOS - disable aux

Security Impact	Unused ports should be disabled since they provide a potential access path for attackers.
Importance	3
For More Info	See RSCG page 58 for more information.
Rule Actions	See section 3.1.20.
Rule Match	<code>no exec\$</code>

3.2.12 IOS - login default

Security Impact	The default under AAA (local or network) is to require users to log in using a valid user name and password. If this line appears, then some behavior other than the secure default is being specified. This rule applies for both local and network AAA.
Importance	10
For More Info	See RSCG page 58 and RSCG page 68 for more information.
Rule Actions	See section 3.1.21.
Rule Match	<code>login [^\n\s]+</code>

3.2.13 IOS - login named list

Security Impact	If an named AAA authentication list, other than default, is to be used, then it must be specified explicitly on each IOS line. If selected, this rule applies for both local and network AAA.
Importance	10
For More Info	See RSCG page 58 and RSCG page 168 for more information.
Rule Actions	See section 3.1.22.
Rule Match	<code>login authentication \$(AAA_LIST_NAME)</code>

3.2.14 IOS - require line passwords

Security Impact	This requires a password to be set on each line. Note, that given the use of local usernames (level 1) or TACACS (level 2) line passwords will not be used for authentication. There they are included as a fail-safe to ensure that some password is required for access to the router in case other AAA options are not configured.
Warning	The encryption used for line passwords is weak, reversible and the algorithm is well known. You should assume that anyone with access to the configuration can decode the line passwords. For this reason line passwords should be different than the enable passwords and any local user passwords.
Importance	10
For More Info	See RSCG page 58 for more information.
Rule Actions	See section 3.1.24.
Rule Match	<code>password [^\n\s]+</code>

3.2.15 IOS - enable secret

Security Impact	Enable secrets use a strong, one-way cryptographic hash (MD5). This is preferred to enable passwords, which use a weak, well known, reversible encryption algorithm.
Warning	This should be different than line passwords, local username passwords or SNMP community strings. If passwords are written, be sure to properly secure the written copies.
Importance	10
For More Info	See RSCG page 61 for more information.
Rule Actions	See section 3.1.25.
Rule Match	<code>enable secret \d \S+</code>

3.2.16 IOS - line password quality

Security Impact	Low quality passwords are easily guessed possibly providing unauthorized access to the router.
Importance	5
For More Info	AAA should normally be used instead of line password, but if you do set a line password it should be hard to guess. All passwords should contain a mixture of upper- and lower-case letters, digits, and punctuation. If this rule fails, it is because a line password received a score of 45/100 or less in a common password quality metric. See RSCG page 62 for more information.
Rule Actions	See section 3.1.26.
Rule Match	<code>password 7 \S+</code>

3.2.17 IOS - user password quality

Security Impact	Low quality passwords are easily guessed possibly providing unauthorized access to the router.
Importance	5
For More Info	Passwords should be hard to guess. They should contain a mixture of upper- and lower-case letters, digits, and punctuation. If this rule fails, it is because one or more user passwords received a score of 45/100 or less in a common password quality metric. See RSCG page 62 for more information.
Rule Actions	See section 3.1.27.
Rule Match	<code>user.*password 7 \S+</code>

3.2.18 IOS - apply VTY ACL

Security Impact	VTY ACLs control what addresses may attempt to log in to your router.
Importance	10
For More Info	See RSCG page 64 for more information.
Rule Actions	See section 3.1.28.
Rule Match	<code>access-class \$(VTY_ACL_NUMBER) in</code>

3.2.19 IOS - Define VTY ACL

Security Impact	VTY ACLs control what addresses may attempt to log in to your router.
Importance	10
For More Info	See RSCG page 64 for more information.
Rule Actions	See section 3.1.30.
Rule Match	<code>access-list \$(VTY_ACL_NUMBER) permit tcp \$(VTY_ACL_BLOCK_WITH_MASK) any access-list \$(VTY_ACL_NUMBER) permit tcp host \$(VTY_ACL_HOST) any access-list \$(VTY_ACL_NUMBER) deny ip any any log</code>

3.2.20 IOS 11 - no finger service

Security Impact	From Cisco IOS documentation: "As with all minor services, the Finger service should be disabled on your system if you do not have a need for it in your network. Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks."
Importance	5
For More Info	See RSCG page 71 for more information.
Rule Actions	See section 3.1.34.
Rule Match	<code>no (service ip) finger</code>

3.2.21 IOS 11 - no identd service

Security Impact	Services that are not needed should be turned off because they present potential avenues of attack and may provide information that could be useful for gaining unauthorized access.
Importance	7
Rule Actions	See section 3.1.35.
Rule Match	<code>ip identd</code>

3.2.22 IOS 12.1,2,3 - no finger service

Security Impact	From Cisco IOS documentation: "As with all minor services, the Finger service should be disabled on your system if you do not have a need for it in your network. Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks."
Importance	5
For More Info	See RSCG page 71 for more information.
Rule Actions	See section 3.1.36.
Rule Match	<code>^ip finger</code>

3.2.23 IOS 12.0 - no finger service

Security Impact	From Cisco IOS documentation: "As with all minor services, the Finger service should be disabled on your system if you do not have a need for it in your network. Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks."
Warning Importance	For 12.0 only this rule turns off finger every time.
For More Info	See RSCG page 71 for more information.
Rule Actions	See section 3.1.37.
Rule Match	<code>^This will always fail</code>

3.2.24 IOS - no ip http server

Security Impact	The HTTP server allows remote management of routers. Unfortunately, it uses simple HTTP authentication which sends passwords in the clear. This could allow unauthorized access to, and [mis]management of the router. The http server should be disabled.
Importance	10
For More Info	See RSCG page 72 for more information.
Rule Actions	See section 3.1.38.
Rule Match	<code>^ip http server</code>

3.2.25 IOS - encrypt passwords

Security Impact	This requires passwords to be encrypted in the configuration file to prevent unauthorized users from learning the passwords by reading the configuration.
Importance	7
For More Info	See RSCG page 62 for more information.
Rule Actions	See section 3.1.39.
Rule Match	<code>^service password-encryption</code>

3.2.26 IOS - ntp server

Security Impact	Set the NTP server(s) from which you obtain time. Obtaining time from a trusted source increases confidence in log data and enables correlation of events.
Importance	5
For More Info	See RSCG page 136 for more information.
Rule Actions	See section 3.1.42.
Rule Match	<code>ntp server \$(NTP_HOST)</code>

3.2.27 IOS - ntp server 2

Security Impact	Set an additional NTP server(s) from which you obtain time. Additional time sources increase the accuracy and dependability of system time.
Importance	5
For More Info	See RSCG page 136 for more information.
Rule Actions	See section 3.1.44.
Rule Match	<code>ntp server \$(NTP_HOST_2)</code>

