Global Information Assurance Certification Paper

Disabling Unneeded Features and Services on Cisco Internet Gateway Routers
Toon Mordijck
GSEC Practical Assignment Version 1.2e

Introduction

Cisco is known as the market leader for Internet gateway routers in corporate environments. Sometimes these routers have a specific role in protecting the internal network. However, in many cases this role is given to one or more firewalls. This leaves the Internet gateway routers in many cases as the only device not protected by the firewall(s) for malicious network traffic over the Internet connection. Therefore it is quite important for many businesses to have good guidance on how to secure their Cisco Internet gateway router(s).

A lot of work has been done and many publications and course material (e.g. in the SANS curriculum) exist. Some excellent books on Cisco can be bought but luckily lots of formation is also freely available on the Internet. However, not always the same message is given. In books that try to cover all aspects of Cisco routers including e.g. the 'Cisco Router Handbook' from George C. Sackett, covering security aspects is very limited. Protecting the router itself is in most cases not covered at all.

More specific security focussed publications and courses show many differences in their list of recommended actions to secure a Cisco router and also the quality of the recommendations made varies a lot.

The best freely available guide on Cisco security I found is clearly the 'Router Security Configuration Guide' from the System and Network Attack Center (SNAC) from the US National Security Agency (NSA). The NSA publicised this document recently together with other Security guides. This 240-page publication is excellent. I do recommend downloading and reading it. Part of my research project consists of commenting on it, as I do not have the ambition to write a better document than this one.

A few other GIAC GSEC research projects have been done on Cisco security. The present work covers a topic not yet covered in the other ones.

The focus of this document is on closing down services and features as part of the hardening of the router. The classical idea behind this is that it is best practice to close down not only some services known as dangerous, but also all services and features that are not needed. There seems to be a consensus that especially on border routers, which are not protected by a firewall, this has high value. Originally I was convinced that it would be easy to build a list of services to close down. While concentrating on this during my research it turned out to be a major challenge.

Why is it so hard to know which services to disable?

Something very specific about IOS (the Cisco router operating system) is the fact that a router configuration is defined as the set of changes compared to a default situation. The problem with this is that, while reviewing a configuration file, one cannot determine the services and

features that are enabled by default. Many router administrators do not know which services are active on their router and as a result are not aware of the related risks. The only way to find out which services and features are active is by researching the available documentation and publications.

One would expect to find to necessary information in Cisco white papers and documentation and indeed a lot of it can be found on Cisco's web site. However this site is so huge that it is very difficult to find what you need. In a previous GIAC practical Pepin C. Barrameda Jr. explained that using a third party site can help in finding your way around the CCO (Cisco Connection Online) site and he specifically mentioned a site owned by a CCIE named Randall S. Benn (Cisco Systems in a Nutshell). I agree with him that this is a good alternative to find interesting documents on the Cisco site. However, it should be noted that it is also not the way to find really all documents on a specific subject, e.g. security. My impression is that every time someone checks the CCO site again, he/she will find more documents and more information. Exploring this site surely gives me the feeling of a never-ending job.

Another, quite annoying problem is the presence of clear errors in some of the existing documents, including white papers by Cisco. Many links on the CCO site lead you a document titled: 'Improving Security on Cisco Routers'. Some details in this document are in contradiction with details on the same subject in the IOS technical documentation (e.g. in the 'IOS 12.1 Basic System Management Commands' command reference) and contain errors. This means that sometimes it is even hard to find out how to disable a service that is enabled by default.

My approach to determine which services to disable and how to disable them

As soon as I learned about the contradictions in the available documents, I decided to take the approach to believe only the official Cisco IOS Command Reference documents.

I understand the limitations of this approach. To be really sure about the accuracy of a specific command, one should test it on a real Cisco router to cover for typing/printing errors in the documentation. Due to time and resource limitations I could only test a few commands on one specific router (Cisco 1605) with one specific IOS software version (IOS 12.0). On the other hand, I am convinced that similar limitations were present for all the authors of the other Cisco IOS security guides available.

Furthermore it should be noted that if the tests were not performed on a freshly installed system, they would even not reveal the default behaviour of a specific configuration command. Both the enabled and the disabled version are shown in a configuration dump.

