Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security improvement of a wide and heterogeneous set of network devices: a global approach

This case study describes the most interesting steps of a project to improve the security of a wide set (about one thousand) of network devices (switches, routers, firewalls) originated from many manufacturers. It is intended to describe a global approach which could be reused to tackle such situations. We will examine how to establish a security baseline through a network scan. Afterwards, we will estimate the risk on the organization induced by each family of network devices. This will provide the list of devices to ...

Copyright SANS Institute
Author Retains Full Rights

AD

Security improvement of a wide and heterogeneous set of network devices : a global approach

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 2 - Case Study in
Information Security

Submitted by: Jean-Marc MILLET
December 2004

SANS Conference : London June 2004

Paper keywords **:** network device, security, switch, router, firewall, configuration hardening, health checking, network scan, RAT, security checklist, best practices, security compliance, security indicator, risk assessment

© SANS Institute 2005 Author retains full rights.

© SANS Institute 2005 Author retains full rights.

1 ABSTRACT/SUMMARY

This case study describes the most interesting steps of a project to improve the security of a wide set (about one thousand) of network devices (switches, routers, firewalls) originated from many manufacturers. It is intended to describe a global approach which could be reused to tackle such situations.

We will examine how to establish a security baseline through a network scan. Afterwards, we will estimate the risk on the organization induced by each family of network devices, first in an intrinsic manner, and then according to the actual set of devices in the scope. This will provide the list of devices to secure in top priority.

State of the art tools and best practices in configuration security hardening are then studied. Cisco devices will be handled with an improved version of the Router Auditing Tool (RAT), Nokia firewalls through a security audit checklist, as no adequate tool has been found. Other types of devices will be handled by an ad hoc network scan, considered as the default control procedure. Other security aspects like user access management are also examined.

Security compliance indicators have been defined to measure the progresses towards more security and to report them management. They will contribute establishing the final state of security that we qualify as satisfactory. Finally we will outline remaining risks like value added servers (DNS, DHCP, Authentication) not yet controlled and new risks such as those induced by the use of security tools.

© SANS Institute 2005 Author retains full rights.

2 DOCUMENT CONTENT

Table of Contents

1 ABSTRACT/SUMMARY II
2 DOCUMENT CONTENT i
3 CURRENT CONDITION EVALUATION BEFORE STUDY 1
3.1 Current Security Posture 1
3.2 Problem Description 3
3.3 Current Risks 3
3.3.1 Risk assessment method 3
3.3.2 Devices configuration security baseline 6
3.4 Added value of SANS Training on the situation 8
4 ACTION PLAN 8
4.1 Proposed Solution 9
4.1.1 Problem analysis 9
4.1.2 Solution definition 11
4.2 Solution Implementation 13
4.2.1 Inventory 13
4.2.2 Configuration security hardening 14
4.2.3 Network scan improvement 17
4.2.4 Centralized access management 19
4.3 Added value of SANS Training 20
5 FINAL CONDITION EVALUATION AND FUTURE 20
5.1 Solution deployment 20
5.1.1 Security indicators 21
5.1.2 Solution validation 21
5.2 Risk Assessment 23
5.3 Added value of SANS Training 25
5.4 Conclusion 25
6 REFERENCES i
7 APPENDICES iv
7.1 Additional explanations on uncovered vulnerabilities iv
7.2 Generic security audit checklist vi
7.3 Nokia firewall security audit checklist xi
7.4 Cisco IOS and catOS RAT rules xvi

© SANS Institute 2005 Author retains full rights.

List of Figures

Figure 1 : ITCORP network logical topology 1
Figure 2: Network devices inventory as per family..... 13
Figure 3 : Cisco Secure Access Control Server functional architecture [] 19

List of Tables

Table 1 : Security baseline by network environment..... 7
Table 2 : Security baseline by vulnerability occurrence 8
Table 3: Security risk assessment as per device family..... 11
Table 4 : Weighted risk per device family 14
Table 5 : Network scan security indicators value 22
Table 6 : RAT IOS security compliance ratio evolution 23
Table 7 : Generic network device security audit checklist.....x
Table 8 : Nokia firewalls security audit checklist xv
Table 9 : Cisco IOS and catOS RAT rules.....xix

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

3 CURRENT CONDITION EVALUATION BEFORE STUDY

3.1 Current Security Posture

I am working at ITCORP, an international company whose main activity is Information Technology (IT) systems outsourcing. Enterprises who choose to concentrate on their core business delegate ITCORP the task to manage their computing resources on their behalf.
Figure 1 shows how ITCORP global network is split in different kinds of sub-networks in order to support its business.

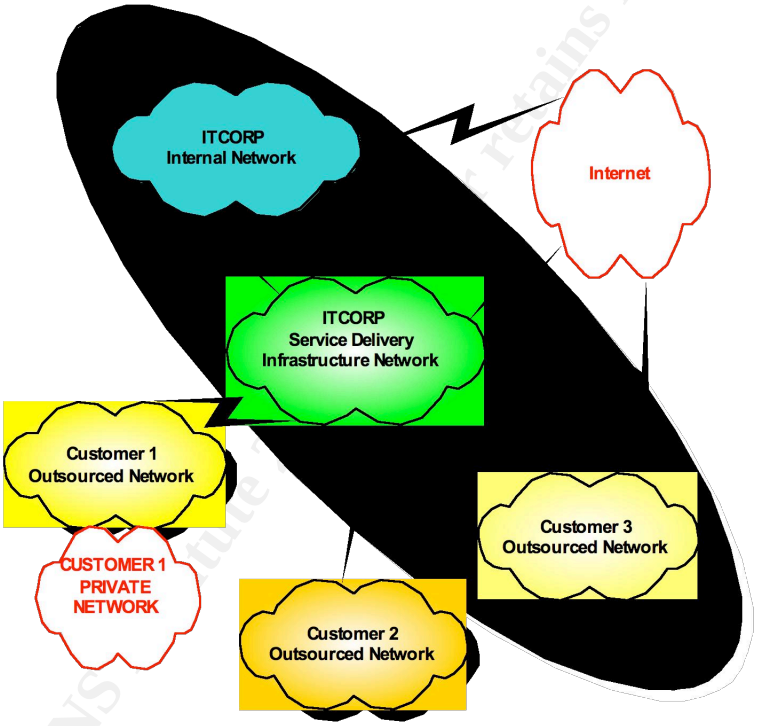

Figure 1 : ITCORP network logical topology

In summary, there are:

1. *ITCORP Internal Network*: it is the company intranet. It is not in the scope of this study as it is not directly related to outsourcing activities

© SANS Institute 2005 Author retains full rights.

2. *ITCORP Service Delivery Infrastructure Network*: it is a set of servers and network devices used to support outsourced customers. It provides the means and connectivity to perform remote administration of customer networks and provide them extranet or internet access in a secure way. Equipments such as network management stations or routers are common to several customers.
3. *Customer X Outsourced Network*: it is dedicated to customer X operations. This network can be located either in ITCORP premises (like Customer 3 Network) or customer X premises (like Customer 2 Network).
   In addition customer X may have kept a private part of its network under its own responsibility (like Customer 1 Network)
   Customer Outsourced Networks are connected to the Service Delivery Infrastructure Network, but they don't interoperate among them.

IT security is an important component of any outsourcing activity. To ensure that security rules are correctly enforced, ITCORP has internal teams of auditors reporting directly to the Chief Executive Officer, that he delegates regularly to all parts of its organization. Obviously, findings of such audits can not be ignored: their "recommendations" must be put in place quickly with no escape.

I was hired to put in place recommendations of a security audit on network devices, which happened in the ITCORP subsidiary of my country. In the long run, my job was to define and enforce the necessary controls to ensure that network devices were operated according to security policies. The management wanted to be in a better posture when the next audit would occur!

Indeed as outsourcing business in ITCORP has grown up quickly, network security was left a little behind. The focus has been put first on servers' security which was seen as more critical than network devices one. In the context of this paper, a network device is defined as an equipment providing network connectivity. This includes:

- Hub, Switches and Routers
- Nokia and Cisco PIX firewalls

But this excludes devices like printers and faxes and network value added servers like DNS or DHCP servers.

At the time I started my job, network devices managed by ITCORP were already operated according to some security guidelines. But as tools to control servers' security like Symantec Enterprise Security Manager ™ (ESM) [1] were largely deployed, nothing equivalent existed for network devices. ESM supports the most common operating systems in the server area like Windows, Linux, RedHat, Solaris, AIX but none in the network area like Cisco IOS, catOS, PIX or Nokia IPSO.

[1] Symantec Enterprise Security Manager ™

© SANS Institute 2005 Author retains full rights.

3.2 Problem Description

When I took the job, the situation was the following:

- ITCORP's subsidiary had 28 outsourced customers with a total of about 800 devices from many different manufacturers: Cisco Systems, IBM, Nortel, Hewlett-Packard, Nokia and BayNetworks.
- The main ITCORP audit findings were (associated risks will be discussed later on):
  - Network devices configuration security holes:

    For instance:
    - SNMP community strings (i.e. passwords) with trivial value (like "public", "private") or easily guessable (equal to customer or device name …).
    - Dangerous IP features like source routing enabled on routers.
    - Administrative services like SSH activated without a business need.
  - User access authorization to devices not correctly verified.
  - Unpatched software open to security vulnerabilities.
  - Lack of security controls:

    For instance:
    - Some devices were managed according to security best practices instead of ITCORP security policies.
    - Firewalls packet filtering rules were not regularly reviewed.
    - System logs retention time was not verified.
    - Security health checking procedures to ensure that devices were correctly configured with respect to ITCORP security policy did not exist.

3.3 Current Risks

We are going to look at the security risks which may be attributed to single network devices (i.e. routers, switches and firewalls as said earlier). But we will not address the risks associated to the network as a global entity, such as bad network security architecture or lack of intrusion detection systems, neither address physical security related issues.

3.3.1 Risk assessment method

I had to choose one of these two options:

© SANS Institute 2005 Author retains full rights.

1. Study exhaustively a representative sample of devices from which I may infer the overall security posture. Then define the complete path to reach a satisfactory level of security (i.e. match security policy).
2. Or choose the most important security potential issues and look for their appearance on all the devices.

The second approach doesn't give a comprehensive picture of the activities to plan, but it has the advantage of allowing quickly a huge security improvement by identifying and closing the most severe security holes.

A *network scan* is the cheapest way to proceed to address weak configuration and obsolete software level problems. *User access management* risks will be examined by a manual review.