3.2.28 IOS - ntp server 3

Security Impact	Set an additional NTP server(s) from which you obtain time. Additional time sources increase the accuracy and dependability of system time.
Importance	5
For More Info	See RSCG page 136 for more information.
Rule Actions	See section 3.1.46.
Rule Match	<code>ntp server \$(NTP_HOST_3)</code>

3.2.29 IOS - clock timezone - GMT

Security Impact	Set the clock to GMT. This ensures that it is possible to correlate logs.
Warning	If you manage devices in more than one timezone, consider using GMT.
Importance	3
For More Info	See RSCG page 134 for more information.
Rule Actions	See section 3.1.50.
Rule Match	<code>clock timezone GMT 0</code>

3.2.30 IOS - forbid clock summer-time - GMT

Security Impact	Adjusting for local variances in time of day could lead to confusion. Use of unadjusted GMT removes ambiguities.
Importance	5
Rule Actions	See section 3.1.51.
Rule Match	<code>clock summer-time</code>

3.2.31 IOS - service timestamps logging

Security Impact	Including timestamps in log messages will allow you to correlate events and trace network attacks.
Importance	5
For More Info	See RSCG page 129 for more information.
Rule Actions	See section 3.1.52.
Rule Match	<code>service timestamps log datetime(msec)? show-timezone</code>

3.2.32 IOS - service timestamps debug

Security Impact	Including timestamps in debug messages will allow you to correlate events and trace network attacks.
Importance	5
For More Info	See RSCG page 129 for more information.
Rule Actions	See section 3.1.53.
Rule Match	<code>service timestamps debug datetime(msec)? show-timezone</code>

3.2.33 IOS - enable logging

Security Impact	Logging should be enabled to allow monitoring of both operational and security related events.
Importance	5
For More Info	See RSCG page 129 for more information.
Rule Actions	See section 3.1.54.
Rule Match	<code>no logging on</code>

3.2.34 IOS - set syslog server

Security Impact	Cisco routers can send their log messages to a Unix-style syslog service. A syslog service simply accepts messages, and stores them in files or prints them according to a simple configuration file. This form of logging is the best available for Cisco routers, because it can provide protected long-term storage for logs.
Importance	5
For More Info	See RSCG page 130 for more information.
Rule Actions	See section 3.1.55.
Rule Match	logging <code>\$(SYSLOG_HOST)</code>

3.2.35 IOS - logging buffered

Security Impact	Cisco routers can store log messages in a memory buffer. The buffered data is available only from a router exec or enabled exec session. This form of logging is useful for debugging and monitoring when logged in to a router.
Warning	The buffered data is cleared when the router boots. So while the data is useful, it does not offer enough long-term protection for the logs. Also, be aware that space reserved for buffering log messages reduces memory available for other router functions. Also note that if you choose the default IOS size for buffers (currently 4096), RAT will report a rule failure since IOS does not display settings for some default values.
Importance	5
For More Info	See RSCG page 129 for more information.
Rule Actions	See section 3.1.57.
Rule Match	logging buffered <code>\d+</code>

3.2.36 IOS - logging console critical

Security Impact	This determines the severity of messages that will generate console messages. This form of logging is not persistent; messages printed to the console are not stored by the router. Console logging is handy for operators when they use the console
Warning	It is possible that excessive log messages on the console could make it impossible to manage the router, even on the console. To prevent this, use 'no logging console' to turn off all console logging.
Importance	3
For More Info	'term monitor' may be used to see log messages on the currently connected session without logging messages to the console. See RSCG page 129 for more information.
Rule Actions	See section 3.1.59.
Rule Match	logging console critical

3.2.37 IOS - logging trap info or higher

Security Impact	This determines the severity of messages that will generate an SNMP trap and syslog messages.
Importance	3
For More Info	set SNMP/Syslog trap level. This determines the level of message that will generate an SNMP trap and/or a Syslog log message. It should be set to either "debugging" (7) or "informational" (6), but no lower. The default, in IOS 11.3 and later is "informational". See RSCG page 132 for more information.
Rule Actions	See section 3.1.60.
Rule Match	<code>logging trap ((alerts) (critical) (emergencies) (errors) (warnings) (notifications) ([0-5]))</code>

3.2.38 IOS 11 - no tcp-small-servers

Security Impact	Services that are not needed should be turned off because they present potential avenues of attack and may provide information that could be useful for gaining unauthorized access.
Importance	7
For More Info	See RSCG page 71 for more information.
Rule Actions	See section 3.1.62.
Rule Match	<code>no service tcp-small-servers</code>

3.2.39 IOS 11 - no udp-small-servers

Security Impact	Services that are not needed should be turned off because they present potential avenues of attack and may provide information that could be useful for gaining unauthorized access.
Importance	7
For More Info	See RSCG page 71 for more information.
Rule Actions	See section 3.1.63.
Rule Match	<code>no service udp-small-servers</code>

3.2.40 IOS 12 - no tcp-small-servers

Security Impact	Services that are not needed should be turned off because they present potential avenues of attack and may provide information that could be useful for gaining unauthorized access.
Importance	7
For More Info	See RSCG page 71 for more information.
Rule Actions	See section 3.1.64.
Rule Match	<code>^service tcp-small-servers</code>

3.2.41 IOS 12 - no udp-small-servers

Security Impact	Services that are not needed should be turned off because they present potential avenues of attack and may provide information that could be useful for gaining unauthorized access.
Importance	7
For More Info	See RSCG page 71 for more information.
Rule Actions	See section 3.1.65.
Rule Match	<code>^service udp-small-servers</code>

3.2.42 IOS - no ip bootp server

Security Impact	From Cisco IOS documentation: "As with all minor services, the async line BOOTP service should be disabled on your system if you do not have a need for it in your network. Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks."
Importance	5
For More Info	See RSCG page 73 for more information.
Rule Actions	See section 3.1.66.
Rule Match	<code>^no ip bootp server</code>

3.2.43 IOS - no cdp run

Security Impact	The Cisco Discovery Protocol is a proprietary protocol that Cisco devices use to identify each other on a LAN segment. It is useful only in specialized situations, and is considered to be a security risk. There have been published denial of service attacks that use CDP. CDP should be completely disabled unless there is a need for it.
Importance	7
For More Info	See RSCG page 71 for more information.
Rule Actions	See section 3.1.67.
Rule Match	<code>no cdp run</code>

3.2.44 IOS - no service config

Security Impact	Service config allows a router to load its startup configuration from a remote device (e.g. a tftp server). Unless the router absolutely needs to autoloading its startup configuration from a TFTP host, disable network auto-loading.
Importance	7
For More Info	See RSCG page 73 for more information.
Rule Actions	See section 3.1.68.
Rule Match	<code>service config</code>

3.2.45 IOS - tcp keepalive service

Security Impact	Stale connections use resources and could potentially be hijacked to gain illegitimate access.
Importance	5
Rule Actions	See section 3.1.69.
Rule Match	<code>^service tcp-keepalives-in</code>