Comments on the NSA document

In the 'Router Security Configuration Guide' from the SNAC-NSA the subject of disabling unneeded services and features is covered in section 4.2. As I appreciate the clear explanations in this section (and in the whole document) I use it as a base for some comments that result from my research:

- General: One of the major problems with this kind of document is the fact that details

can change with every new release of IOS. It is not always clear in the NSA document clear which command to use with a specific IOS version. At the time of the writing of this practical, documentation for IOS 12.2 was online available. However, I cover only IOS 12.1 and earlier and for testing I used IOS 12.0(7)T.

- General: Some of the recommendations relate to services that are already disabled by default. These include HTTP Server, Auto-Loading, IP Subnet Zero and IP Mask-Reply. It clearly does not hurt to explicitly disable such services. However, the result is most of the times not shown in a configuration dump. For some of them the associated risk is clearly higher than for others (e.g. http server versus ip subnet zero). Furthermore it should also be noted that many more services with potential risks on border routers can be activated. My personal approach is to limit hardening recommendations to the services and features that are enabled by default.
- CDP: In IOS 12.0(3)T the Cisco Discovery Protocol Version 2 (CDPv2) advertising functionality was introduced. Similar to the first version this service is enabled by default.
- Finger: Presumable from IOS 12.0 on both the commands **no ip finger** and **no service finger** can be used and act the same. The first one shows up in the configuration. The Cisco documentation on this is not clear.
- NTP: Something weird is happening with this service. The NSA document and some other Cisco Security guides recommend to use the **no ntp enable** command. However, all official IOS reference documents mention the **ntp disable** command. I could not test it myself: none of these commands was accepted on my test router. Maybe NTP is not supported on the Cisco 1600 hardware. However, a correspondent confirmed that he needed to use the **ntp disable** command on his routers (IOS 11.2(21) and 12.0(4)).
- DNS Name Resolution: the **ip name-server** command can be used to specify the name servers to be used in name resolution. By default no name server is specified. To explicitly deny all name-resolution the **no ip domain-lookup** command is best used.
- PAD – X.25: To my surprise I found that this service is enabled by default, even on my small test router. The probability that it will cause security problems seems very low. However, the general principle recommends disabling it. I discovered this in a Cisco white paper intended for ISP's. It was the only reference to it that I found in white papers or similar publications. I really wonder how many other services or features are even better hidden in the Cisco documentation.
- MOP: To disable an interface to support the Maintenance Operation Protocol (MOP), use the **no mop enabled** interface configuration command. This service seems to be enabled by default on Ethernet interfaces and disabled on all other interfaces. However, this command was not available on my test router.

Audit guide

In this section I provide a simple list to verify if unneeded services and features are disabled on an Internet gateway router. The idea is to provide a checklist to compare a specific router configuration with. First the IOS release in use needs to be verified (use the **show version** command) as some of the configuration commands below have been changed at some point in time.

Services and features that should be disabled:

- CDP: use the global configuration commands:
  - **no cdp run** (from IOS 10.3 on) and
  - **no cdp advertise-v2** (from IOS 12.0(3)T on) or use the interface configuration command:
  - **no cdp enable** (from IOS 10.3 on)
- TCP and UDP Small Services: use the global configuration commands:
  - **no service tcp-small-servers** (from IOS 11.1 on, default from IOS 12.0 on) and
  - **no service udp-small-servers** (from IOS 11.2 on, default from IOS 12.0 on)
- Finger: use the global configuration commands:
  - **no service finger** (from IOS 10.0 on) or
  - **no ip finger** (from IOS 12.0 on)
- Bootp server: use the global configuration command:
  - **no ip bootp server** (from IOS 11.2 on)
- IP Source Routing: use the global configuration command:
  - **no ip source-route** (from IOS 10.0 on)
- Proxy ARP: use the interface configuration command:
  - **no ip proxy-arp** (from IOS 10.0 on)
- IP Directed Broadcast: use the interface configuration command:
  - **no ip directed-broadcast** (from IOS 10.0 on, default from IOS 12.0 on)
- Classless Routing: use the global configuration command:
  - **no ip classless** (from IOS 11.3 on as it is disabled by default in earlier versions)
- IP Unreachables and Redirects: use the interface configuration commands:
  - **no ip unreachables** (from IOS 10.0 on) and
  - **no ip redirects** (from IOS 10.0 on)
- NTP: use the interface configuration command:
  - **ntp disable** (from IOS 10.0 on)
- SNMP: use the global configuration command:
  - **no snmp-server** (from IOS 10.0 on)
- DNS: use the global configuration command:
  - **no ip domain-lookup** (from IOS 10.0 on)
- PAD – X.25: use the global configuration command:
  - **No service pad** (from IOS 10.0 on)
- MOP: use the interface configuration command:
  - **No mop enabled** (from IOS 10.0 on)

