DOWNLOAD PDF SECURING AND CONTROLLING CISCO ROUTERS

Chapter 1 : Securing Administrative Access on a Cisco Router | Demch

Securing and Controlling Cisco Routers is an important book for anyone tasked with securing routers and corporate networks. Given that Cisco dominates the router industry, this book is especially pertinent.

It may be important to note that other routers like Juniper and Force10 allow for alpha-numeric names in most if not all ACLs, and that the ACL name convention is not a standard applied to all network routers. ACLs are configured based on their protocol first. Some, but not all, ask for standard or extended qualifiers in their statements and then the numeric name is assigned. Here are some examples: Destination addresses are not considered in a standard ACL. The final two parts of the statement are associated with the source IP address and a wild card mask that determine if the address is a single host or a range of IP addresses. The second statement denies a range of IP addresses in the The range covers IP addresses, 0 to for that subnet. A shorter range is shown in the third statement, which permits IP addresses from the All comparisons start at the top of the list and work down. Once a match is made, the traffic is either permitted or denied and then comparison stops. The first statement denies IP traffic from the The second statement is similar, but denies traffic from the Single hosts in the Extended version utilize the host identifier before the IP address and no wildcard mask is required. The third statement permits TCP traffic from the Continuing down the list, the next statement denies the UDP traffic from the first IP addresses in the Cisco and other routers can associate well known ports for these protocols to acronyms for familiarity. Most routers will automatically translate the port number to these acronyms for you and you can see them in the ACL list when you perform a show ip access-list or show running config command. The next statement is slightly different. This statement permits icmp traffic, which is associated with network ping. The statement allows ICMP traffic from any source and to any destination, but uses the flag host-unreachable. This flag identifies ICMP traffic that is replied from a ping request, that the target host cannot be contacted. The final statement in the list is an implicit deny of all traffic that was not matched in previous ACL statements. Implementation of ACLs on a router interface Now that we have seen the structure of these ACLs, we need to be able configure them to a router interface. To place the ACL on the egress side, the final flag at the end would be changed to out. What Have We Learned? These topics are extremely important to understand for network security and for the Cisco network certification exams. This brief introduction to IP ACLs can start you on the journey to better understanding of this topic, but in-depth Cisco networking training can provide you with the tools you need to grasp these concepts and master them. In future articles, we will look at ACL tips and best practices that will provide real world examples and valuable information for achieving your certification. Get our content first. If this message remains, it may be due to cookies being disabled or to an ad blocker.

Chapter 2 : Security Hardening Checklist for Cisco Routers/Switches in 10 Steps

Added in Cisco IOS Software Release (1)M for the Cisco , , and Series routers, the Digitally Signed Cisco Software feature facilitates the use of Cisco IOS Software that is digitally signed and thus trusted, with the use of secure asymmetrical (public-key) cryptography.

