Hardening your router in 9 easy steps

searchnetworking.techtarget.com/tip/Hardening-your-router-in-9-easy-steps

For most enterprise LANs, the router has become one of the most critical security appliances in use. Generally,...

most networks have one primary access point, which is referred to as a "border router," that is often paired with a dedicated firewall.

Configured properly, it can keep all but the most determined bad guys out, and if you want, it can even keep the good guys in. But an improperly configured router is only marginally better than having no security in place at all.

In the following tip, we'll explore nine easy steps that you can take to ensure that you have a brick wall protecting your network and not an open door.

1. Change the default password!

According to CERT/CC at Carnegie Mellon University, 80% of security incidents are caused by weak passwords. Extensive lists of default passwords are available online for most routers, and you can be sure that *someone*, somewhere knows your birthday. SecurityStats.com maintains a thorough do/don't list for passwords, as well as a password strength test.

2. Disable IP directed broadcasts

Your router is obedient. It will do what it's told, no matter who's doing the telling. A Smurf attack is a version of a Denial of Service (DOS) attack in which an attacker sends an ICMP echo request to your network's broadcast address using a spoofed source address. This causes all the hosts to respond to the broadcast request, which will slow down your network, at the very least.

Consult your router's documentation for information on how to disable IP directed broadcasts. For instance, the command "Central(config)#no ip source-route" will disable IP directed broadcasts on Cisco routers.

3. Disable HTTP configuration for the router, if possible

As outlined in a Cisco Tech Note, "The authentication protocol used for HTTP is equivalent to sending a cleartext password across the network, and, unfortunately, there is no effective provision in HTTP for challenge-based or one-time passwords."

Although it may be convenient to configure your router from a remote location (from home for example), the fact that you can do it means that anyone else can as well. *Especially* if you're still using the default password! If you must remotely manage the router, make sure that you are using SNMPv3 or greater, as it supports hashed passwords.

4. Block ICMP ping requests

The primary purpose of a ping request is to identify hosts that are currently active. As such, it is often used as part of reconnaissance activity preceding a larger, more coordinated attack. By removing a remote user's ability to receive a response from a ping request, you are more likely to be passed over by unattended scans or from "script kiddies," who generally will look for an easier target.

Note that this does not actually protect you from an attack, but will make you far less likely to become a target.

5. Disable IP source routing

The IP protocol allows a host to specify the packet's route through your network, instead of allowing the network components to determine the best path. The only legitimate use that you may come across for this feature is to troubleshoot connections, but this is rare. It's far more common to be used to map your network for reconnaissance purposes, or when an attacker is attempting to locate a backdoor into your private network. Unless specifically needed for troubleshooting, this feature should be disabled.

6. Determine your packet filtering needs

There are two philosophies to blocking ports, and which one is appropriate for your network depends on the level of security that you require.

For a high-security network, especially when storing or maintaining confidential data, it is normally recommended to "filter by permission." This is the scheme in which all ports and IP address permissions are blocked, except for what is explicitly required for network functions. For instance, port 80 for web traffic and 110/25 for SMTP can be allowed to come from a dedicated address, while all other ports and addresses can be disabled.

Most networks will enjoy an acceptable level of security by using a "filter by rejection" scheme. When using this filtering policy, ports that are not used by your network and are commonly used for Trojan Horses or reconnaissance can be blocked to increase the security of your network. For instance, blocking ports 139 and 445 (TCP and UDP) will make your network more difficult to enumerate, and blocking port 31337 (TCP and UDP) will make you more secure from Back Orifice.

This should be determined during the network planning phase, when the level of security required is compared to the needs of the network users. Check out this extensive list of ports with their normally associated uses.

7. Establish Ingress and Egress address filtering policies.

Establish policies on your border router to filter security violations both outbound (egress) and inbound (ingress) based on IP address. Except for unique and unusual cases, all IP addresses that are attempting to access the Internet from inside of your network should bear an address that is assigned to your LAN. For instance, 192.168.0.1 may have a legitimate need to access the Internet through the router, but 216.239.55.99 is most likely to be spoofed, and part of an attack.

Inversely, traffic from the outside of the Internet should not claim a source address that is part of your internal network. For that reason, inbound addresses of 192.168.X.X, 172.16.X.X and 10.X.X.X should be blocked.

And lastly, all traffic with either a source or a destination address that is reserved or unroutable should not be permitted to pass thorough the router. This can include the loopback address of 127.0.0.1 or the class E address block of 240.0.0.0-254.255.255.255.

8. Maintain physical security of the router

A router is much more secure than a hub, especially from network sniffing. This is because a router intelligently routes packets based on IP destination, where a hub broadcasts the data to all nodes. If one system that is connected to that hub places their network adapter in promiscuous mode, they are able to receive and view all broadcasts, including passwords, POP3 traffic and web traffic.

It is important then to make sure that physical access to your networking equipment is secure to prevent the placement of sniffing equipment, such as an unauthorized laptop, on the local subnet.

9. Take the time to review the security logs

Reviewing your router's logs (via its built-in firewall functions) is often the most effective way to identify security incidents, both in-progress attacks and indicators of upcoming attacks. Using outbound logs, you can also identify Trojans and spyware programs that are attempting to establish an outbound connection. Attentive security administrators were able to identify the Code Red and Nimda attacks before antivirus publishers were able to react.

Also, generally, the router is on the perimeter of your network, and allows you to get an overall picture of the inbound and outbound activity of your network.

Chris Cox is a network administrator for the United States Army, based in Fort Irwin, California.