3.2.46 IOS - no tftp-server

Security Impact	The TFTP protocol has no authentication. It allows anyone who can connect to download files, such as router configs and system images.
Importance	10
Rule Actions	See section 3.1.70.
Rule Match	<code>tftp-server</code>

3.2.47 IOS 11 - no directed broadcast

Security Impact	Router interfaces that allow directed broadcasts can be used for "smurf" attacks.
Importance	7
For More Info	See RSCG page 75 for more information.
Rule Actions	See section 3.1.73.
Rule Match	no ip directed-broadcast

3.2.48 IOS 12 - no directed broadcast

Security Impact	Router interfaces that allow directed broadcasts can be used for "smurf" attacks.
Importance	7
For More Info	See RSCG page 75 for more information.
Rule Actions	See section 3.1.74.
Rule Match	^ ip directed-broadcast

3.2.49 IOS - no ip source-route

Security Impact	Source routing is a feature of IP whereby individual packets can specify routes. This feature is used in several kinds of attacks. Cisco routers normally accept and process source routes. Unless a network depends on source routing, it should be disabled.
Warning	There may be legitimate operational reasons for leaving source routing enabled, particularly in larger networks as an aid to diagnosing routing problems.
Importance	7
For More Info	See RSCG page 74 for more information.
Rule Actions	See section 3.1.75.
Rule Match	no ip source-route

4 The Level-2 Benchmark

4.1 Actions

4.1.1 Management Plane Level 2

Description	Services, settings, and data streams related to setting up and examining the static configuration of the router, and the authentication and authorization of router administrators. Examples of management plane services include: administrative telnet, SNMP, TFTP for image file upload, and security protocols like RADIUS and TACACS+.
--------------------	---

4.1.2 TACACS Plus AAA Rules

Description	Rules in the TACACS Plus AAA Rules Configuration class implement TACACS+ authentication. Only one set of authentication rules (LocalAAARules, TACACS+) may be selected.
--------------------	---

4.1.3 IOS - Create Emergency Local User Account

Description	Check for the presence of a local user account
Applicability	10.0+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒TACACS Plus AAA Rules
Documentation	See section 4.2.1.
Action	! ! 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". ! !router(config)# username \$(LOCAL_USERNAME) password LOCAL_PASSWORD

4.1.4 IOS - aaa new-model

Description	Use centralized AAA system (new-model).
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒TACACS Plus AAA Rules
Documentation	See section 4.2.2.
Action	router(config)# aaa new-model

4.1.5 IOS - aaa authentication login

Description	Use AAA authentication methods for login authentication (with fall-back).
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒TACACS Plus AAA Rules
Documentation	See section 4.2.3.
Action	router(config)# aaa authentication login \$(AAA_LIST_NAME) group tacacs+ local enable

4.1.6 IOS - aaa authentication enable

Description	Use AAA authentication methods for enable authentication (with fall-back).
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒TACACS Plus AAA Rules
Documentation	See section 4.2.4.
Action	router(config)# aaa authentication enable default group tacacs+ enable

4.1.7 IOS - aaa accounting exec

Description	use AAA accounting for exec.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒TACACS Plus AAA Rules
Documentation	See section 4.2.5.
Action	router(config)# aaa accounting exec default start-stop group tacacs+

4.1.8 IOS - aaa accounting commands

Description	use AAA accounting for commands.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒TACACS Plus AAA Rules
Documentation	See section 4.2.6.
Action	<code>router(config)# aaa accounting commands 15 default start-stop group tacacs+</code>

4.1.9 IOS - aaa accounting network

Description	use AAA accounting for network events.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒TACACS Plus AAA Rules
Documentation	See section 4.2.7.
Action	<code>router(config)# aaa accounting network default start-stop group tacacs+</code>

4.1.10 IOS - aaa accounting connection

Description	use AAA accounting for connections.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒TACACS Plus AAA Rules
Documentation	See section 4.2.8.
Action	<code>router(config)# aaa accounting connection default start-stop group tacacs+</code>

4.1.11 IOS - aaa accounting system

Description	use AAA accounting for system events.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒TACACS Plus AAA Rules
Documentation	See section 4.2.9.
Action	<code>router(config)# aaa accounting system default start-stop group tacacs+</code>

4.1.12 IOS - aaa source-interface

Description	Bind AAA services to the loopback interface.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒TACACS Plus AAA Rules
Documentation	See section 4.2.10.
Action	<code>router(config)# ip tacacs source-interface Loopback\$(LOOPBACK_NUMBER)</code>

4.1.13 LOOPBACK_NUMBER

Info Needed	The number of the local loopback interface to use as the router's source address (almost always Loopback0).
How To Obtain	<code>show ip interface brief</code>

4.1.14 IOS - One loopback interface must exist

Description	Define and configure one loopback interface.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒TACACS Plus AAA Rules⇒IOS - aaa source-interface
Documentation	See section 4.2.11.
Action	<pre>router(config)# interface Loopback\$(LOOPBACK_NUMBER) router(config-if)# ip address \$(LOOPBACK_ADDRESS) router(config-if)# exit</pre>

4.1.15 LOOPBACK_ADDRESS

Info Needed	The IP address of this router's loopback interface (if any).
Default Value	192.168.1.3
How To Obtain	Consult local topology maps, your ISP or network administrators.

4.1.16 Access Rules Level 2

Description Apply level 2 checks to control access to the router.

4.1.17 Access Require SSH

Description Select this class if SSH is the only remote access protocol permitted for the router.

4.1.18 IOS - VTY transport SSH

Description	Permit only SSH for incoming VTY login
Applicability	12.0+ IOSLine configuration mode
Rule Type	Management Plane Level 2⇒Access Rules Level 2⇒Access Require SSH
Documentation	See section 4.2.12.
Action	<pre>router(config)# line INSTANCE router(config-line)# transport input ssh router(config-line)# exit</pre>

4.1.19 IOS - apply VTY SSH ACL

Description	Apply VTY access control list to all VTY lines
Applicability	12.0+ IOSLine configuration mode
Rule Type	Management Plane Level 2⇒Access Rules Level 2⇒Access Require SSH
Documentation	See section 4.2.13.
Action	<pre>router(config)# line INSTANCE router(config-line)# access-class \$(VTY_ACL_NUMBER) in router(config-line)# exit</pre>

4.1.20 IOS - define VTY SSH ACL

Description	Define VTY access control list
Applicability	12.0+ IOSGlobal configuration mode
Rule Type	Management Plane Level 2⇒Access Rules Level 2⇒Access Require SSH
Documentation	See section 4.2.14.
Action	<pre>router(config)# no access-list \$(VTY_ACL_NUMBER) router(config)# access-list \$(VTY_ACL_NUMBER) permit tcp \$(VTY_ACL_BLOCK_WITH_MASK) any router(config)# access-list \$(VTY_ACL_NUMBER) permit tcp host \$(VTY_ACL_HOST) any router(config)# access-list \$(VTY_ACL_NUMBER) deny ip any any log</pre>