Password cisco rocks I have no idea; please explain. The password assigned to the privilege EXEC mode will be Password cisco rocks because all spaces after the first character are part of the password. If you do a show running-config on the router, you will note that the enable secret is encrypted and the 5 after enable secret identifies that it is an MD5 hash. Here is an example to illustrate this concept: Last configuration change at NVRAM config last updated at Different Cisco routers have different ways of doing password recovery. You can get information on password recovery by doing a search on the keywords "password recovery" on http: Always use the enable secret command instead of the older enable password command; enable password uses a very week encryption algorithm. Password recovery on the router can only be done using the console port. The console port allows a hard break signal that interrupts the boot sequence of the router. You can issue the break sequence on a router within 60 seconds of the reboot, and it gives complete access to the user issuing this command. Cisco routers are vulnerable if you have physical access to the devices. However, if someone is trying to access the console port of the router remotely, you can apply an additional layer of security by prompting the user for a password. Here is how you protect the console port on the router: Remember, to assign a password to the console port of the router, you first have to access the global configuration mode of the router. Once in the global configuration mode, you access the console port by issuing the line console 0 command. Remember, the console port is always 0 because there is only one console port on every Cisco device, and Cisco starts its numbering of the ports with 0: This password by default is not encrypted: Router config-line password Ciscorocks Once you issue the password command, you issue the login command. The login command tells the router to ask for the password when someone is typing to access the router using the console port: Router config-line login When you do a show running-config on the router, you note that the password is not encrypted. This output is truncated to fit the page; however, you must note that the line console information is always at the bottom of the configuration: There is built-in security on the VTY lines that mandates the use of passwords to access the router via a Telnet session. If a Telnet session is initiated to a router that does not have a password assigned to the VTY lines, the following message appears on the screen: Password required, but not set Connection closed by remote host Figure 3. Essentially, no Telnet sessions are allowed to the router. This measure is good security, but it disallows everyone to access the router, even the legitimate user. To remotely manage the routers using Telnet, it is imperative that you assign a password to the VTY lines. Here is how you protect the Telnet lines on the router: The only difference is the following line: Router config line vty 0 4 This line can be interpreted as follows: As we said earlier, by default, Cisco routers allow up to five simultaneous Telnet sessions, and in the Cisco world, all counting begins with 0. Hence, 0 4 would give you five Telnet lines. You can assign separate passwords to each and every line. However, managing the passwords becomes an administrative nightmare. You should consider a few guidelines when configuring VTY access to the router: If there is no password set on the router to access the privilege EXEC mode, you will not be able to access the privilege EXEC mode of the router via the Telnet session. Telnet transmits and receives all data in cleartext, even the passwords. You can provide additional security by using access lists to manage administrative access to the routers from specific IP addresses. Remember, Cisco routers work with SSH1 only. Make sure you have a password assigned to the VTY lines of the router; otherwise, no one will be able to access the router via Telnet. Do not use Telnet, use SSH instead. SSH encrypts all data flowing between you and the router, thus providing high-level security. The aux port on the router is another way you can gain access to the router. You can protect the aux port on the router by assigning a password to it. Here is how you accomplish the task: If you are not using the aux port on the router, you can disable it by issuing the following command: Router config line aux 0 Router config-line no exec Figure 3. The no exec command disables all EXEC sessions to the router via that port. Encrypting All Passwords on the

Router By default, only the enable secret password is encrypted. To encrypt all other passwords configured on the router, issue the following command in global configuration mode: Router config service password-encryption In Figure 3. The service password-encryption command uses a Cisco proprietary Vigenere cipher to encrypt all other passwords on the router except the enable secret password which uses MD5. The Vigenere cipher is easy to break, and if you do a show running-config on the router, it appears as follows: The number 7 after the keyword password indicates that the password has been encrypted using the Vigenere cipher. This command does not change the fact that the Vigenere cipher can be cracked. Configuring Session Activity Timeouts You can also control access to the router by configuring activity timeouts. You can use the exec-timeout command to accomplish this task. Here is an example of the configuration: This command sets the no activity timeout to 5 minutes. Setting a lower activity timeout automatically locks up the console once the timeout expires. Configuring Access Levels on the Router You can configure access levels on the routers so the junior administrators do not have complete access to the router. Cisco routers have 16 different privilege levels that you can configure. The 16 levels range from 0 to 15, where 15 is equal to full access. You can customize levels 2 to 15 to provide monitoring abilities to the secondary administrators. Here is a sample configuration for privilege levels on the router: Central config username junioradmin privilege 3 password 0 s3cUr! Central config privilege exec level 3 ping Central config privilege exec level 3 traceroute Central config privilege exec level 3 show ip route Central config-line line vty 0 4 Central config-line password CisC0r0cK5 Central config-line login local Figure 3. Notice that in addition to the login local command a password is configured on the VTY lines. However, users will need to use the local router database to log in to the VTY lines because the login local command takes precedence over the password command. Looking at this config, whenever junioradmin logs into the router, he or she is allowed only three commands: Using the privilege command, you can provide another layer of security to your network backbone. Configuring Routers with a Statutory Warning It is imperative that you configure a statutory warning on all your networking devices that clearly states the repercussions of attempting to log on to an unauthorized system. You can achieve this by using various banner messages: You can configure a few more banner messages on routers to ensure that you get the word out that unauthorized users will be prosecuted. Do not use such phrases as "Welcome to the ABC Network" because they can create a loophole that a hacker can use to avoid legal action. We highly recommend that you consult your legal department to come up with the correct verbiage. SNMP uses community strings that act as the passwords to access the routers. Whenever you are setting up SNMP community strings, make sure you know which strings will have read-only access; which ones will have read-write access; and, most of all, which systems will be allowed SNMP access via ACLs.

