Global Information Assurance Certification Paper

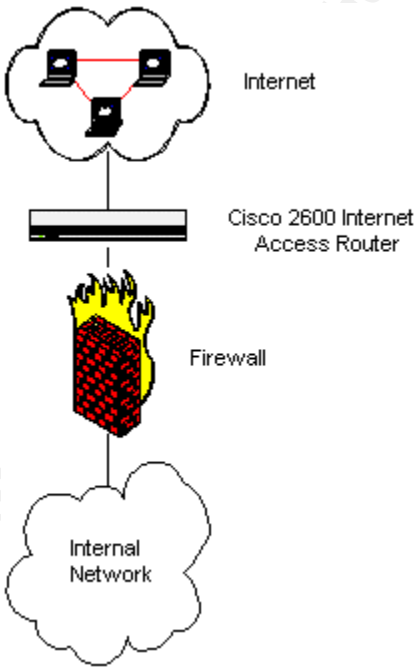
Securing your Internet Access Router

Richard Langley
2001-01-23

Preface

The name "Internet Access Router" is used in this paper to describe the router most organizations place between the Internet and their internal network. What makes this router unique is not the hardware or software but its placement and role on the organization's perimeter. This role is to defend against intruders and to protect against various forms of attack.

This paper is based on the Cisco 2600 router using Internet Operating System (IOS) 11.3 as used by our organization. These security solutions should be applicable to most 'Internet Access Router' scenarios. For specific implementation procedures please follow the links as listed or refer to the 'Sources' at the end of this paper.



Why Secure your Internet Access Router?

If you are not familiar with what a Router is, I suggest you visit http://www.howstuffworks.com/router.htm.

Why would we want to secure the router that connects our Firewall to the Internet? We have a firewall so what's the point?
In a word, vulnerability. A few other words might be: Control, Power, and Ownership. We don't want to be vulnerable to attackers and we don't want to allow them to have control, power or ownership over our router (or our Internal network).
An example of a vulnerability is presented here and is followed with ways you can secure your Internet Access Router. Each of the suggestions is addressing known vulnerabilities.

If your Internet Access Router is physically accessible, an attacker can gain User EXEC mode access by logging on locally through the console or AUX port, no password is required. If you do not have a password on your Privilege EXEC account, an attacker could easily make a number of 'annoying' changes to your configuration tables and/or routing tables. Given enough time, and by accessing the User EXEC account, a skilled attacker could probably gain Privilege EXEC rights despite an encrypted password. He could then isolate your network from the Internet. Depending on your business, even a temporary service disruption could be costly. Removing the ACL (Access Control List) or modifying it to allow unimpeded access could be even worse since it probably wouldn't be immediately apparent.

So how do we secure our Internet Access Router?

1. Start by making sure the router is physically secure. Place it in a locked room or locked cabinet (or both).
2. Do all maintenance while logged on locally or
3. Restrict Telnet access to specific workstations on the internal network side of the router only.
4. Restrict and or disable all maintenance services that would allow access from outside the network (if your security policy will support it). Your network services administrators will not be happy with this restriction unless the risk can be demonstrated to be such that the inconvenience is warranted.
5. Add passwords where applicable and use the "service password encryption" command on all of the type 7 passwords to prevent these passwords from being viewed while working on the configuration table.
6. Use MD5 encryption, the "enable secret" command, on the "Privileged EXEC Mode" password (equivalent to Administrator or Root level).
7. Add an EXEC password to the AUX and Console ports.
8. Stop RIP (Router Interface Protocol) and OSPF (Open Shortest Path First) protocol on the Internet interface both inbound and outbound.
9. Disable CDP (Cisco Discovery Protocol) on all interfaces.
10. Consider disabling inbound Telnet from the Internet and even disabling the telnet listener completely (if you can accept that all maintenance and/or troubleshooting will have to be done while logged on locally).
11. Display a login banner to cover you in the event that legal action is required.
12. If possible, disable SNMP.

For detailed implementation procedures go to:
http://www.routergod.com/bastion/bastion.html or
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

Can we do more to secure our Internet Access Router?

Yes. One example would be the implementation of the Terminal Access Controller Access Control System (TACACS). This is a password validation tool that requires a separate server to authenticate the user requesting access to the router.
TACACS is the result of a need identified by the US Department of Defense and is described in (RFC) 1492. For more information see:
http://www.dtool.com/rsec.html or
http://www.cisco.com/warp/public/480/10.html

Now what?

Defense-in-depth

Every publication that speaks to the subject of Security reminds us that securing our network means more than implementing isolated security initiatives.
Defense-in-depth means layering our defenses. Now that our Internet Access Router is secure we can use it as our first line of defense in protecting our internal network.

Defense-In-Depth

By blocking the services identified in the following tables, an organization can make attacking their network so difficult that only the most determined will bother trying.

There are numerous services that can be blocked from passing through the router. Many of the services, listed in the following tables, are blocked on the 'Internet interface' at the authors site. The tables are check lists from CERT (first table) & SANS (second table).