This list can be used to implement Cisco router hardening or to review it. In both cases deviations have to be justified by business reasons together with risk analysis. For every service or feature that is enabled, other measures (e.g. the use of access-lists) need to be investigated to reduce as much as possible the associated risk.

One should also keep in mind that this list focuses only on disabling unneeded services and features. Other aspects of securing Cisco routers including but not limited to restricting commands, have to be considered too.

Analysis of the current role of Cisco in giving guidance on securing their own routers

I am quite disappointed in the guidance that is currently given by Cisco on securing routers.

As mentioned before, the white papers and the other documents that can be found at the Cisco Connection Online site are most of the time incomplete and some of them contain even errors.

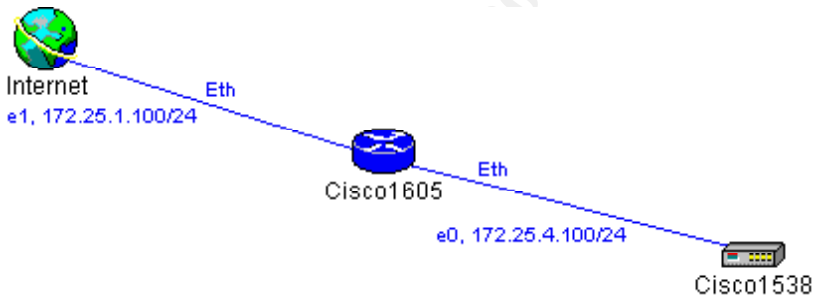
I mainly used the IOS 12.1 documentation, as the version 12.2 documentation is less good in specifying default settings and command history anymore (at the time of the writing of this paper).

The book 'Managing Cisco Network Security' by Michael J. Wenstrom is sold as 'the Official MCNS Coursebook' to 'Prepare for the Cisco Security Specialist Certification'. It looks really good in general. However, on the aspect of disabling unneeded services, it lacks completeness and accuracy in a similar way as most other publications on this topic.

Cisco provides a free tool 'Configmaker' that can be downloaded from the Cisco site. It is a nice tool with an easy GUI that helps you configure various Cisco devices.

I downloaded version 2.5 build 8, claims to support IOS release 11.2 and later.
It is known as a real nice tool to generate configurations that make your network 'work'. However, as is written in the README file: 'Cisco ConfigMaker does not try to configure every IOS parameter or support every IOS feature. Rather, it helps you get your device up and running by supporting the most common features.'

Indeed, when building a very simple network (a Cisco 1605 router between the internal network (Cisco 1538M hub) and the Internet:



An IOS nice configuration file is generated. However, the configuration commands that disable unneeded services are limited to:

- no service tcp-small-servers
- no service udp-small-servers
- no ip name-server
- no ip domain-lookup
- no ip http server

The **enable secret** command was even not suggested!

My conclusions and suggestions

Many elements in this document clearly demonstrate that the subject 'Disabling Unneeded Features and Services on Cisco Internet Gateway Routers' is very complex. The ultimate guide on this subject does not exist and will probably never be written. A major contribution in the right direction is clearly the NSA document 'Router Security Configuration Guide'. However, although this is a document with eleven main authors and five more contributors and a development history of more than a year, I could formulate quite a few comments on its content.

I made my own contribution to this subject and I hope that my research will help many people in securing their Cisco Internet Gateway routers.

My first suggestion is to all the authors or editors of the various existing documents (including the NSA and Cisco documents) to make corrections or additions to their documents based on the results presented in this document.

I am however aware that also in my list of configuration commands to consider, some errors may be present. The way Cisco reveals a router configuration to its administrators is just too unclear and I do not have, as most other people, the time and the resources to learn everything about it. The only people probably that have enough knowledge to guarantee the correctness of such a list are the IOS developers at Cisco.