Network scan vulnerabilities

I could have used Nessus [2] vulnerability scanner, but as ITCORP has developed a similar scanner of its own, this one was chosen. There was no need to discover the devices plugged on the network as they were listed in the commercial contracts. ITCORP scanner was configured to search for these severe security vulnerabilities:

- **TFTP server enabled**: Trivial File Transfer Protocol (UDP port 69) allows transferring files from or to a host. It is often used by network devices as it is easy to implement and requires few memory space. Configuration files or software images may be uploaded or downloaded through it. From a security point of view, it is very dangerous as it requires no authentication at all (no password, no host authentication)
- **Diagnostics services enabled**: Also known as TCP/UDP small services because they correspond to low numbered ports, they may be used for denial of services attacks and must be disabled. The main diagnostics services are :
  - Echo (TCP/UDP port 7)
    According to Cisco Router and Security Device Manager User's Guide [3] :
    > *An attacker might send a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the router's UDP echo port, the result would be the router sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered to be locally generated by the router itself.*
    A denial of service condition could arise on the server.
  - Chargen (TCP/UDP port 19)
    Character Generator is a protocol generating characters on the network in

[2] Nessus
[3] Cisco Router and Security Device Manager User's Guide, Chapter 16 page 7

© SANS Institute 2005 Author retains full rights.

order to test it. It dates from the early days of the Internet.
According to CERT® Advisory CA-1996-01[4]:

> *By connecting a host's chargen service to the echo service on the same or another machine, all affected machines may be effectively taken out of service because of the excessively high number of packets produced. In addition, if two or more hosts are so connected, the intervening network may also become congested and deny service to all hosts whose traffic traverses that network*

Chargen permits denial of service attacks and as it is no longer used, it must be disabled.

- ⇨ Discard (TCP/UDP port 9)
  When a discard/UDP server receives a packet, it just throws it away. No answer is returned. An attacker can use this service to waste the network bandwidth.
- ⇨ Daytime (TCP/UDP port 13)
  Daytime is used to give the local time of the day. The date format issued by this service may help an attacker guess the operating system version of the device, or set up timed authentication attacks against it. In addition, with the UDP version of daytime, an attacker may link it to the echo port of a third party host using spoofing, thus creating a possible denial of service condition between this device and the third party.

- **Trivial SNMP community string:** Simple Network Management Protocol (specified in RFC 1157) may be used to monitor and manage network devices from a centralized station. Information such as link operation or CPU load may be got from the device. Configuration changes may be ordered from the SNMP manager. The monitored device may also generate unsolicited messages, called traps, towards the manager.

  The SNMP community string is the password used by the SNMP manager to read or write information into the device configuration or system files (MIB). Many devices are shipped by the manufacturer with default community strings such as "public", "private", "secret", "cisco" and not changed later on.

  Note that SNMP community strings as well as traffic are not encrypted prior to SNMP v3 version, which is not yet widely spread.

  By using a dictionary, the network scan can probe if a device uses these default or trivial passwords.

- **Telnet/FTP trivial password:** As with SNMP community strings, telnet and FTP passwords may be tested against a set of values contained in a dictionary.

- **Both telnet and SSH activated:** telnet (TCP port 23) and SSH (TCP port 22) are protocols used to remotely administrate devices.

[4] CERT Advisory CA-1996-01

© SANS Institute 2005 Author retains full rights.

Secure Shell (SSH) is a secure replacement for the UNIX remote copy (rcp), remote shell (rsh) and remote login (rlogin) utilities. The entire SSH session is encrypted, including the transmission of user names and passwords, using methods of encryption defined by negotiation between the SSH client and server. In the contrary, telnet is an unsecured protocol which provides no encryption at all, even for the passwords.

If SSH is activated on a device, telnet is then not necessary and must be disabled.

- **Vulnerable software version**: as a vulnerability scanner, ITCORP scanner is able to test the target against a library of know vulnerabilities. If the software is up to date, the target should not respond positively to these tests.

  Special mention must be made to "buffer overflows" tests: as I tuned the scanning procedure against a few number of devices, it appears that some Cisco IOS devices were brought out of service and have to be rebooted. This was due to an unpatched buffer overflow vulnerability in the SNMP message handling [5].

  A buffer overflow may arise when the input parameters of a program are not correctly checked and their size is greater than the buffer reserved to contain them. This makes it possible to execute malicious instructions on the device or generate a denial of service. A detailed explanation of buffer overflow mechanism can be found in Russell's book [6].

  As it was probable that software version of other network devices were also vulnerable to this SNMP buffer overflow vulnerability and as the purpose was not to perform a full penetration test, I decided to deactivate buffer overflows checks.

Access Management vulnerabilities

Access management related risks have been evaluated by reviewing the user accounts. As it is traditionally the case for network devices, only one account for telnet logging is defined per device. This account is shared among the many devices administrators. Indeed to make its outsourcing business profitable, ITCORP must make common its support staff for the different customers, as it does for its infrastructure network. This staff may even be ITCORP subcontractors with a quick turn-over.
This operating mode has two main drawbacks:

1. No individual accounting for device access is possible, preventing any serious investigation in case of incident.
2. The shared account password must be changed each time somebody leaves the support staff, which is an additional burden to manage.

3.3.2 Devices configuration security baseline

Network scan results have been analyzed in two ways to establish the security baseline:

[5] Cisco Security Advisory 19294
[6] Russell, p185-187

© SANS Institute 2005 Author retains full rights.

1. By network environment to identify the networks to secure first
2. By vulnerability to determine the most frequent one

Scan results as per network environment

Table 1 shows as per network environment:

- The number of devices which have been scanned.
- The number of security rules which have been violated.
- A security compliance ratio which is the ratio between the number of passed rules versus the number of tested rules.

Customer	Scanned devices number	Total violated rules number	Security compliance ratio
CUSTOMER-B2	2	0	100%
CUSTOMER-B3	26	0	100%
CUSTOMER-D1	12	0	100%
CUSTOMER-D2	2	0	100%
CUSTOMER-F1	4	0	100%
CUSTOMER-G1	2	0	100%
CUSTOMER-J1	6	0	100%
CUSTOMER-L1	1	0	100%
CUSTOMER-R1	2	0	100%
CUSTOMER-S1	2	0	100%
CUSTOMER-S3	2	0	100%
CUSTOMER-S4	2	0	100%
CUSTOMER-S6	124	0	100%
CUSTOMER-T1	2	0	100%
CUSTOMER-T2	12	0	100%
CUSTOMER-T3	8	0	100%
CUSTOMER-V2	2	0	100%
CUSTOMER-C1	57	4	99%
CUSTOMER-M1	140	9	99%
INFRA-S	41	2	99%
CUSTOMER-S5	34	2	99%
INFRA-U	46	2	99%
INFRA-E	34	4	98%
CUSTOMER-F2	15	2	98%
CUSTOMER-S2	10	2	97%
CUSTOMER-V1	3	1	94%
CUSTOMER-B1	202	134	89%
CUSTOMER-A1	2	2	83%
SUM : 28	795	164	96%

Table 1 : Security baseline by network environment

© SANS Institute 2005 Author retains full rights.

A network with a compliance ratio different than 100% is really in jeopardy since only the most severe vulnerabilities were probed and all networks are in production.

Scan results as per vulnerability :

Vulnerability name	Number of devices	Percentage of devices
TFTP server enabled	20	3%
Diagnostics services enabled	2	0,3%
Trivial SNMP community string	143	**18%**
Telnet/FTP trivial password	1	0,1%
Both telnet and SSH activated	1	0,1%
Vulnerable software version	1	0,1%

Table 2 : Security baseline by vulnerability occurrence

Trivial SNMP community string is the most common vulnerability, which is rather good news as it may be easily corrected.

3.4 Added value of SANS Training on the situation

I started this work before I attended the SANS training, but it help me better understand the problems afterwards. Especially the following topics covered during the course:

- Networking Concepts: IP concepts, Routers, IOS.
- Defense in Depth
  - Threat and vulnerabilities.
  - Security Policies.
  - Password management.
  - Access control.
- Internet Security technologies
  - Vulnerability scanning – Nessus.

4 ACTION PLAN

After this first security assessment, I had to deepen the subject.

© SANS Institute 2005 Author retains full rights.

- Discovered configuration vulnerabilities have obviously to be corrected. The next step was to refine the point of controls and industrialize the security control process.
- The user access management lack of security, as it was related to the way device administration is performed, could not be addressed immediately.

4.1 Proposed Solution

4.1.1 Problem analysis

Let's summarize the problem:

1. Discovering the boxes plugged on the network is not necessary: the scope consists of managed network devices, which are listed in an inventory.
2. A scalable solution is necessary: the point is not to strengthen one device so that it becomes an impregnable bastion, but to bring at a satisfactory level of security a lot of network device models representing hundreds (and tomorrow thousands) of boxes.
3. Prioritization is needed as all can not be handled simultaneously. Therefore security risks have to be assessed.

Risk assessment

According to the National Institute of Standards and Technology (NIST) [7]:
"Risk is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability* and the resulting *impact* of that adverse event on the organization".
This may be summarized as:

Risk = Threat*Vulnerability*Impact

I evaluated the equation parameters in the following way in order to keep a "macroscopic" approach. This is obviously somehow arbitrary.

- **Threat**: Three levels are possible according to the visibility of the device:
  - ⇨ Firewall: high as a firewall is highly visible, being the first layer in a defense in depth strategy.
  - ⇨ Router: medium as it is an IP addressable element.

[7] NIST Special Publication 800-30, p14

© SANS Institute 2005 Author retains full rights.

- ⇨ Switch or hub: low as it is normally an OSI layer 2 device not addressable through IP.

- **Vulnerability**: It is measured by the probability of discovering a vulnerability on a given device model. This may be estimated by compiling all the advisories published during a certain period of time. A site like SecurityFocus™ Bugtraq [8] which publishes all known vulnerabilities may be used. It shows that Cisco advisories frequency is far more important than the one for other switches and routers. Same for Nokia firewalls with respect to other types of firewalls.

  Two levels are retained:

  - ⇨ Cisco or Nokia devices: high.
  - ⇨ Other devices: low.

- **Impact**: It is necessary to split the switches family according to the device function in the network. According to Cisco's Internetwork Design Guide [9] classification:

  - ⇨ A core switch is a switch with routing capabilities. It is at the centre of the network topology.
  - ⇨ An access switch provides connectivity to end users.
  - ⇨ A distribution switch is in between.