4.1.21 Control Plane Level 2

Description	Services, settings, and data streams that support and document the operation, traffic handling, and dynamic status of the router. Examples of control plane services include: logging (e.g. Syslog), routing protocols, status protocols like CDP and HSRP, network topology protocols like STP, and traffic security control protocols like IKE. Network control protocols like ICMP, NTP, ARP, and IGMP directed to or sent by the router itself also fall into this area.
--------------------	--

4.1.22 Logging Rules Level 2

Description	Apply non-standard logging rules.
--------------------	-----------------------------------

4.1.23 Localtime Rules

Description	Use local time for logging, etc. Not compatible with GMT. This should be selected if all your devices are in one timezone.
--------------------	--

4.1.24 LOCAL.TIMEZONE

Info Needed	Specify the name of the timezone to be used. For example, GMT,EST, etc.
Default Value	GMT
How To Obtain	Select your local timezone. See http://greenwichmeantime.com

4.1.25 TIMEZONE.OFFSET

Info Needed	Specify the number of hours difference from GMT. For example, 0, -5, 2, etc.
How To Obtain	Select your GMT offset in hours. See http://greenwichmeantime.com

4.1.26 IOS - clock timezone - localtime

Description	Set timezone explicitly.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 2⇒Logging Rules Level 2⇒Localtime Rules
Documentation	See section 4.2.15.
Action	<pre>router(config)# clock timezone \$(LOCAL.TIMEZONE) \$(TIMEZONE.OFFSET)</pre>

4.1.27 IOS - require clock summer-time - localtime

Description	Adjust to summertime if local timezone is used.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 2⇒Logging Rules Level 2⇒Localtime Rules
Documentation	See section 4.2.16.
Action	<code>router(config)# clock summer-time \$(LOCAL_TIMEZONE) recurring</code>

4.1.28 Loopback Rules

Description	Apply extra loopback checks. Note that addresses that are assigned loopback interfaces on routers must be routable to the management devices (syslog, telnet, TACACS, SNMP) that the router must communicate with.
--------------------	--

4.1.29 IOS - ntp source

Description	Bind the NTP service to the loopback interface.
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 2⇒Loopback Rules
Documentation	See section 4.2.17.
Action	<code>router(config)# ntp source Loopback\$(LOOPBACK_NUMBER)</code>

4.1.30 IOS - Defined loopback must be only loopback

Description	Define no more than one loopback interface
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 2⇒Loopback Rules
Documentation	See section 4.2.18.
Action	<code>router(config)# no interface INSTANCE</code>

4.1.31 IOS - tftp source-interface

Description	Bind the TFTP client to the loopback interface
Applicability	11+ IOSGlobal configuration mode
Rule Type	Control Plane Level 2⇒Loopback Rules
Documentation	See section 4.2.19.
Action	<code>router(config)# ip tftp source-interface Loopback\$(LOOPBACK_NUMBER)</code>

4.1.32 Control Service Rules Level 2

Description	Unneeded services should be disabled.
--------------------	---------------------------------------

4.1.33 Data Plane Level 2

Description	Services and settings related to the data passing through the router (as opposed to directed to it). Basically, the data plane is for everything not in control or management planes. Settings on a router concerned with the data plane include interface access lists, firewall functionality (e.g. CBAC), NAT, and IPSec. Settings for traffic-affecting services like unicast RPF verification and CAR/QoS also fall into this area.
--------------------	--

4.1.34 Border Router Filtering

Description A border router is a router that connects "internal" networks such as desktop networks, DMZ networks, etc., to "external" networks such as the Internet. If this group is chosen, then ingress and egress filter rules will be required. "Building Internet Firewalls" by Zwicky, Cooper and Chapman, O'Reilly and Associates.

4.1.35 EXTERNAL_INTERFACE

Info Needed The router interface that attached to an external or untrusted network (e.g. the Internet). This should be the full name as it appears in the configuration file (e.g. "Ethernet0"), not an abbreviation (e.g. "eth0").

Default Value Ethernet0

How To Obtain show ip interface brief

4.1.36 Border Router Second IF

Description Require and configure a second external interface.

4.1.37 SECOND_EXTERNAL_INTERFACE

Info Needed A second router interface that attached to an external or untrusted network (e.g. the Internet). This should be the full name as it appears in the configuration file (e.g. "Ethernet0"), not an abbreviation (e.g. "eth0").

Default Value Ethernet1

How To Obtain show ip interface brief

4.1.38 IOS - Apply ingress filter to 2nd IF

Description Apply inbound anti-spoof filters.

Applicability 10.0+ IOSInterface configuration mode

Rule Type Data Plane Level 2⇒Border Router Filtering⇒Border Router Second IF

Documentation See section 4.2.20.

Action

```
router(config)# interface $(SECOND_EXTERNAL_INTERFACE)
router(config-if)# ip access-group $(INGRESS_ACL_NUMBER) in
router(config-if)# exit
```

4.1.39 INGRESS_ACL_NUMBER

Info Needed The number of the IP access list used for RFC2827 filtering on packets incoming from the untrusted network.

Default Value 180

How To Obtain Choose an ACL number between 100 and 199.

4.1.40 IOS - Apply egress filter to second external IF

Description	Apply outbound anti-spoof filters.
Applicability	10.0+ IOSInterface configuration mode
Rule Type	Data Plane Level 2⇒Border Router Filtering⇒Border Router Second IF
Documentation	See section 4.2.21.
Action	<pre>router(config)# interface \$(SECOND_EXTERNAL_INTERFACE) router(config-if)# ip access-group \$(EGRESS_ACL_NUMBER) out router(config-if)# exit</pre>

4.1.41 EGRESS_ACL_NUMBER

Info Needed	The number of the IP access list used for RFC2827 filtering on packets being sent to the untrusted network.
Default Value	181
How To Obtain	Choose an ACL number between 100 and 199.

4.1.42 IOS - require second external interface to exist

Description	Check for existence of 2nd external interface.
Applicability	10.0+ IOSGlobal configuration mode
Rule Type	Data Plane Level 2⇒Border Router Filtering⇒Border Router Second IF
Documentation	See section 4.2.22.
Action	

4.1.43 IOS - egress filter definition

Description	Define ACL to block all outbound traffic that does not have a valid internal source address.
Applicability	10.0+ IOSGlobal configuration mode
Rule Type	Data Plane Level 2⇒Border Router Filtering
Documentation	See section 4.2.23.
Action	<pre>router(config)# no access-list \$(EGRESS_ACL_NUMBER) router(config)# access-list \$(EGRESS_ACL_NUMBER) permit ip \$(INTERNAL_NETBLOCK_WITH_MASK) any router(config)# access-list \$(EGRESS_ACL_NUMBER) deny ip any any log</pre>

4.1.44 INTERNAL_NETBLOCK_WITH_MASK

Info Needed	The LAN address and netmask of your internal (trusted) network.
Default Value	192.168.1.0 0.0.0.255
How To Obtain	Consult local topology maps, your ISP or network administrators.