My second suggestion is to Cisco to drastically re-engineer IOS in such a way that a configuration file gives a clear view on the detailed behaviour that can be expected from the router.

Probably, it will take several more IOS releases, to reach such a situation. My suggestion on the short term to the Cisco IOS developers is to publish a list of default active services and features and the correct configuration command to disable (and re-enable) them. Ideally this list should be available for all IOS releases (and sub-releases if relevant) but starting with the most recent releases is probably best. These lists should be published at the Cisco web site. Every author, every course leader and every consultant will still have his/her own vision on the best way to secure Cisco routers but at least they will be able to share the real facts on how a Cisco router works.

References and additional reading

SANS courses that cover Cisco security include at least:

Crabb-Guel, Michele and Stewart, John Cisco's Security Features: What, Where to Use, and How to Configure. NS1999 and other SANS conferences
Brenton, Chris and Spitzner, Lance Advanced Perimeter Protection and Defense In-Depth. part of the GIAC program "Firewalls and Intrusion Detection"

Sackett, George C. Cisco Router Handbook. McGraw-Hill 1999

Antoine, Vanessa et al. Router Security Configuration Guide. SNAC-NSA 2001. URL:

http://nsa1.www.conxion.com/

SANS-GIAC GSEC Research Projects on Cisco security include at least:

Lindsay, Paul "Cisco Reflexive Access Lists." 2001. URL:
http://www.sans.org/infosecFAQ/firewall/reflex.htm

Langley, Richard "Securing Your Internet Access Router" 2001. URL:
http://www.sans.org/infosecFAQ/firewall/router.htm

Barrameda Jr., Pepin C. "Restricting commands on a Cisco Router with Privilege Levels." 2001. URL: http://www.sans.org/infosecFAQ/firewall/commands.htm

The Cisco Systems in a Nutshell site originally could be found at
http://www.ciscoinanutshell.com. This site has been moved to
http://iponeverything.net/cisco.shtml.

Cisco "Improving Security on Cisco Routers." URL:
http://www.cisco.com/warp/public/707/21.html

Cisco "IOS 12.1 Basic System Management Commands." URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_r/frprt3/frd3003.htm

Cisco, all "Cisco IOS Software Configuration" technical documents. URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm

Cisco "ISP Essentials Guide." URL:
http://www.cisco.com/public/cons/isp/documents/IOSEssentialsPDF.zip

Wenstrom, Michael J. Managing Cisco Network Security Cisco Press, 2001

Cisco "ConfigMaker." URL: http://www.cisco.com/public/sw-center/sw-netmgmt.shtml

Appendix 1: configuration of the test router I used

Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Ethan

```
!
enable secret 5 ***removed***
!
!
!
!
!
no ip subnet-zero
no ip source-route
no ip routing
no ip finger
no ip domain-lookup
!
!
!
!
interface Ethernet0
 description Internal
 ip address 172.25.4.100 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip directed-broadcast
 no ip proxy-arp
 no ip route-cache
!
interface Ethernet1
 description External
 ip address 172.25.1.100 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip directed-broadcast
 no ip proxy-arp
 no ip route-cache
!
no ip classless
no ip http server
!
no cdp advertise-v2
no cdp run
!
line con 0
 exec-timeout 15 0
 password 7 ***removed***
 login
 transport input none
line vty 0 4
 exec-timeout 30 0
 password 7 ***removed***
```

```
 login
!
end
```

Appendix 2: configuration build by ConfigMaker in a similar situation

```
! ************************************************************************
! Cisco1605.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.5 Build 8
!   13 August 2001, 05:06:37 PM
!
! Hostname: Cisco1605
! Model: 1605
! ************************************************************************
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Cisco1605
!
enable password a
!
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Ethernet 0
 no shutdown
 description connected to Cisco1538
 ip address 172.25.4.100 255.255.255.0
 keepalive 10
!
interface Ethernet 1
 no shutdown
 description connected to Internet
 ip address 172.25.1.100 255.255.255.0
 keepalive 10
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Ethernet 1
no ip http server
```

```
snmp-server community public RO
no snmp-server location
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password a
 login
!
line vty 0 4
 password a
 login
!
end
```