  Using a three levels scale for measuring impact:

  - ⇨ Firewall: classified as high as web access or network segmentation may be compromised by an attack.
  - ⇨ Router, core switch: classified as medium as a large part of the network may be impacted, but alternate routes may often be used due to the redundant nature of an IP network.
  - ⇨ Access switch or distribution switch or hub: classified as low as only a limited part of the network is impacted.

Table 3 shows the resulting risk values computed from the preceding assumptions. A "high" level value is 3, a "medium" level is 2 and a "low" level is 1.

[8] Bugtraq
[9] Cisco Internetwork Design Guide, Chapter 2 p4

© SANS Institute 2005 Author retains full rights.

Family	Threat	Vulnerability	Impact	Risk
Firewall : Nokia or Cisco	3	3	3	27
Router : Cisco	2	3	2	12
Core switch : Cisco	1	3	2	6
Router : not Cisco	2	1	2	4
Distribution or Access switch or Hub : Cisco	1	3	1	3
Core switch : not Cisco	1	1	2	2
Distribution or Access switch or Hub : not Cisco	1	1	1	1

Table 3: Security risk assessment as per device family

4.1.2 Solution definition

The main idea behind the action plan was that it was necessary to have a precise knowledge of the actual set of network devices. Combining this knowledge with those of the risks associated to a device family will help determine in which order to start securing the boxes. Another direction was that it was interesting to spend some time to search for any existing method or tool on the matter, in order to integrate them in the global solution.

1. **Inventory**

   Build an inventory of all network devices in the scope, showing a detailed classification as per

   ⇨ Device type (router/switch/firewall).

   ⇨ Device family (Cisco switch, Nokia firewall …).

   ⇨ Device model (Cisco switch 3550, Nokia Firewall IP530 …).

   This is necessary to put in perspective the risk assessment per device family given by Table 3 and the proportion of the corresponding family in the set of devices managed.

2. **Existing security tools and best practices**

   Investigate the existing tools and "best practices" documents describing ways to harden network devices configuration from a security viewpoint.

3. **Security audit checklists**

   A checklist is an efficient mean to formalize a text document describing rules such as a security policy.

   a. First, a security audit generic checklist has to be developed for each type of network devices (router, switch and firewall).This will be achieved by mapping the relevant ITCORP security policy into precise network security criteria.

      These checklists will contain a set of:

      ⇨ Rule names: for instance "unneeded services".

© SANS Institute 2005 Author retains full rights.

- ⇨ Rule objectives: for instance "check that unneeded services are deactivated".
- ⇨ Expected result: for instance "diagnostics services, finger, bootp must all be disabled".

b. Then this generic checklist has to be declined into specific one for each device model. Prioritization of this activity will depend on risk assessment (Table 3) and inventory split per device model. The purpose is to give the precise action to perform to check one criterion according to the device family: checking that unneeded services are disabled is not performed in the same way on a Cisco PIX or a Nokia IPSO firewall.

These specific checklists will contain a set of:

- ⇨ Rule names : for instance "unneeded services"
- ⇨ Actions to perform to verify the rule : for instance "Using Nokia Firewall Management Voyager summary web page – Network Access and Services section"
- ⇨ Expected results : for instance "Echo, discard, chargen, daytime, time services are all disabled"

4. Network scan

Improve the network scan security criteria to address less severe vulnerabilities than previously. The intended purpose is to use network scan as a "default" procedure to audit device models which will not be handled through other means (automatic tools, checklists).

5. Security advisories

A process was already in place to follow security advisories publication for servers and the resulting software upgrades on the machines. This had just to be extended to network devices.

6. Centralized Access Management

By default, Cisco devices maintain one password to log onto the device with limited rights (line password) and a second password with full privileges to access to configuration commands (enable access). Individual user accounts may also be created on Cisco devices as they may on Nokia firewalls.

In large-scale environments as it is the case in ITCORP, it is cumbersome to synchronize and maintain individual user accounts on each device. It is the reason why very often, a unique shared administrative account is defined and used by every administrator.

To simplify account management, these devices can be configured to authenticate the users with the help of a central authentication server. This also will remove usernames and passwords from local configuration files increasing security.

7. Indicators and reporting

© SANS Institute 2005 Author retains full rights.

Simultaneously with the technical developments, it is necessary to define and put in place indicators to measure the progresses and the remaining gap to reach a full satisfactory situation.

4.2 Solution Implementation

4.2.1 Inventory

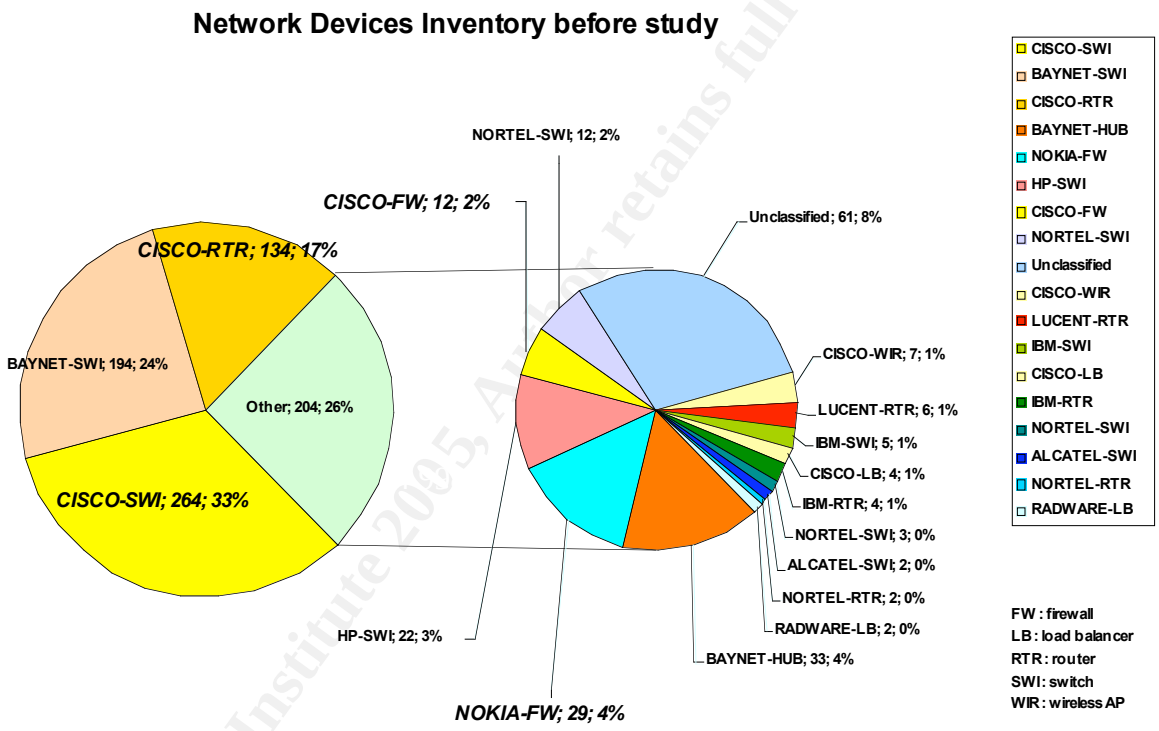

Figure 2: Network devices inventory as per family

(Unidentified models were unknown due to inventory inaccuracy at the time of the study)

Combining Table 3: Security risk assessment as per device family and Figure 2: Network devices inventory as per family, it is possible to estimate a *weighted risk* for the real set of network devices which we have to cope with.

© SANS Institute 2005 Author retains full rights.

Taking a statistical approach, the risk brought to the organization by a device family is proportional to its intrinsic risk (Table 3) times its proportion in the actual inventory (Figure 2). An intrinsic high risk brought by a family has less chance to materialize if the corresponding family is not widespread and vice-versa. Results are displayed in Table 4 for the most widespread families in the scope.

Family name	Family proportion (%)	Intrinsic risk (Table 3)	Weighted risk
Cisco routers	17	12	204
Cisco switches	33	6 or 3	198 or 99
Nokia firewalls	4	27	108
Cisco firewalls	2	27	54
Bay Networks switches or Hub	28	1	28

Table 4 : Weighted risk per device family

Setting priorities, Cisco routers and switches have to be handled first, along with Nokia and Cisco firewalls. For these equipments, we will examine how to strengthen the security controls. Other equipments will continue being controlled with a network scan for the time being.

4.2.2 Configuration security hardening

Existing tools and best practices

Some tools exist to audit network devices configurations:

- Router Auditing Tool (RAT) which is the reference tool, available from the Center for Internet Security [10]. It has been described in many publications such as Stewart's one [11]. It supports Cisco IOS routers and now Cisco PIX firewalls.
- CROCODILE® (Cisco Router Configuration Diligent Evaluator) is a commercial tool for Cisco IOS routers from the Fraunhofer IESE [12]. It may be seen as a "sophisticated" RAT.

Both tools are based on string pattern analysis from a device configuration file. A set of security rules is defined, each rule being associated to the presence or absence of keywords. Depending on whether these keywords are present or not in the configuration file determine if the rule is passed or failed.

[10] Center for Internet Security RAT
[11] Stewart, Brian
[12] Fraunhofer IESE CROCODILE®

© SANS Institute 2005 Author retains full rights.

I choose the Router Auditing Tool for Cisco devices as it appeared easier to adapt, to fit our needs. I did not find any equivalent tool to audit Nokia firewalls: that's why I took the security checklist approach.

Best practices publications on network devices configuration security hardening (sometimes also called security health checking) are numerous. Let's quote the one which were of the greatest help for me:

- Cisco Systems: Security best practices for configuring a router [13]
- National Security Agency: Router security configuration guide [14]
- National Security Agency: Cisco IOS switch security configuration guide [15]
- Strassberg et al book [16]
- Llorens, Levier's book [17]
- Malik's book [18]

Security audit checklists

With the help of the above documentation, the generic network device security audit checklist was built in accordance to ITCORP security policy. It is applicable to a hypothetical network device being simultaneously a router, a switch and a firewall. It contains:

- The name of the rule ("Rule name")
- The rule family ("Rule family").This defines a classification (alphabetic order) :
  - Administrative access security.
  - Software image version.
  - Packet filter rules security.
  - Network services security.
  - Passwords.
  - SNMP security.
  - Syslog : logging of system messages.
  - Unused ports disabling.
  - User authentication.
- The domain of applicability ("Applicable on") :
  - A "common" rule is not dependent on the device type.