Computer Emergency Response Team (CERT) recommends filtering these services.		
Service	**Port Type**	**Port Number**
DNS Zone transfers except from external secondary DNS servers	TCP	53
TFTP daemon	UDP	69
Link	TCP	87
SUN RPC	TCP & UDP	111
BSD UNIX	TCP	512 through 514
LPD	TCP	515
UUCPD	TCP	540
Open Windows	TCP & UDP	2000
NFS	TCP & UDP	2049
X Windows	TCP & UDP	6000+ (to 6255)

SANS recommends blocking the following where practical. Most of these services are blocked at the Authors site as well as those in the table above.		
Service	**Port Type**	**Port Number**
Small Services	TCP & UDP	20 and below
FTP	TCP	21
SSH	TCP	22
Telnet	TCP	23
SMTP (Except external mail relays)	TCP	25
NTP	TCP & UDP	37

DNS (Except DNS servers)	UDP	53
Finger	TCP	79
HTTP (Except to external Web servers)	TCP	80
POP	TCP	109 &110
NNTP	TCP	119
NTP	TCP	123
NetBIOS in Windows NT	TCP &UDP	135
NetBIOS in Windows NT	UDP	137 &138
NetBIOS	TCP	139
IMAP	TCP	143
SNMP	TCP	161 & 162
SNMP	UDP	161 & 162
BGP	TCP	179
LDAP	TCP & UDP	389
SSL (Except to external web servers)	TCP	443
NetBIOS in W2K	TCP &UDP	445
Syslog	UDP	514
SOCKS	TCP	1080
Cisco AUX port	TCP	2001
Cisco AUX port (stream)	TCP	4001
Lockd (Linux DoS Vulnerability)	TCP & UDP	4045
Cisco AUX port (binary)	TCP	6001
Common High-order HTTP ports	TCP	8000, 8080, 8888 ETC.

Blocking all the services in the tables will be impossible if you support a web server behind your Internet Access Router. For an in depth review on how to, among other things, setup a screened subnet (often incorrectly referred to as a DMZ) for your web server off your Internet Access Router see 'Top Ten Blocking Recommendations Using Cisco ACLs ' by Scott Winters www.sans.org/infosecFAQ/firewall/blocking_cisco.htm

Can we do more to protect our network using the Internet Access Router?

The following are other changes you can make to limit or prevent various attacks on your network.

- Block the following types of ICMP traffic on the 'Internet interface'—incoming echo request (ping and Windows traceroute), outgoing echo replies, time exceeded, unreachable messages and ICMP redirects.
  These changes will limit DoS attacks

- Drop and log inbound packets on the 'Internet interface' that have a source address of the internal network or 127.0.0.x or reserved address spaces (see RFC 1918)
  These changes will stop 'spoofing' and some DoS attacks.

- Drop and log outbound packets on the 'internal interface' that have a source address of anything other than an internal network address or if the source is 127.0.0.x or a reserved address (see RFC 1918). These changes will prevent internal attackers from launching some Denial of Service attacks from inside your network as well as identifying Zombie machines on your network

- Disable IP Source Routing. Unscrupulous people use IP Source Routing to generate DoS attacks (with you as the unwitting attacker) on another site or to redirect traffic to somewhere other than to whom you intended. This is one form of IP-spoofing that is easily stopped. See RFC2267 for a detailed description of IP Source-Routing at:
  http://www.cis.ohio-state.edu/htbin/rfc/rfc2267.html

- Drop and log requests for IP directed-broadcast at 'all interfaces' of all your routers not just the Internet Access Router.
  This change will prevent your network from being used or victimized by a Smurf (DoS) attack.
  Go to http://www.powertech.no/smurf/ to test your network.

- Configure NTP (Network Time Protocol) to allow updates from the internal time servers only. Disable NTP on the Internet interface inbound and outbound. Synchronizing your Internet Access Router time with the rest of your network will be invaluable in the event an attacker does break into your network. If your router log files are not time stamped in-step with the rest of your network, it will be difficult or impossible to perform a forensic audit later.

Disabling or enabling services will be unique to each organization. If you don't need a service then disable it. You can always enable it later if required.

Last Step

Now that you have your Internet Access Router secured as well as restrictions in place to protect your internal network there is one last thing to do. Test it.
Use a port scanner to see if you have missed anything that should be closed and use a packet sniffer to see what packets make it through your ACLs and what doesn't. If you have anything closed that shouldn't be, your users will let you know soon enough (proper planning should avoid this with the exception, possibly, of some unique users – there are always a few of those!)

Sources

Eldridge, Brett. "Building Bastion Routers Using Cisco IOS" Sept 9 1999 URL: http://www.routergod.com/bastion/bastion.html

Winters, Scott. "Top Ten Blocking Recommendations Using Cisco ACLs" Aug 15 2000. www.sans.org/infosecFAQ/firewall/blocking_cisco.htm

Author Unknown. "Increasing Security on IP Networks" Posted: Feb 9 2000 URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

Author Unknown. "Improving Security on Cisco Routers" Date unknown. http://www.ieng.com/warp/public/707/21.html

Author Unknown. "Your Routers are Probably Not Secure" Posting date Unknown URL: http://www.dtool.com/rsec.html

Author Unknown. "TACACS+ and RADIUS Comparison" Posting Date Unknown. Owner: Cisco URL: http://www.cisco.com/warp/public/480/10.html

Author unknown. "How Routers Work" Date unknown URL: http://www.howstuffworks.com/router.htm

Wilson, Curt. "Firewall and Perimeter Protection" Practical Assignment SANS, May 2000 URL http://www.sans.org/y2k/practical/Curt_Wilson.doc

Huegen, Craig. "The latest in denial of service attacks: (SMURFING)" 8 Feb 2000 URL: http://www.pentics.net/denial-of-service/white-papers/smurf.cgi

Graham, Robert. "The recent DDoS attacks" 10 Feb 2000 URL: http://www.robertgraham.com/op-ed/magic-ddos.html