4.1.45 IOS - Apply ingress filter

Description	Apply inbound anti-spoof filters.
Applicability	10.0+ IOSInterface configuration mode
Rule Type	Data Plane Level 2⇒Border Router Filtering
Documentation	See section 4.2.24.
Action	<pre>router(config)# interface \$(EXTERNAL_INTERFACE) router(config-if)# ip access-group \$(INGRESS_ACL_NUMBER) in router(config-if)# exit</pre>

4.1.46 IOS - ingress filter definition

Description	Define ACL to block RFC1918-reserved and internal addresses inbound
Applicability	10.0+ IOSGlobal configuration mode
Rule Type	Data Plane Level 2⇒Border Router Filtering
Documentation	See section 4.2.25.
Action	<pre> router(config)# no access-list \$(INGRESS_ACL_NUMBER) router(config)# access-list \$(INGRESS_ACL_NUMBER) deny ip 10.0.0.0 0.255.255.255 any log router(config)# access-list \$(INGRESS_ACL_NUMBER) deny ip 127.0.0.0 0.255.255.255 any log router(config)# access-list \$(INGRESS_ACL_NUMBER) deny ip 172.16.0.0 0.15.255.255 any log router(config)# access-list \$(INGRESS_ACL_NUMBER) deny ip 192.168.0.0 0.0.255.255 any log router(config)# access-list \$(INGRESS_ACL_NUMBER) deny ip \$(INTERNAL_NETBLOCK_WITH_MASK) any router(config)# access-list \$(INGRESS_ACL_NUMBER) deny ip any 10.0.0.0 0.255.255.255 log router(config)# access-list \$(INGRESS_ACL_NUMBER) deny ip any 127.0.0.0 0.255.255.255 log router(config)# access-list \$(INGRESS_ACL_NUMBER) deny ip any 172.16.0.0 0.15.255.255 log router(config)# access-list \$(INGRESS_ACL_NUMBER) deny ip any 192.168.0.0 0.0.255.255 log router(config)# access-list \$(INGRESS_ACL_NUMBER) permit ip any any </pre>

4.1.47 IOS - Apply egress filter to first external interface

Description	Apply outbound anti-spoof filters.
Applicability	10.0+ IOSInterface configuration mode
Rule Type	Data Plane Level 2⇒Border Router Filtering
Documentation	See section 4.2.26.
Action	<pre> router(config)# interface \$(EXTERNAL_INTERFACE) router(config-if)# ip access-group \$(EGRESS_ACL_NUMBER) out router(config-if)# exit </pre>

4.1.48 IOS - require external IF to exist

Description	Check for existence of external interface.
Applicability	10.0+ IOSGlobal configuration mode
Rule Type	Data Plane Level 2⇒Border Router Filtering
Documentation	See section 4.2.27.
Action	

4.1.49 Routing Rules Level 2

Description	Unneeded services should be disabled.
--------------------	---------------------------------------

4.1.50 Unicast RPF Router

Description Unicast Reverse-Path Forwarding Verification is an IOS 12 facility that uses the routing table to reject mis-addressed and spoof-addressed packets. It is suitable for use when a router should have unambiguous symmetric routes to everywhere, such as a border router with a single upstream link.

4.1.51 IOS 12 - apply unicast RPF

Description Apply IP Unicast RPF on each interface.
Applicability 12.0+ IOSInterface configuration mode
Rule Type Data Plane Level 2⇒Routing Rules Level 2⇒Unicast RPF Router
Documentation See section 4.2.28.
Action

```
router(config)# ip cef
router(config)# interface INSTANCE
router(config-if)# ip verify unicast reverse-path
router(config-if)# exit
```

4.1.52 IOS - no ip proxy-arp

Description Disable proxy ARP on all interfaces
Applicability 10.0+ IOSInterface configuration mode
Rule Type Data Plane Level 2⇒Routing Rules Level 2
Documentation See section 4.2.29.
Action

```
router(config)# interface INSTANCE
router(config-if)# no ip proxy-arp
router(config-if)# exit
```

4.1.53 IOS - tunnel interfaces must not exist

Description Do not define any tunnel interfaces.
Applicability 11+ IOSTunnelNumber
Rule Type Data Plane Level 2⇒Routing Rules Level 2
Documentation See section 4.2.30.
Action

```
router(config)# no interface Tunnel INSTANCE
```

4.2 Supporting Documentation**4.2.1 IOS - Create Emergency Local User Account**

Security Impact A single local account should exist to be used in an emergency when other authentication methods (tacacs, radius) are not available. This account information should not be used by any user except in the case of emergency. Account information (username and password) should be stored in a secure location. There may be reasons for creating more than one local account. Check local policy.

Importance 4
Rule Actions See section 4.1.3.
Rule Match

```
username \S+ password \d \S+
```

4.2.2 IOS - aaa new-model

Security Impact Centralized AAA systems improve consistency, access control and accountability.
Importance 5
For More Info See RSCG page 163 and RSCG page 167 for more information.
Rule Actions See section 4.1.4.
Rule Match `aaa new-model`

4.2.3 IOS - aaa authentication login

Importance 5
For More Info See RSCG page 168 for more information.
Rule Actions See section 4.1.5.
Rule Match `aaa authentication login ($(AAA_LIST_NAME) |(group |)tacacs\+ local enable`

4.2.4 IOS - aaa authentication enable

Importance 5
For More Info See RSCG page 168 for more information.
Rule Actions See section 4.1.6.
Rule Match `aaa authentication enable (default |(group |)tacacs\+ enable`

4.2.5 IOS - aaa accounting exec

Importance 5
Rule Actions See section 4.1.7.
Rule Match `aaa accounting exec (default |)start-stop (group |)tacacs\+`

4.2.6 IOS - aaa accounting commands

Importance 5
For More Info See RSCG page 171 and RSCG page 175 for more information.
Rule Actions See section 4.1.8.
Rule Match `aaa accounting commands 15 (default |)start-stop (group |)tacacs\+`

4.2.7 IOS - aaa accounting network

Importance 5
For More Info See RSCG page 171 for more information.
Rule Actions See section 4.1.9.
Rule Match `aaa accounting network (default |)start-stop (group |)tacacs\+`

4.2.8 IOS - aaa accounting connection

Importance 5
For More Info See RSCG page 171 for more information.
Rule Actions See section 4.1.10.
Rule Match `aaa accounting connection (default |)start-stop (group |)tacacs\+`

4.2.9 IOS - aaa accounting system

Importance	5
For More Info	See RSCG page 171 for more information.
Rule Actions	See section 4.1.11.
Rule Match	aaa accounting system (default)start-stop (group)tacacs\+