[13] Cisco Systems
[14] NSA Router Security Configuration guide
[15] NSA Switch Security Configuration Guide
[16] Strassberg chapter 4 p6-15
[17] Llorens, Levier p148-159
[18] Malik p54-78

© SANS Institute 2005 Author retains full rights.

- ⇨ A "Router (rtr) ", "Switch (sw)" or "Firewall (fwl)" rule applies only on the corresponding device.
- The rule objective ("Rule objective") details its purpose.
- The criteria to be met ("Expected result") to consider the rule as being fulfilled.

A total of 44 security rules have been defined as shown in Table 7 in Appendix 7.2.

Nokia firewalls audit checklist

The generic audit checklist has then been refined in a specific checklist for Nokia firewalls with the additional help of Naidu [19] and Tu [20] work, and ITCORP colleagues specialists in firewall administration.

The action to take to verify a rule and the expected result to be compliant have been detailed so that it becomes straightforward for a non specialist to fill the checklist. Most actions consist in checking through the Nokia Voyager interface that some parameters are correctly set.

The result is shown in Table 8 in Appendix 7.3

RAT improvement

After evaluating the Router Auditing Tool, it was found that modifications and improvements were mandatory for the tool to match our needs. We will only outline them below, as it is not the purpose of this paper to go into the detail of each one and how it was realized: a Cisco specialist with software development skills was hired to do this job.

Four topics needed improvement:

- **The user interface**: The command line interface was replaced by a web style interface with the RAT tool bundled with a web server.
- **New functionalities**: Some miscellaneous functions like audit reports archiving were added, but the main one was the capability to define exceptions to security rules on a device or customer basis.

  This is necessary as security policies may differ from one customer to another according to the customer specific needs. So the generic security checklist is considered as the reference (most secure policy) and no customer commitment may be taken for more security. All deviations from this policy are handled as exceptions and do not appear in the RAT report. Otherwise said, a 100 % RAT compliant device shows no deviations from the security checklist except for the rules in exception which may or may not be passed.

[19] Naidu
[20] Tu

© SANS Institute 2005 Author retains full rights.

- **New rules**: Available RAT rules set for Cisco IOS have to be modified. From the original set of 67 RAT rules (at that time) for benchmark 1 and benchmark 2, 30 were kept with 12 modified, and 13 new one were added. So the total is 43 points of control for Cisco IOS devices.
- **New operating system support**: Due to the large proportion of Cisco catOS devices, it was necessary to add support for them with the development of 14 rules. Cisco Pix support was also added with 23 points of control.

Table 9 in appendix 7.4 shows the set of RAT rules used for Cisco IOS and catOS boxes and their mapping against the reference security checklist.

4.2.3 Network scan improvement

I have extended the network scan control points with the intent to cover all possible security checks from a scan, within the frame of the generic security checklist. Hereafter is the new list.

1. Unneeded services

Keeping enabled unneeded TCP/UDP/ICMP services on the devices presents three main security risks:

a. It is often a mean to gather information about the device.
b. It may be used to launch denial of service attacks.
c. Even if not known vulnerability is present, nothing prevents one to be discovered tomorrow and exploited before you have time to patch the software.

The presence of the following unneeded services is checked:

- *TFTP server:* Should be disabled as already explained (See page 4)
- *Diagnostics services*: Should be disabled as already explained (See page 4)
- *Both telnet and SSH activated*: Telnet should be disabled as already explained (See page 4)
- *Finger service*: The finger service (TCP port 79) can be queried to obtain the list of users logged on the device. This may be interesting information for an attacker which can then use it as a starting point to try to crack passwords. Finger service should be disabled.
- *Bootp service*: The bootp service (UDP port 67) is used to allow other devices to boot from this one. For instance, a Cisco router may act as the central repository for IOS software. An attacker connecting to this router may obtain a copy of the IOS software, giving him knowledge of the software run by its target. Bootp service should be disabled if no business need.
- *ICMP address mask reply and ICMP timestamp reply*: the Address Mask Request ICMP query message allows a device to ask another for the subnet mask in use on

© SANS Institute 2005 Author retains full rights.

the local network. Sending an ICMP address mask reply gives information about network sub-netting, and hence network topology. ICMP address mask messages are now somewhat obsolete.

Nowadays, ICMP timestamp messages are no longer used to synchronise a network as Network Time Protocol (NTP) is the preferred solution. Moreover, replying to an ICMP timestamp request informs about the local clock value, from which some internal algorithms such as encryption may be based.

In addition these ICMP messages replies may be used to fingerprint the operating system as shown by the Sys-Security Group [[21]]. It is the reason why they should be disabled on interfaces to untrusted networks.

Note that ICMP echo reply messages are not forbidden as they may be used for network administration purpose. But ICMP echo request and reply messages must be dropped at the network boundary as they may be used by attackers to detect available devices.

- *FTP server and HTTP servers*: devices may be configured to act as FTP (TCP port 21) and as HTTP (TCP port 80) server for administration purpose. As these services are potentially dangerous, their use must correspond to a real business need where no alternative is possible. Else they must be disabled.
- *Domain Name Services* (DNS): DNS service (TCP/UDP port 53) must not be started on the device, except if its function is to be a DNS server.
- *SNMP services*: SNMP trap catcher service (UDP port 162) must not be started on the device.
- *Rexec, Rlogin and Rsh services*: the so called "Unix R-commands" allow to log or execute commands remotely on a system. They were created at the genesis of the Internet with no security concern in mind. For instance the rlogin protocol uses a trusted relation and privileged ports between two hosts so that the user remote login may proceed without further authentication. Theses services (TCP port 512, 513 and 514) must be disabled on network devices.
- *Syslog server:* Syslog is a logging and auditing mechanism coming from the UNIX world. System log messages generated on a device may be kept locally or forwarded to a remote host acting as a syslog server (UDP port 514). Syslog server must be disabled on network devices.
- *Telnet server on firewall*: firewall administration should be done only through secure protocols such as SSH (TCP port 22) or HTTPS (TCP port 443). Telnet service (TCP port 23) must be deactivated on firewalls.

2. Trivial or no password

- *Trivial SNMP community string* : already explained page 4
- *Telnet/FTP trivial password* : already explained page 4

[21] Sys-Security Group

© SANS Institute 2005 Author retains full rights.

3. Uncorrected software image vulnerability

- *Software image vulnerability* : already explained page 4

4. Welcome banners

When a user logs on the device, a welcome banner has to be displayed. It must:

- Contain a business use notice of the system to deter unintentional access (exact content depends on the country).
- Not reveal information on the device itself such as device model, software version …

4.2.4 Centralized access management

Two main authentication protocols are used in the network world: Radius and Tacacs+. Radius is the de facto industry standard specified in RFCs 2865 and 2866 whereas Tacacs+ is Cisco solution, but is widely supported by non Cisco devices.

The choice of the solution was done by administrative staff as it has operational impacts, but I have to validate the solution as being the security representative. This solution was the Cisco Secure Access Control Server (or ACS server). The Cisco ACS server offers three main functionalities:

1. **A**uthentication: Verification of user identity by means of a username and password.
2. **A**uthorization: Restriction of user access to authorized resources according to its profile.
3. **A**ccounting: Logging of user activity on the device.

It's the reason why this server is also called "ACS AAA server". Figure 3 shows the functional architecture of the Cisco ACS solution.

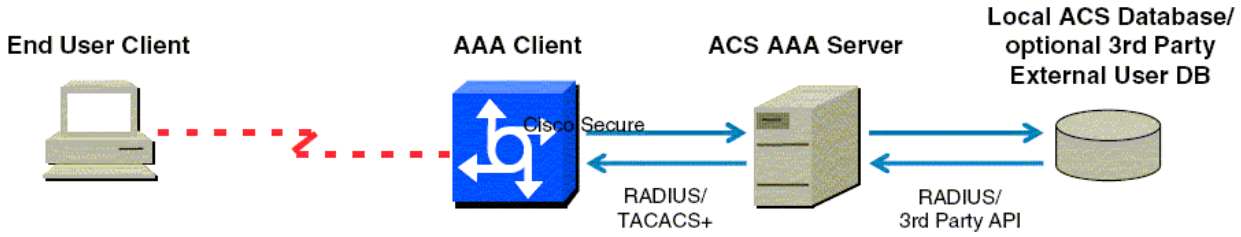

Figure 3 : Cisco Secure Access Control Server functional architecture [22]

When an end user client wants to sign on a network device named "AAA client", it establishes a connection (SSH, telnet, dial-up) to the device and is prompted to enter its

[22] Cisco ACS Chapter 2 page 29

© SANS Institute 2005 Author retains full rights.

username and password. Theses parameters are transmitted by the AAA client to the AAA server. The later *authenticates* the user by querying its local user database or an external one. It then returns a positive response to the AAA client along with session attributes such as user privileges (*authorization*). The positive response is sent back to the end user client, allowing it to connect to the device. Each time it will send a command to the network device, this one will send an *accounting* record to the AAA server.

From a security standpoint, this solution is fully satisfactory for the following reasons:

- User accounts and passwords management are centralized, which facilitate their control.
- Primary authentication information like userids and passwords are not stored locally on device memory.
- Authentication is performed by username AND password (not just VTY enable password on Cisco devices).
- Shared accounts among several administrators may be limited to only one. This single account is defined locally on the network device and must only be used in case of AAA server failure.
- Passwords are encrypted all along their network travel from the AAA client to the AAA server (but not necessarily from the end user client to the AAA client if a connection protocol likes telnet is used!)
- Commands entered by the end user are logged on the AAA server allowing an investigation in case of incident.

4.3 Added value of SANS Training

The main topics from the SANS Security Essential course I used to write this chapter in addition to the one previously mentioned were:

- Defense in Depth
  - Relation between risk, threat and vulnerability
- Internet Security technologies
  - Attack strategies and mitigation
  - Firewalls

5 FINAL CONDITION EVALUATION AND FUTURE

5.1 Solution deployment

The deployment of the solution consisted in putting in place the security controls described in the previous chapter. Considering that about one thousand devices were now in the scope, the participation of the administrative staff to run the network scans,

© SANS Institute 2005 Author retains full rights.

provide the Cisco configuration files and fill the security audit checklists was necessary. The control tasks of analyzing the scan reports, generating the RAT audit files and validating the security audit checklists was shared with other members of the security team.

5.1.1 Security indicators

To measure progresses and report it periodically to management, I had to put in place indicators. Some are in relation with the size of the controlled perimeter to measure the progression of the activity, while the other reflect a security compliance level. The following indicators were defined:

1. Activity progression:
   - ⇨ Number of devices in scope to check (targeted devices).
   - ⇨ Number of devices in scope checked (audited devices).
2. Security compliance:
   - ⇨ Number of devices for which security vulnerabilities have been found (non compliant devices).
   - ⇨ Number of violated security rules.
   - ⇨ Security compliance ratio: a severity (number) may be associated to each security rule to weight its importance. The compliance ratio is defined as the ratio of the weighted sum of security rules passed, versus the same sum if all rules were passed successfully (100 % indicates full compliance).

5.1.2 Solution validation

Network scan

Table 5 shows the evolution of the security indicators value for the network scan, between the time the project was started (795 devices) and the time this study was written (950 devices).

Vulnerability name	First assessment		Final assessment	
	Number of devices	% of devices	Number of devices	% of devices
TFTP server	20	3%	4	0,4%
Diagnostics services	2	0%	1	0,1%
Both telnet and SSH activated	1	0%	2	0,2%
Trivial SNMP community string	143	18%	9	0,9%
Telnet/FTP trivial password	1	0%	0	0,0%
Vulnerable software version	1	0%	2	0,2%
Finger service	Not tested		1	0,1%
Bootp service	Not tested		0	0,0%

© SANS Institute 2005 Author retains full rights.

ICMP replies	Not tested		2	0,2%
HTTP server	Not tested		0	0,0%
FTP server	Not tested		0	0,0%
DNS service	Not tested		0	0,0%
SNMP service	Not tested		0	0,0%
Rexec, Rlogin, Rsh services	Not tested		6	0,6%
Syslog server	Not tested		0	0,0%
Telnet server on a firewall	Not tested		0	0,0%
Welcome banners	Not tested		0	0,0%
Indicators				
Targeted devices	795		950	
Audited devices	795		950	
Devices with found vulnerabilities	163	21%	21	2%
Number of security rules violated	168	3,5 %	26	0,15 %
Security compliance ratio		96,5%		99,84%

Table 5 : Network scan security indicators value

(Severity of all rules identical)

Only the final security state is displayed. Several intermediate scans were performed and the corresponding findings corrected in between.

During this period, it is to be noticed that the scope of devices increased due to the arrival of new ITCORP customers. At constant perimeter, the security compliance ratio would have been near 100%. Nevertheless the result is rather satisfactory.

RAT and checklists on Cisco and Nokia devices

Table 6 shows the evolution of the security compliance ratio for Cisco devices running under IOS and audited with RAT. Results for Cisco catOS audited are similar. The Nokia or PIX firewall auditing results by means of the security checklists are also identical.

© SANS Institute 2005 Author retains full rights.

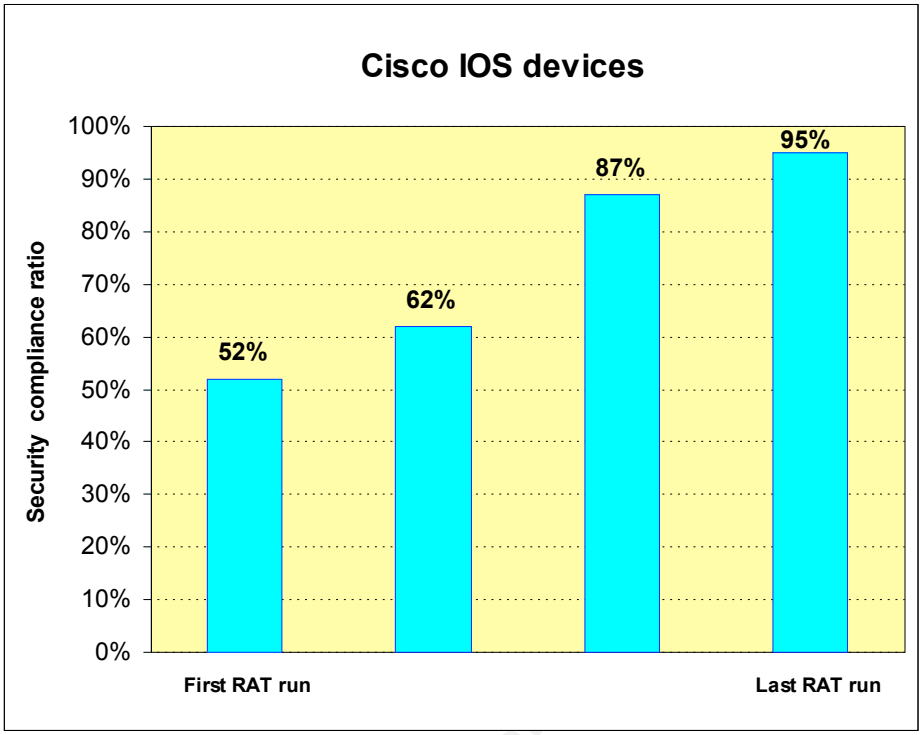

Table 6 : RAT IOS security compliance ratio evolution

User access management

When running RAT on Cisco device configurations or the checklists on Nokia firewalls, we tracked the fact that these boxes were correctly configured to authenticate the users by means of the Cisco Secure ACS server.

5.2 Risk Assessment

We may now assume that the routers, switches and firewalls of ITCORP customers are correctly immune to potential security attacks.

This *situation must be consolidated* by:

1. Introducing periodicity in the controls in order to detect any deviation coming from new security advisories (software update), administrators leaving or joining the team (access management), and device configuration changes (device administration). Quarterly verification is a good compromise between risk and cost.
2. Assuring that a new device is not plugged on the production network before having been controlled 100% compliant by the security team. This procedure must be supported by the management since we may easily imagine that due to business

© SANS Institute 2005 Author retains full rights.

constraints, bypasses will be requested for some "emergency" situations.

The *depth of the controls should be increased* on key items where potential risks may exist:

1. It is necessary to control that log files sent by the network devices to the Syslog or Cisco Secure ACS servers are saved for a sufficient period of time (for instance 60 days) and not lost due to disk space problems. This could endanger the investigation should a security problem occur.
2. The vast majority of network devices now support SSH protocol to perform administrative access. A migration plan should be put in place to abandon telnet and use SSH instead. This is a security concern to use a secure user access management method like TACACS+, with encryption between the device and the authentication server, and go on using telnet protocol with passwords in clear text between the administrator station and the network device.
3. Access Control List (ACL) consistency checking must be improved: refer to Llorens and Levier's book [23] for security tests to perform on router ACLs.

The *scope of the controls should the widened* to address network devices only covered today with the default network scan procedure. An extension of the specific audit checklist to cover some of these devices is necessary.

Having done all this stuff, are there still remaining risks? If I was in the place of a hacker, I would probably quickly realize that "basic" network infrastructure devices (routers, switches, firewalls) are difficult to compromise. But what about value added servers like DNS, DHCP and authentication servers? Is there not a chance that they are less closely watched?

DNS and DHCP servers are often Windows or Linux style boxes and in a big organization like ITCORP, I could guess that in term of responsibility, they are somewhere in between network administration and server administration teams. I may even guess that nobody is really in charge of their security. Compromising them could be not so difficult and have a big impact on the network! The *security control of value added servers is a must*.

Last question: does the solution described above introduce new risks to the organization? In fact there is one: the centralized RAT web server. We have explained how the RAT tool was improved with a more convenient web interface associated with a web server. This server contains a copy of all the Cisco device configurations and even the audit reports with the found vulnerabilities. This is highly valuable information for an inside attacker which could easily learn the existence and the name of such server (social engineering): the *RAT web server must be carefully secured*.

[23] Llorens, Levier p182-195

© SANS Institute 2005 Author retains full rights.

5.3 Added value of SANS Training

The following additional concept learned in the SANS course was helpful for this section (see the conclusion)

- Internet Security Technologies
  - Network and Host Intrusion Detection

5.4 Conclusion

We described a method to improve the security of network devices by hardening their configuration, authenticating the user accesses, patching the software. Progresses accomplished were measured by means of security indicators. We identified remaining concerns such as lack of security control in value added network services, insufficient controls for some kinds of boxes. These items will be addressed soon. And what happen then? Will we have reached a safe haven?

The fact that each individual box is secure is a necessary starting point. But it does not guarantee that the whole network is bullet proof. It is not because each house in a residential area has high fences and solid locks that the area is safe!

That's why we have to change the focus from the individual box to the network as an independent entity. Let me outline two aspects of this viewpoint:

1. How can I verify that the network as a whole is secure?

- *Boundary packet filters*: the first obvious action is to check how and which data may enter the network. Data exiting the network must not be forgotten either. For instance Time To Live (TTL) exceeded ICMP messages may be gathered by an outside attacker using the "traceroute" command to identify open ports beyond the perimeter firewall. (See the description of the tool firewalk [24] for an in depth explanation).

  Packet filters on network boundary firewalls have to be carefully reviewed and periodically validated to guarantee that their settings only allow necessary traffic for valid business needs to pass through and reject all other kinds of traffic. Are they automatic tools for that?

- *Topology security assessment:* tools and methods to check and measure the security of network components exist, but what about equivalent tools and methods at network level? How to compare the security level of one network topology with respect to another one?

2. How can I detect suspicious activities and react to them? Intrusion detection and/or intrusion prevention are the solution and must be deployed in the network.

[24] firewalk

© SANS Institute 2005 Author retains full rights.

Several alternatives are possible: intrusion detection at network level or/and on some sensible boxes? How to characterize a suspicious or hostile traffic? What action should I take when it is detected?

Last but not least question: is it not a potential threat that the vast majority of the network boxes are Cisco one, most of the firewalls Nokia's? Should we not consider introducing some diversity in the equipment providers for the same reason that the real world is more likely to survive a cataclysm with many different species than with a single one?

It's definitely time to close the subject of network box security and go on with the more challenging one of global network security!