4.2.10 IOS - aaa source-interface

Security Impact	This is required so that the aaa server (radius or TACACS+) can easily identify routers and authenticate requests by their IP address.
Importance	5
Rule Actions	See section 4.1.12.
Rule Match	ip tacacs source-interface Loopback\$(LOOPBACK_NUMBER)

4.2.11 IOS - One loopback interface must exist

Security Impact	The loopback interface provides a standard interface to be used in logging, time, routing protocols, and for ACLs limiting administrative access.
Importance	5
For More Info	See RSCG page 57 for more information.
Rule Actions	See section 4.1.14.
Rule Match	interface Loopback\$(LOOPBACK_NUMBER)

4.2.12 IOS - VTY transport SSH

Security Impact	Only permit protocols you intend to use. This prevents the other protocols from being mis-used.
Importance	5
For More Info	Note that many newer versions of IOS support SSH. SSH should be used instead of Telnet whenever possible. See RSCG page 64 and RSCG page 214 for more information.
Rule Actions	See section 4.1.18.
Rule Match	transport input ssh\$

4.2.13 IOS - apply VTY SSH ACL

Security Impact	VTY ACLs control what addresses may attempt to log in to your router.
Importance	10
For More Info	See RSCG page 64 for more information.
Rule Actions	See section 4.1.19.
Rule Match	access-class \$(VTY_ACL_NUMBER) in

4.2.14 IOS - define VTY SSH ACL

Security Impact	VTY ACLs control what addresses may attempt to log in to your router.
Importance	10
For More Info	See RSCG page 64 for more information.
Rule Actions	See section 4.1.20.
Rule Match	access-list \$(VTY_ACL_NUMBER) permit tcp \$(VTY_ACL_BLOCK_WITH_MASK) any access-list \$(VTY_ACL_NUMBER) permit tcp host \$(VTY_ACL_HOST) any access-list \$(VTY_ACL_NUMBER) deny ip any any log

4.2.15 IOS - clock timezone - localtime

Security Impact	Set the clock to local timezone. This ensures that it is possible to correlate logs.
Warning	If you manage devices in more than one timezone, consider using GMT.
Importance	3
For More Info	See RSCG page 134 for more information.
Rule Actions	See section 4.1.26.
Rule Match	<code>clock timezone \$(LOCAL_TIMEZONE) \$(TIMEZONE_OFFSET)</code>

4.2.16 IOS - require clock summer-time - localtime

Security Impact	Time should either use absolute GMT for adjust to the local timezone. This setting, along with local timezone settings, will cause the system clock to be set to the "normal" human-friendly local time.
Importance	5
Rule Actions	See section 4.1.27.
Rule Match	<code>clock summer-time \$(LOCAL_TIMEZONE) recurring</code>

4.2.17 IOS - ntp source

Security Impact	Set the source address to be used when sending NTP traffic. This may be required if the NTP servers you peer with filter based on IP address.
Importance	5
For More Info	See RSCG page 136 for more information.
Rule Actions	See section 4.1.29.
Rule Match	<code>ntp source Loopback\$(LOOPBACK_NUMBER)</code>

4.2.18 IOS - Defined loopback must be only loopback

Security Impact	Alternate loopback addresses create a potential for abuse, mis-configuration, and inconsistencies. Additional loopback interfaces must be documented and approved prior to use by local security personnel.
Importance	5
For More Info	See RSCG page 57 for more information.
Rule Actions	See section 4.1.30.
Rule Match	<code>interface Loopback(!\$(LOOPBACK_NUMBER))</code>

4.2.19 IOS - tftp source-interface

Security Impact	This is required so that the TFTP servers can easily identify routers and authenticate requests by their IP address.
Importance	3
For More Info	Note that this rule does not require the use of tftp. It simply requires that its source interface be bound. See RSCG page 57 for more information.
Rule Actions	See section 4.1.31.
Rule Match	<code>ip tftp source-interface Loopback\$(LOOPBACK_NUMBER)</code>

4.2.20 IOS - Apply ingress filter to 2nd IF

Security Impact	Apply the ingress filters to all external interfaces. This activates the defined ingress filters on the 2nd external interface.
Importance	7
For More Info	See http://www.ietf.org/rfc/rfc2827.txt . See RSCG page 87 for more information.
Rule Actions	See section 4.1.38.
Rule Match	<code>ip access-group \$(INGRESS_ACL_NUMBER) in</code>

4.2.21 IOS - Apply egress filter to second external IF

Security Impact	Apply the egress filters to second external interfaces. This activates the defined egress filters on the second external interface.
Importance	7
For More Info	It is an acceptable alternative to apply egress filters as input filters on all internal internal interfaces instead of as output filters on external interfaces. See http://www.ietf.org/rfc/rfc2827.txt . See RSCG page 87 for more information.
Rule Actions	See section 4.1.40.
Rule Match	<code>ip access-group \$(EGRESS_ACL_NUMBER) out</code>

4.2.22 IOS - require second external interface to exist

Security Impact	Generate a warning if the 2nd selected external interface does not exist.
Importance	1
Rule Actions	See section 4.1.42.
Rule Match	<code>interface \$(SECOND_EXTERNAL_INTERFACE)</code>

4.2.23 IOS - egress filter definition

Security Impact	This filter rejects outbound traffic with illegal source addresses. This includes any packets with a source other than a valid internal address. This usually indicates that something is mis-configured, or an attack is originating from within your network – either from a compromised host or a malicious user. Note that an egress ACL may be applied to either an external or an internal interface, when used with the appropriate access-group directive (in or out).
Warning	This rule assumes that you are on a "stub network", i.e. you are not providing transit for address ranges other than your internal netblock. Egress filters can stop legitimate traffic if the addresses are not set up correctly. (Note: when defining filters be aware that netmasks in Cisco ACLs are inverted, e.g. a /24 mask is specified as 0.0.0.255, not 255.255.255.0.) The implementation of this rule by the Router Audit Tool assumes that you have a single, contiguous internal netblock.
Importance	7
For More Info	See http://www.ietf.org/rfc/rfc2827.txt . See RSCG page 87 for more information.
Rule Actions	See section 4.1.43.
Rule Match	<code>access-list \$(EGRESS_ACL_NUMBER) permit ip \$(INTERNAL_NETBLOCK_WITH_MASK) any access-list \$(EGRESS_ACL_NUMBER) deny ip any any log</code>

4.2.24 IOS - Apply ingress filter

Security Impact	Apply the ingress filters to all external interfaces. This activates the defined ingress filters.
Importance	7
For More Info	See http://www.ietf.org/rfc/rfc2827.txt . See RSCG page 87 for more information.
Rule Actions	See section 4.1.45.
Rule Match	<code>ip access-group \$(INGRESS_ACL_NUMBER) in</code>