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

6 REFERENCES

[8] Bugtraq."Vulnerabilities". SecurityFocus™. 6 Dec 2004 <http://www.securityfocus.com/bid>

[10] Center for Internet Security. "IOS/PIX Benchmarks and RAT for Windows". Benchmarks and Tools Version 2.2. 6 Dec 2004 <http://www.cisecurity.org/bench_cisco.html>

[4] CERT. CERT® Advisory CA-1996-01 "UDP Port Denial-of-Service Attack". 24 Sept 1997. 6 Dec 2004 <http://www.cert.org/advisories/CA-1996-01.html>

[22] Cisco Systems. Cisco Secure Access Control Server V3.0 Tutorial. Revision Mar 2002.6 Dec 2004 <http://www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/acstu_pg.pdf>

[13] Cisco Systems. "Improving Security on Cisco Routers". Document ID: 13608. Updated 12 Oct 2004. 6 Dec 2004<http://www.cisco.com/warp/public/707/21.html>

[9] Cisco Systems. "Internetworking Design Basics". Internetwork Design Guide. 10 Apr 2002. 6 Dec 2004 <http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2002.htm#xtocid7>

[3] Cisco Systems. "Cisco Router and Security Device Manager 1.2 User's Guide". Document ID OL-4015-04.26 Oct 2004. 6 Dec 2004 <http://www.cisco.com/univercd/cc/td/doc/product/software/sdm/20ugd/saudt.htm#wp1046444>

[5] Cisco Systems. "Cisco Security Advisory: Malformed SNMP Message-Handling Vulnerabilities". Document ID 19294. 23 Dec 2003. 6 Dec 2004. <http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml>

[12] Fraunhofer Institut Experimentelles Software Engineering. "CROCODILE®: A tool to analyse router configurations". Last modified 12 March 2004. 6 Dec 2004 <http://www.iese.fhg.de/CROCODILE>

[17][23] Llorens, Cedric and Levier, Laurent. Tableaux de bord de la sécurité réseau. Paris. Edition Eyrolles. Sept 2003. 148-159 and 182-195

[19] Naidu, Krishni. "Firewall Checklist". SANS SCORE. Version 1.0. 6 Dec 2004 <http://www.sans.org/score/firewallchecklist.php>

© SANS Institute 2005 Author retains full rights.

[14] United States. National Security Agency. Security Configuration Guides: Router Security Configuration Guide. Version 1.1b. 5 Dec 2003. 6 Dec 2004 <http://www.nsa.gov/snac/downloads_cisco.cfm?MenuID=scg10.3.1>

[15] United States. National Security Agency. Security Configuration Guides: Cisco IOS Switch Security Configuration Guide. Version 1.0. 21 Jun 2004. 6 Dec 2004 <http://www.nsa.gov/snac/downloads_switches.cfm?MenuID=scg10.3.1>

[2] Nessus project. "Nessus Security Scanner documentation". 6 Dec 2004 <http://www.nessus.org/documentation.html>

[6] Ryan, Russell. Strategies anti-hackers.2nd edition. Paris. Edition Eyrolles. 2002.

[18] Malik, Saadat.Network Security Principles and Practices. Cisco Press.15 Nov 2002. <http://safari.ciscopress.com/?XmlId=1587050250>

[24] Schiffman, Mike D., Goldsmith, David. Firewalk tool. Last updated 27 Jan 2003. 6 Dec 2004. <http://www.packetfactory.net/projects/firewalk/>

[11] Stewart, Brian. "Router Audit Tool: Securing Cisco Routers Made Easy!" SANS Reading Room. 29 March 2002. 6 Dec 2004. <http://www.sans.org/rr/papers/38/238.pdf>

[7] Stoneburner, Gary, Goguen, Alice, Feringa, Alexis.United States. National Institute of Standards Technology. "Risk Management Guide for Information Technology Systems. Special Publication 800-30". Recommendations of the NIST. July 2002. 6 Dec 2004 <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf >

[16] Strassberg, Keith, Rhodes-Ousley, Mark, Bragg, Roberta. "Chapter 4: Network Device Security". Network Security: the Complete Reference. ISBN: 0072226978. Mc Graw-Hill Osborne Media. 10 Nov 2003. < http://books.mcgraw-hill.com/getbook.php?isbn=0072226978>

[1] Symantec. Symantec Enterprise Security Manager™. 6 Dec 2004 <http://enterprisesecurity.symantec.com/products/products.cfm?productid=45>

[21] Sys-Security Group. "Using ICMP queries to fingerprint some networking equipment". Advisories. Published: 7 April 2003. 6 Dec 2004 <http://www.sys-security.com/html/advisories.html>

[20] Tu, James. "Auditing a Nokia 440 Check Point Firewall-1 Firewall: An Auditor's Perspective". SANS GSNA Practical Assignment. June 2002. 6 Dec 2004 <http://www.giac.org/practical/James_Tu_GSNA.doc>

© SANS Institute 2005 Author retains full rights.

[25] Wagner, Robert. "Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks". SANS GSEC Practical. Aug 2001. 6 Dec 2004 <http://www.sans.org/rr/papers/60/474.pdf >

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

7 APPENDICES

7.1 Additional explanations on uncovered vulnerabilities

Hereunder are additional considerations for security criteria not covered in the main body of the document and present in the checklist below:

- *Cisco Discovery Protocol (CDP)*: CDP is a layer 2 protocol used by Cisco routers and switches to identify their neighbours. CDP packets contain sensitive information such as IP addresses and software version. CDP can be disabled on a global or per-interface basis.
- *Directed broadcast:* The first and last IP addresses of any subnet are known as the network and the broadcast address respectively. Sending a packet to either of these addresses is akin to sending an individual packet to each device on that network. Thus sending a simple ping to the broadcast address on a subnet with 100 hosts will generate 100 replies to the sender. This functionality has become the basis for "smurf" attacks: if an attacker sends ICMP traffic to the broadcast address of large networks, having changed the source address by the victim's, the victim will receive all the ICMP replies.
- *IP source routing*: Source routing is used to dictate the path that a packet should take through a network. Such information could be used to route traffic around known filters or to cause a denial of service attack by forcing large amounts of traffic through a single router, overloading it. Routers should drop packets containing source routing information.
- *ICMP redirect*: ICMP redirect messages are used in the normal operation of a network to inform hosts of a more efficient route to a destination network. A malicious user may be able to manipulate routing paths. Disable redirect messages generation on router interfaces to untrusted networks.
- *ICMP unreachable:* ICMP destination unreachable messages are returned by a router in the proper operation of a network to indicate that it cannot forward a packet because the destination address or service specified is unreachable. A malicious user can use them to determine available hosts and services. Drop them on interfaces towards untrusted networks.
- *Logging:* Most network devices are able to log information related to ACL activity as well as system-related information. Often devices offer only limited memory space to log locally, but they do provide facilities for remote logging to a centralized Syslog server. If possible log messages on a centralized server and keep the logs for a while.
- *Packet filtering:* packet filtering may be performed by layer 2 devices (switches) by means of MAC address filtering or by level 3 devices (routers) by means of IP address and port filtering. An Access Control List (ACL) contains the list of MAC addresses, or IP addresses and port numbers belonging to the authorized (permit)

© SANS Institute 2005 Author retains full rights.

or banned (deny) devices. For instance, administrative access to a device may be restricted to the management station by means of an ACL.

- *Password encryption*: on Cisco IOS devices, locally stored account information is saved in clear text unless otherwise configured. Two methods of encryption are used: level 7 and secret encryption.
  - Level 7 encryption was designed to avoid casual "over-the-shoulder" password theft: it can be easily guessed with tools available from the internet.
  - The Secret level of encryption uses a reliable MD5 hash function to obfuscate the password. Unfortunately, not all stored passwords can be protected with the secret encryption. For example, passwords used for TTY connections can only be protected with Level 7 encryption.
- *Proxy arp:* proxy ARP is the function used when one host responds to an Address Resolution Protocol request on behalf of the targeted host. This is commonly used on a firewall that is proxying traffic for protected hosts. It may also be enabled on Cisco routers. ARP being a non secure protocol, this may allow an attacker to mount an ARP poisoning attack against a host that is not on the local subnet or VLAN, by compromising the ARP tables of the victim's host partners. Additional information on ARP related attacks may be found in Robert Wagner paper [25].
- *VLAN:* VLANs (Virtual LAN) are layer 2 broadcast domains used to segment a network and controlled by a switch. ARP broadcasts are sent between all devices within the same VLAN. To allow communication between hosts which are not in the same VLAN, a switch must pass the host's packets through a layer 3 device which will route them to the appropriate VLAN. Segmenting a network increases the security.

[25] Robert Wagner

© SANS Institute 2005 Author retains full rights.

7.2 Generic security audit checklist

Rule name	Rule family	Applicable on : common, sw,rtr, fwl	Rule objective (if technically feasible)	Expected result
Require login banner	**administrative access**	**common**	Verify the existence of a login banner and its content	The login banner should contain : - a legal notice notifying the users that the system is for conducting company business only or its uses must be authorized by management. - no mention of company name, device type, location
ACL for administrative access	**administrative access**	**common**	Ensure access controls lists are configured for the administration services enabled on the device	Administrative access to the device (SSH/ http / telnet/ snmp ..) is restricted by ACL from the only IP or MAC addresses used for administration
Console time-out	**administrative access**	**common**	Console access should be blocked if not used during a certain period of time	Console blocked after being idle 10 minutes
no rlogin	**administrative access**	**sw and rtr**	Remote logging on the device through the rlogin protocol is forbidden	rlogin access disabled
SSH V2 only	**administrative access**	**sw and rtr**	If possible, device administration is done through SSH.	- SSH enabled - SSH V1 not used - If SSH enabled, then telnet is disabled
SSH V2 only	**administrative access**	**fwl**	Firewall administration must be done with SSH. Telnet is forbidden. SSH V2 must be used if supported by the device.	- SSH V2 activated - Telnet disabled
No ip http server	**administrative access**	**sw and rtr**	Web interface is disabled if not required to support an application or process.	http disabled
https only	**administrative access**	**sw and rtr**	If web administration is needed, it should be done with the SSL protocol	https enabled with 128 bits key minimum length
https only	**administrative access**	**fwl**	- Http is never authorized on a firewall - Only https access with at least 128 bits key length for SSL is authorized	If SSL used, minimum key length is 128 bits
no ftp	**administrative access**	**fwl**	FTP is never allowed to administrate a firewall - use secure FTP if necessary	FTP disabled

© SANS Institute 2005 Author retains full rights.

Rule name	Rule family	Applicable on : common, sw,rtr, fwl	Rule objective (if technically feasible)	Expected result
OS patch	**code**	**common**	Latest security patches approved by the security team are installed in the operating system code image	No uncorrected security vulnerability in the operating system
Fwl patch	**code**	**fwl**	Latest patches approved by the security team are installed in the firewall application (checkpoint, …) code image	No uncorrected security vulnerability in the firewall application
Filter review	**filter review**	**common**	Reviews of packet filter rules are required periodically on network boundary devices to verify they are current and only authorized network traffic can pass through. Filters can take a variety of formats. The more common are: - IP address filtering - TCP ou UDP port filtering - MAC address filtering	Check that the packet filters review has been performed at the right period of time
hostname	**miscellaneous**	**common**	Device must have an hostname	The hostname is initialized and set according to the naming convention
no port monitor	**miscellaneous**	**common**	Network sniffing is not allowed from the device without authorization	Check that no interface is set in sniffer (promiscuous) mode. Else verify it has been authorized by network administrator and recorded.
no tftp server	**network services**	**common**	TFTP server must be disabled	no tftp service
no unneeded services	**network services**	**common**	Unneeded network services are disabled if not required to support and application or process.	- TCP and UDP small servers always disabled - bootps, finger always disabled - NTP service disabled if not to provide network clock synchronisation - on untrusted interfaces : Cisco Discovery Protocol , ICMP address mask reply, ICMP timestamp reply are disabled if not required to support a valid application or process.

© SANS Institute 2005 Author retains full rights.

Rule name	Rule family	Applicable on : common, sw,rtr, fwl	Rule objective (if technically feasible)	Expected result
no unneeded IP features	**network services**	**common**	Unneeded IP features must be disabled. This applies to : - IP directed broadcast - ICMP unreachable notification on untrusted interfaces - ICMP redirects on untrusted interfaces	- no IP directed broadcast On interfaces to untrusted network, no : - ICMP unreachable notification - ICMP redirects
no ip proxy arp	**network services**	**common**	Proxy ARP is disabled unless the device is serving as a LAN bridge or required by static NAT.	proxy arp is disabled
DNS	**network services**	**common**	If the device has to perform DNS name resolution, set a DNS server address explicitly. Else disable DNS service	DNS server name initialized or no DNS function
NAT	**network services**	**rtr**	Check NAT to make sure that no intranet IP range may be seen externally	Intranet IP addresses are always translated
no DLSw dynamic partner	**network services**	**rtr**	Remote Data Link Switching (DLSw) peers have to be manually defined	Forbid connections from non configured DLSw peer
ip source route	**network services**	**rtr**	IP source routing is disabled	IP source routing disabled
no UNIX unneeded services	**network services**	**fwl**	For Unix appliance, the following services are disabled (in addition to those of the "no unneeded services" rule) - netstat, rusersd, talkd, nfsd, rshelld, - pcnfsd,rexecd,uupc, rexd,rwalld - echo,rpc,statd,sprayd,rstatd,systat	The following services are disabled - netstat, rusersd, talkd, nfsd, rshelld, - pcnfsd,rexecd,uupc, rexd,rwalld - echo, rpc, statd, sprayd, rstatd, systat
no IIS	**network services**	**fwl**	For Windows systems, Internet Information Server (IIS) is disabled.	IIS disabled
ESM installed	**network services**	**fwl**	For HP / SUN / AIX / LINUX / WINDOWS, Symantec ESM ä tool or equivalent must be installed on the server to check its operating system	Symantec ESM agent installed and running

© SANS Institute 2005 Author retains full rights.

Rule name	Rule family	Applicable on : common, sw,rtr, fwl	Rule objective (if technically feasible)	Expected result
Routing table	**network services**	**fwl**	Only static routing is allowed: dynamic routing is forbidden. Review routing table to be sure all defined routes are for a valid business need or application	- no dynamic routing protocol like OSPF,RIP, IGMP enabled - all defined static routes are for a valid business need
Password quality	**password**	**common**	Passwords follow password rules policy	- check password against policy rules (this may be done by using password cracking tools)
Encrypt password	**password**	**common**	Passwords are encrypted	Passwords encrypted locally in a file or when transmitted over the network
SNMP community string quality	**SNMP**	**common**	SNMP community strings follow password rules policy	Check SNMP community strings against password policy rules
no SNMP without ACL	**SNMP**	**common**	SNMP access is restricted by Access Control List to only management systems IP addresses.	SNMP ACL defined and limited to device administration stations
forbid SNMP read-write	**SNMP**	**common**	SNMP write access is disabled except if required to support a valid application (like CiscoWorks)	SNMP write forbidden
SNMP traps to SNMP manager	**SNMP**	**common**	SNMP traps sent to an infrastructure management system.	SNMP trap receiver configured
log login attempts	**syslog**	**common**	Successful and unsuccessful login attempts are logged on an external logging system (e.g. syslog) and kept for 60days.	- device configured to log user login attempts - syslog server address configured on device - syslog files kept 60 days
timestamp logging	**syslog**	**common**	Log messages are timestamped.	log messages timestamped
logging buffered	**syslog**	**common**	If a syslog server can not be used, enough memory space must be defined on the device to keep logs	logging messages buffered locally
disable unused interfaces	**unused port**	**common**	Unused ports and network interfaces are disabled.	check all logical ports or physical network interfaces have a valid use

© SANS Institute 2005 Author retains full rights.

Rule name	Rule family	Applicable on : common, sw,rtr, fwl	Rule objective (if technically feasible)	Expected result
forbid modem attach	**unused port**	**common**	Forbid modem attached	no modem attached
VLAN definition	**unused port**	**sw**	Check VLAN definitions	VLAN with non defined ports or VLAN that are not used anymore must be disabled.
User access	**user authentication**	**common**	Check user accounts to verify owner identity and business need	- Check all users with security or system administrative authority have a business need. - For users which are not part of the support staff, only read access is authorized. - Customer accounts are read only and documented in the customer security contract.
Authentication enabled	**user authentication**	**common**	Check that a centralized authentication server is used	Authentication server use is configured
Individual userid	**user authentication**	**common**	Individual userID must be used instead of a shared userID.	no shared userid defined
Enable secret	**user authentication**	**common**	- Log remotely to the machine using low administrative privilege account if login protocol is not secured (i.e. telnet) - Then use the "su" (UNIX) or "enable secret" (Cisco) or equivalent command to perform administrative tasks.	- Non secure administrative remote login like telnet disabled. - "Enable secret" enabled on Cisco devices
Admin login	**user authentication**	**fwl**	- SSH administrator login allowed through individual user account in order to be able to trace back actions. - login with administrative privilege account through non secure protocol (i.e. Telnet) is forbidden	- telnet login forbidden

Table 7 : Generic network device security audit checklist

© SANS Institute 2005 Author retains full rights.

7.3 Nokia firewall security audit checklist

Rule name	Rule objective (if technically feasible)	Nokia verification action	Nokia expected result
Require login banner	Verify the existence of a login banner and its content	**Not supported on Nokia**	
ACL for administrative access	Ensure access controls lists are configured for the administration services enabled on the device	**See firewall filter rules**	**Check accesses to SSH, https and SNMP ports on the firewall are restricted to administrative stations**
Console time-out	Console access should be blocked if not used during a certain period of time	**Not supported on Nokia**	
no rlogin	Remote logging on the device through the rlogin protocol is forbidden	**Not supported on Nokia**	
SSH V2 only	Firewall administration must be done with SSH. Telnet is forbidden. SSH V2 must be used if supported by the device.	**Using Nokia Voyager Web browser under Summary** **- Network Access and Services section** **- SSH section**	**- telnet access is disabled** **- SSH service is enabled and protocol version is 2**
https only	- Http is never authorized on a firewall - Only https access with at least 128 bits key length for SSL is authorized	**Using Nokia Voyager Web browser under Summary** **- Voyager Web access section**	**- SSL Voyager port defined** **- SSL security : enabled 128 bits minimum key length**
no ftp	FTP is never allowed to administrate a firewall - use secure FTP if necessary	**Using Nokia Voyager Web browser under Summary - Network Access and Services section**	**FTP access is not allowed**
OS patch	Latest security patches approved by the security team are installed in the operating system code image	**Using Nokia Voyager Web browser under Summary** **- Manage IPSO image section**	**Check current selected IPSO image is latest**
Fwl patch	Latest patches approved by the security team are installed in the firewall application (checkpoint, …) code image	**Using Nokia Voyager Web browser under Summary** **- Manage installed package**	**Check Checkpoint package level is latest**

© SANS Institute 2005 Author retains full rights.

Rule name	Rule objective (if technically feasible)	Nokia verification action	Nokia expected result
Filter review	Reviews of packet filter rules are required periodically on network boundary devices to verify they are current and only authorized network traffic can pass through. Filters can take a variety of formats. The more common are: - IP address filtering - TCP ou UDP port filtering - MAC address filtering	**Check the filter review has been performed**	
hostname	Device must have an hostname	**Using Nokia Voyager Web browser under Summary - Change hostname section**	**Hostname is set according to naming convention**
no port monitor	Network sniffing is not allowed from the device without authorization	**Not supported on Nokia**	
no tftp server	TFTP server must be disabled	**Using Nokia Voyager Web browser under Network Access and Services**	**TFTP access is not allowed**
no unneeded services	Unneeded network services are disabled if not required to support and application or process.	**Using Nokia Voyager Web browser under Summary - network access and services section - router services**	**- echo, discard, chargen, daytime, time services are disabled - bootp relay : no - NTP reference clock : not active**
no unneeded IP features	Unneeded IP features must be disabled. This applies to : - IP directed broadcast - ICMP unreachable notification on untrusted interfaces - ICMP redirects on untrusted interfaces	**Built-in in device. No need to check**	
no ip proxy arp	Proxy ARP is disabled unless the device is serving as a LAN bridge or required by static NAT.	**Using Nokia Voyager Web browser under Summary - ARP section**	**Check that only permanent entries are present for NAT purpose**
DNS	If the device has to perform DNS name resolution, set a DNS server address explicitly. Else disable DNS service	**Not supported on Nokia : the firewall can not be configured as a DNS server**	**DNS primary /secondary servers name value initialized or not configured**

© SANS Institute 2005 Author retains full rights.