4.2.25 IOS - ingress filter definition

Security Impact	This rejects incoming traffic with illegal or internal source addresses. You should not receive external traffic with these addresses. If you do, either something is mis-configured or the sender is attempting to do something malicious.
Warning	Ingress filters can stop legitimate traffic if the addresses are not set up correctly. (Note: when defining filters, be aware that netmasks in Cisco ACLs are inverted, e.g. a /24 mask is specified as 0.0.0.255, not 255.255.255.0.)
Importance	7
For More Info	See http://www.ietf.org/rfc/rfc2827.txt . See RSCG page 87 for more information.
Rule Actions	See section 4.1.46.
Rule Match	<pre> access-list \$(INGRESS_ACL_NUMBER) deny ip 10.0.0.0 0.255.255.255 any log access-list \$(INGRESS_ACL_NUMBER) deny ip 127.0.0.0 0.255.255.255 any log access-list \$(INGRESS_ACL_NUMBER) deny ip 172.16.0.0 0.15.255.255 any log access-list \$(INGRESS_ACL_NUMBER) deny ip 192.168.0.0 0.0.255.255 any log access-list \$(INGRESS_ACL_NUMBER) deny ip \$(INTERNAL_NETBLOCK_WITH_MASK) any access-list \$(INGRESS_ACL_NUMBER) deny ip any 10.0.0.0 0.255.255.255 log access-list \$(INGRESS_ACL_NUMBER) deny ip any 127.0.0.0 0.255.255.255 log access-list \$(INGRESS_ACL_NUMBER) deny ip any 172.16.0.0 0.15.255.255 log access-list \$(INGRESS_ACL_NUMBER) deny ip any 192.168.0.0 0.0.255.255 log access-list \$(INGRESS_ACL_NUMBER) permit ip any any </pre>

4.2.26 IOS - Apply egress filter to first external interface

Security Impact	Apply the egress filters to first external interface. This activates the defined egress filters.
Importance	7
For More Info	As defined, this rule applies the egress filters applied to outbound traffic on the external interfaces. Depending on network topology, it is usually possible to achieve the same effect by applying a separate egress filter inbound on each internal interface. This would have the advantage of stopping the illegitimate traffic as close to the source as possible. This is an acceptable alternative way to implement this rule. (Even if filtering is applied to internal interfaces, it can still be useful to apply egress filtering on the external interfaces as well, because it can prevent routing loops. See http://www.ietf.org/rfc/rfc2827.txt . See RSCG page 87 for more information.
Rule Actions	See section 4.1.47.
Rule Match	<code>ip access-group \$(EGRESS_ACL_NUMBER) out</code>

4.2.27 IOS - require external IF to exist

Security Impact	Generate a warning if the selected external interface does not exist.
Importance	1
Rule Actions	See section 4.1.48.
Rule Match	<code>interface \$(EXTERNAL_INTERFACE)</code>

4.2.28 IOS 12 - apply unicast RPF

Security Impact	Unicast RPF verification rejects incoming packets with bad addresses and spoofed addresses.
Importance	5
For More Info	Unicast Reverse-Path Forwarding Verification is an IOS 12 facility that uses the route table to reject mis-addressed and spoof-addressed packets. Because it uses the route table Unicast RPF reacts automatically to network topology changes. See RSCG page 122 for more information. [trial]
Rule Actions	See section 4.1.51.
Rule Match	<code>ip verify unicast reverse.*</code>

4.2.29 IOS - no ip proxy-arp

Security Impact	Proxy arp breaks the LAN security perimeter, effectively extending a LAN at layer 2 across multiple segments.
Importance	5
For More Info	Network hosts use the Address Resolution Protocol (ARP) to translate network addresses into media addresses. Normally, ARP transactions are confined to a particular LAN segment. A Cisco router can act as an intermediary for ARP, responding to ARP queries on selected interfaces and thus enabling transparent access between multiple LAN segments. This service is called proxy ARP. Because it breaks the LAN security perimeter, effectively extending a LAN at layer 2 across multiple segments, proxy ARP should be used only between two LAN segments at the same trust level, and only when absolutely necessary to support legacy network architectures. Cisco routers perform proxy ARP by default on all IP interfaces. Disable it on each interface where it is not needed, even on interfaces that are currently idle, using the command interface configuration command: <code>no ip proxy-arp</code> . See RSCG page 74 for more information.
Rule Actions	See section 4.1.52.
Rule Match	<code>no ip proxy-arp</code>

4.2.30 IOS - tunnel interfaces must not exist

Security Impact	Tunnel interfaces should not exist in general. They can be used for malicious purposes. If they do exist, the network admins should be well aware of them and what their purpose is.
Warning	Be sure these interfaces do not have a legitimate use before removing them.
Importance	10
Rule Actions	See section 4.1.53.
Rule Match	<code>interface Tunnel</code>

A Other Information

A.1 How Benchmark Items Are Determined

A.1.1 CIS Level-I Benchmarks the prudent level of minimum due care

Level-I Benchmark settings/actions meet the following criteria.

1. System administrators with any level of security knowledge and experience can understand and perform the specified actions.
2. The action is unlikely to cause an interruption of service to the operating system or the applications that run on it.
3. The actions can be automatically monitored, and the configuration verified, by Scoring Tools that are available from the Center or by CIS-certified Scoring Tools.

Many organizations running the CIS scoring tools report that compliance with a CIS "Level-1" benchmark produces substantial improvement in security for their systems connected to the Internet.

A.1.2 CIS Level-II Benchmarks prudent security beyond the minimum level.

Level-II security configurations vary depending on network architecture and server function. These are of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the operating systems and applications running in their particular environments.

See <http://www.cisecurity.org/bench.html> for more information on how benchmarks are determined.

A.2 Understanding Technology, Risks and Your Organizational Goals

This Benchmark and related scoring are intended to be tools to assist in risk analysis and mitigation. The recommendations in the benchmark and tool should not be applied blindly and without thorough understanding of organizational goals and how technologies are applied to meet those goals.

For example, the benchmark recommends that you disable SNMP servers on IOS routers. While this will lessen risk for certain classes of SNMP-based attacks, your organization may rely on SNMP for monitoring its critical infrastructure (routers). Disabling SNMP may result in the devices being un-monitored. Leaving it enabled may result in a downtime due to an exploited vulnerability. You need to understand both the risks and the organizational needs.

A.3 Scoring and Scoring Tools

The benchmarks are designed to make it possible to compute an overall score for each system. This can be done manually or with the aid of a scoring tool. The Center for Internet Security provides free scoring tools which are available from <http://www.cisecurity.org>. There are also third party tools score systems per CIS guidelines.

Overall system scores are defined as follows

$$10 * \frac{ActualScore}{PotentialScore}$$

where

$$ActualScore = \sum PassingTests * IndividualTestImportance$$

and

$$PotentialScore = \sum AllTests * IndividualTestImportance$$

So, for example, if the benchmark contained exactly one rule, say “exec-timeout” requiring each serial line to timeout idle sessions, and the rule was assigned an importance of “5”, and there were three serial interfaces in the config (con,aux,vty), and the test showed that the rule had been applied on only one of the three, then the Actual Score would be 5 (1*5), the potential score would be 15 (3*5) and the overall system score would be 3.3 (10 * 5/15).

A.4 Credits

Many people and organizations have contributed to this document. Some of the many to whom thanks are due are:

- Jared Allison/MCI (nee UUNET)
- John Banghart/CIS,
- Phil Benchoff/Virginia Tech,
- Matt Guiger/DISA,
- Barry Greene/Cisco,
- Kenneth Grossman/FedCIRC,
- George Jones/The MITRE Corporation
- Bob Hockensmith/DISA,
- Clint Kreitner/CIS,
- Bert Miuccio,CIS,
- Karl Schaub/DISA,
- Donald Smith/Qwest,
- John Stewart/Cisco,
- Joshua Wright/Johnson & Wales University,
- Neal Ziring/NSA

Thanks to all who have contributed but were not listed. If you want to be listed in future revisions, send mail to rat-feedback@cisecurity.org. Inclusion in this list is intended only to acknowledge contributions, not to imply endorsement by the individuals or organizations listed.

B Example Configuration

The example below is an IOS router configuration that passes all of the CIS Benchmark level 1 and 2 rules for IOS 12. It is a border router, uses centrally managed AAA, multiple NTP servers, and unicast RPF. This example is not meant to be used on your router, it merely illustrates a configuration that passes all the benchmark tests.

```
!  
version 12.2  
service tcp-keepalives-in  
service timestamps debug datetime show-timezone msec  
service timestamps log datetime msec show-timezone  
service password-encryption  
!  
hostname upper  
!  
no ip bootp server  
!  
logging buffered 16000 informational  
logging rate-limit console 3 except critical  
logging console critical  
!  
username george password 7 022F25563B071C325B401B1D  
aaa new-model  
!  
aaa authentication login default group tacacs+ local enable  
aaa authentication enable default group tacacs+ enable  
aaa accounting exec start-stop group tacacs+  
aaa accounting commands 15 default start-stop group tacacs+  
aaa accounting network start-stop group tacacs+  
aaa accounting connection start-stop group tacacs+  
aaa accounting system start-stop group tacacs+  
aaa session-id common  
enable secret 5 $1$UKAW$u26UyV6TxGPtsgWqKdBL7.  
!  
memory-size iomem 10  
clock timezone GMT 0  
ip subnet-zero  
no ip source-route  
ip cef  
!  
!  
ip telnet source-interface Loopback0  
ip tftp source-interface Loopback0  
ip ftp source-interface Loopback0  
no ip domain-lookup  
!  
ip ssh time-out 120  
ip ssh authentication-retries 3  
!
```

```
call rsvp-sync
!
!
!
interface Loopback0
description local loopback interface
 ip address 14.2.63.252 255.255.255.255
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachable
 no ip proxy-arp
!
interface FastEthernet0/0
description Border router outside interface
 ip verify unicast reverse-path
 ip address 14.2.61.2 255.255.255.0
 ip access-group 100 in
 ip access-group 101 out
 no ip proxy-arp
 no ip mroute-cache
 speed auto
 half-duplex
 no cdp enable
!
interface FastEthernet0/1
 no ip address
 ip verify unicast reverse-path
 no ip proxy-arp
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
interface Ethernet1/0
description Border router inside interface
 ip address 14.2.62.2 255.255.255.0
 ip verify unicast reverse-path
 no ip proxy-arp
 no ip mroute-cache
 half-duplex
 no cdp enable
!
interface Ethernet1/1
 no ip address
 ip verify unicast reverse-path
 no ip proxy-arp
 no ip mroute-cache
```

B EXAMPLE CONFIGURATION

```
shutdown
half-duplex
no cdp enable
!
interface Ethernet1/2
no ip address
ip verify unicast reverse-path
no ip proxy-arp
no ip mroute-cache
shutdown
half-duplex
no cdp enable
!
interface Ethernet1/3
no ip address
ip verify unicast reverse-path
no ip proxy-arp
no ip mroute-cache
shutdown
half-duplex
no cdp enable
!
ip classless
no ip http server
ip pim bidir-enable
!
logging trap debugging
logging facility local6
logging 14.2.61.89
access-list 10 permit 14.2.62.0 0.0.0.127
access-list 10 deny any log
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
access-list 100 deny ip 14.2.60.0 0.0.3.255 any
access-list 100 deny ip any 10.0.0.0 0.255.255.255 log
access-list 100 deny ip any 127.0.0.0 0.255.255.255 log
access-list 100 deny ip any 172.16.0.0 0.15.255.255 log
access-list 100 deny ip any 192.168.0.0 0.0.255.255 log
access-list 100 permit ip any any
access-list 101 permit ip 14.2.60.0 0.0.3.255 any
access-list 101 deny ip any any log
access-list 182 permit tcp 14.2.62.0 0.0.0.127 any
access-list 182 permit tcp host 14.2.63.150 any
access-list 182 deny ip any any log
no cdp run
!
```

```
tacacs-server host 14.2.61.249 key blarg19-H57-02
!
dial-peer cor custom
!
!
!
!
!
line con 0
  exec-timeout 10 0
  password 7 022F25563B071C325B411B1D
line aux 0
  exec-timeout 10 0
  password 7 022F25563B071C325B411B1D
  no exec
line vty 0 4
  access-class 182 in
  exec-timeout 10 0
  password 7 022F25563B071C325B411B1D
  logging synchronous
  transport input ssh
!
ntp clock-period 17179916
ntp source Loopback0
ntp server 14.2.63.150
ntp server 12.168.140.2
ntp server 131.44.150.250
!
logging source-interface Loopback0
!
ip tacacs source-interface Loopback0
!
end
```

References

- [1] National Security Agency
NSA Router Security Configuration Guide
National Security Agency, 2002
<http://www.nsa.gov/snac/cisco/download.htm>
- [2] Thomas Akin
Hardening Cisco Routers
O'Reilly and Associates, 2002
<http://www.oreilly.com/catalog/hardcisco/>
- [3] Cisco Systems
Improving Security on Cisco Routers
Cisco Systems, 2002
<http://www.cisco.com/warp/public/707/21.html>
- [4] George M. Jones at al.
The Router Audit Tool and Benchmark
Center for Internet Security, 2002
<http://www.cisecurity.org>
- [5] John Stewart and Joshua Wright
Securing Cisco Routers Step-by-Step
The SANS Institute, 2002
<http://www.sans.org>
- [6] Rob Thomas
Guides to securing IOS, JunOS, BGP, DoS tracking, etc.
Rob Thomas, 2002
<http://www.cymru.com/robt/Docs/Articles/>
- [7] Elizabeth D. Zwicky, Simon Cooper and D. Brent Chapman
Building Internet Firewalls
O'Reilly and Associates, 2000
<http://www.ora.com/catalog/fire2/>