Rule name	Rule objective (if technically feasible)	Nokia verification action	Nokia expected result
NAT	Check NAT to make sure that no intranet IP range may be seen externally	**Using firewalls rules policy - adress translation rules section**	**Check intranet address are translated**
no DLSw dynamic partner	Remote Data Link Switching (DLSw) peers have to be manually defined	**Not supported on Nokia**	
ip source route	IP source routing is disabled	**Built-in in device . No need to check**	
no UNIX unneeded services	For Unix appliance, the following services are disabled (in addition to those of the "no unneeded services" rule) - netstat, rusersd, talkd, nfsd, rshelld, - pcnfsd,rexecd,uupc, rexd,rwalld -echo,rpc,statd,sprayd, rstatd,systat	**Not supported on Nokia**	
no IIS	For Windows systems, Internet Information Server (IIS) is disabled.	**Not supported on Nokia**	
ESM installed	For HP / SUN / AIX / LINUX / WINDOWS, Symantec ESM tool or equivalent must be installed on the server to check its operating system	**Not supported on Nokia**	
Routing table	Only static routing is allowed: dynamic routing is forbidden. Review routing table to be sure all defined routes are for a valid business need or application	**Using Nokia Voyager Web browser under Summary - routing configuration section**	**- only static routes are allowed - check they are for a valid busines need**
Password quality	Passwords follow password rules policy	**Not supported on Nokia (not enforced automatically by the device)**	
Encrypt password	Passwords are encrypted	**Built-in in device. No need to check**	
SNMP community string quality	SNMP community strings follow password rules policy	**Using Nokia Voyager Web browser under Summary - SNMP configuration section**	**Check SNMP community string**

© SANS Institute 2005 Author retains full rights.

Rule name	Rule objective (if technically feasible)	Nokia verification action	Nokia expected result
no SNMP without ACL	SNMP access is restricted by Access Control List to only management systems IP addresses.	**See firewall filter rules**	**Check access to SNMP services are restricted to administration stations**
forbid SNMP read-write	SNMP write access is disabled except if required to support a valid application (like CiscoWorks)	**Using Nokia Voyager Web browser under Summary - SNMP configuration section**	**Check no SNMP write community string defined**
SNMP traps to SNMP manager	SNMP traps sent to an infrastructure management system.	**Using Nokia Voyager Web browser under Summary - SNMP configuration**	**Trap receiver is defined**
log login attempts	Successful and unsuccessful login attempts are logged on an external logging system (e.g. syslog) and kept for 60days.	**Using Nokia Voyager Web browser under Summary - system logging section**	**Remote IP address to log to is set**
timestamp logging	Log messages are timestamped.	**Built-in in device. No need to check**	
logging buffered	If a syslog server can not be used, enough memory space must be defined on the device to keep logs	**Not supported on Nokia**	
disable unused interfaces	Unused ports and network interfaces are disabled.	**Using Nokia Voyager Web browser under Summary - IP interfaces section**	**check active interfaces**
forbid modem attach	Forbid modem attached	**Using Nokia Voyager Web browser under Summary - Network Access and Services section**	**com2 and com3 login is disabled**
VLAN definition	Check VLAN definitions	**Not applicable on firewall**	
User access	Check user accounts to verify owner identity and business need	**Not done with RAT**	
Authentication enabled	Check that a centralized authentication server is used	**Using Nokia Voyager Web browser under Summary - AAA section**	**auth_profile contains a profile whose type is an authentication method**

© SANS Institute 2005 Author retains full rights.

Rule name	Rule objective (if technically feasible)	Nokia verification action	Nokia expected result
Individual userid	Individual userID must be used instead of a shared userID.	**Using Nokia Voyager Web browser under Summary - User names section**	**Check all userids are attributed to individuals except 'admin,' 'root' and 'monitor 'which can not be removed**
Enable secret	- Log remotely to the machine using low administrative privilege account if login protocol is not secured (i.e. Telnet) - Then use the "su" (UNIX) or "enable secret" (Cisco) or equivalent command to perform administrative tasks.	**see "Admin login" rule for firewall below**	**Check that administrator could not log remotely via Telnet to the device by verifying that "allow admin network logging" is disabled**
Admin login	- SSH administrator login allowed through individual user account in order to be able to trace back actions. - login with administrative privilege account through non secure protocol (i.e. Telnet) is forbidden	**Using Nokia Voyager Web browser under Summary - Network Access and Services section - SSH section**	**- Check that administrator could not log remotely via Telnet to the device by verifying that "allow admin network logging" is disabled - SSH "admin login" must be permitted**

Table 8 : Nokia firewalls security audit checklist

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

7.4 Cisco IOS and catOS RAT rules

Rule name	Rule objective (if technically feasible)	RAT IOS rule (*)	RAT catOS rule (*)
Require login banner	Verify the existence of a login banner and its content	***IOS - require login banner***	***CatOS - set logging banner***
ACL for administrative access	Ensure access controls lists are configured for the administration services enabled on the device	**IOS - Apply vty ACL**	***CatOS - set ip permit enable telnet*** ***CatOS - set ip permit enable SSH***
Console time-out	Console access should be blocked if not used during a certain period of time	**IOS - exec-timeout**	***CatOS - set exec-timeout***
no rlogin	Remote logging on the device through the rlogin protocol is forbidden	**Not supported on IOS**	**Not supported on catOS**
SSH V2 only	If possible, device administration is done through SSH.	**Not controlled : will be done later when administrative staff is ready to migrate fully to SSH**	**Not controlled : will be done later when administrative staff is ready to migrate fully to SSH**
No ip http server	Web interface is disabled if not required to support an application or process.	**IOS - no ip http server**	***CatOS - no ip http server***
https only	If web administration is needed, it should be done with the SSL protocol	**Can not be checked on IOS**	**Can not be checked on catOS**
OS patch	Latest security patches approved by the security team are installed in the operating system code image	**Can not be controlled through RAT**	**Can not be controlled through RAT**
hostname	Device must have an hostname	***IOS – hostname***	***catOS - hostname***
no port monitor	Network sniffing is not allowed from the device without authorization	***IOS - no port monitor***	***CatOS - forbid span or rspan session***
no tftp server	TFTP server must be disabled	**IOS - no service config** **IOS - no tftp-server**	**not applicable on catOS**

© SANS Institute 2005 Author retains full rights.

Rule name	Rule objective (if technically feasible)	RAT IOS rule (*)	RAT catOS rule (*)
no unneeded services	Unneeded network services are disabled if not required to support and application or process.	**IOS - no cdp run IOS - no ip bootp server IOS - no finger service IOS - no tcp-small-servers IOS - no udp-small-servers** ***IOS - no ip mask-replyIOS - no ntp master***	**not applicable on catOS**
no unneeded IP features	Unneeded IP features must be disabled. This applies to : - IP directed broadcast - ICMP unreachable notification on untrusted interfaces - ICMP redirects on untrusted interfaces	**IOS - no directed broadcast** ***IOS - no ip redirects*** ***IOS - no ip unreachables***	**not applicable on catOS**
no ip proxy arp	Proxy ARP is disabled unless the device is serving as a LAN bridge or required by static NAT.	**IOS - no ip proxy-arp**	**not applicable on catOS**
DNS	If the device has to perform DNS name resolution, set a DNS server address explicitly. Else disable DNS service	***IOS - forbid broadcast name resolution***	**not applicable on catOS**
NAT	Check NAT to make sure that no intranet IP range may be seen externally	**Not done with RAT**	**not applicable on catOS**
no DLSw dynamic partner	Remote Data Link Switching (DLSw) peers have to be manually defined	***IOS - forbid DLSW dynamic partners***	**not applicable on catOS**
ip source route	IP source routing is disabled	**IOS - no ip source-route**	**not applicable on catOS**
Password quality	Passwords follow password rules policy	**IOS - line password quality (password type 7)** **IOS - user password quality (password type 7)** **IOS - require line passwords**	***CatOS - set password***
Encrypt password	Passwords are encrypted	**IOS - encrypt passwords**	***CatOS - set password***
SNMPcommunity string quality	SNMP community strings follow password rules policy	***IOS - SNMP community string quality*** ***IOS - forbid trivial SNMP community***	***CatOS - snmp community quality*** ***CatOS - forbid trivial SNMP community public,private,secret***

© SANS Institute 2005 Author retains full rights.

Rule name	Rule objective (if technically feasible)	RAT IOS rule (*)	RAT catOS rule (*)
no SNMP without ACL	SNMP access is restricted by Access Control List to only management systems IP addresses.	**IOS - forbid SNMP without ACLs**	***CatOS - forbid community without ACL***
forbid SNMP read-write	SNMP write access is disabled except if required to support a valid application (like CiscoWorks)	**IOS - forbid SNMP read-write**	***CatOS - forbid SNMP read-write***
SNMP traps to SNMP manager	SNMP traps sent to an infrastructure management system.	***IOS - send traps to snmp manager***	***catOS- send traps to snmp manager***
log login attempts	Successful and unsuccessful login attempts are logged on an external logging system (e.g. syslog) and kept for 60days.	**IOS - enable logging** **IOS - set syslog server** **IOS - logging trap info or higher**	***CatOS - set logging server***
timestamp logging	Log messages are timestamped.	**IOS - service timestamps logging** **IOS - service timestamps debug**	***CatOS - set logging timestamp***
logging buffered	If a syslog server can not be used, enough memory space must be defined on the device to keep logs	**IOS - logging buffered**	**not applicable on catOS**
disable unused interfaces	Unused ports and network interfaces are disabled.	**IOS - disable aux**	**not applicable on catOS**
forfid modem attach	Forbid modem attached	**IOS - disable aux**	**not applicable on catOS**
VLAN definition	Check VLAN definitions	**Not applicable on router**	**Not done with RAT**
User access	Check user accounts to verify owner identity and business need	**Not done with RAT**	**Not done with RAT**
Authentication enabled	Check that a centralized authentication server is used	**IOS - aaa authentication enable** **IOS - aaa authentication login** **IOS - aaa new-model**	***CatOS - set tacacs or radius server***
Individual userid	Individual userID must be used instead of a shared userID.	**Not done with RAT**	**Not done with RAT**

© SANS Institute 2005 Author retains full rights.

Rule name	Rule objective (if technically feasible)	RAT IOS rule (*)	RAT catOS rule (*)
Enable secret	- Log remotely to the machine using low administrative privilege account if login protocol is not secured i.e. Telnet) - Then use the "su" (UNIX) or "enable secret" (CISCO) or equivalent command to perform administrative tasks.	**IOS - enable secret**	***CatOS - set enablepass***

Table 9 : Cisco IOS and catOS RAT rules

(Rules in italic are new one with respect to original RAT version)

********** **END OF DOCUMENT** **********

© SANS Institute 2005 Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**