Chapter 3 : Securing Networks: Access Control List (ACL) Concepts | Pluralsight

Cisco routers work together to extend corporate security to your branch and WAN to defend your entire network. With integrated network security, you get protection against sophisticated threats while maintaining outstanding performance and lowering costs.

Access Control List ACL Concepts - select the contributor at the end of the page - This article is the start of a new series centered in IT Security , but focused on securing networks with access control lists, commonly referred to as ACLs. Future articles will focus on their implementation on Cisco routers, specific designs for permitting and denying services, and venture into the world of firewalls. What are Access Control Lists? ACLs are a network filter utilized by routers and some switches to permit and restrict data flows into and out of network interfaces. When an ACL is configured on an interface, the network device analyzes data passing through the interface, compares it to the criteria described in the ACL, and either permits the data to flow or prohibits it. There are a variety of reasons we use ACLs. The primary reason is to provide a basic level of security for the network. ACLs are not as complex and in depth of protection as stateful firewalls, but they do provide protection on higher speed interfaces where line rate speed is important and firewalls may be restrictive. ACLs are also used to restrict updates for routing from network peers and can be instrumental in defining flow control for network traffic. When do we use Access Control Lists? As I mentioned before, ACLs for routers are not as complex or robust as stateful firewalls, but they do offer a significant amount of firewall capability. As an IT network or security professional, placement of your defenses is critical to protecting the network, its assets and data. ACLs should be placed on external routers to filter traffic against less desirable networks and known vulnerable protocols. One of the most common methods in this case is to setup a DMZ, or de-militarized buffer zone in your network. This architecture is normally implemented with two separate network devices. An example of this configuration is given in Figure 1. The most exterior router provides access to all outside network connections. This router usually has less restrictive ACLs, but provides larger protection access blocks to areas of the global routing tables that you wish to restrict. This router should also protect against well known protocols that you absolutely do not plan to allow access into or out of your network. In addition, ACLs here should be configured to restrict network peer access and can be used in conjunction with the routing protocols to restrict updates and the extent of routes received from or sent to network peers. The internal router of a DMZ contains more restrictive ACLs designed to protect the internal network from more defined threats. ACLs here are often configured with explicit permit and deny statements for specific addresses and protocol services. Regardless of what routing platform you utilize, all have a similar profile for defining an access control list. More advanced lists have more distinct control, but the general guidelines are as follows: Access control list name depending on the router it could be numeric or combination of letters and numbers A sequence number or term name for each entry A statement of permission or denial for that entry A network protocol and associated function or ports Examples include IP, IPX, ICMP, TCP, UDP, NETBIOS and many others Destination and Source targets These are typically addresses and can be defined as a single discrete address, a range or subnet, or all addresses Additional flags or identifiers These additional statements request additional functions when a match is found for the statement. These flags vary for each protocol but a common flag added to statements is the log feature that records any match to the statement into the router log What Types of Access Control Lists Are There? There are several types of access control lists and most are defined for a distinct purpose or protocol. On Cisco routers, there are two main types: These two types are the most widely used ACLs and the ones I will focus on in this and future articles, but there are some advanced ACLs as well. The router will identify this new traffic flow and create an entry in a separate ACL for the inbound path. Once the session ends, the entry in the reflexive ACL is removed. Cisco implementations utilize IOS Firewall capabilities and do not hinder existing security restrictions. Implementation of ACLs on a Router Interface Placement and understanding of the traffic flow is important to understand up front before you configure an ACL on a router interface. Trust me, it happens to us all and I am not immune to that one. Figure 2 provides a good example of the traffic flow when it comes to ingress and

egress on a router network interface. As you can see from this diagram, ingress traffic flows from the network into the interface and egress flows from the interface to the network. IT network and security professionals must pay close attention here. ACLs start with a source address first in their configuration and destination second. As you configure an ACL on the ingress of a network interface it is important to recognize that all local network or hosts should be seen as sources here, and the exact opposite for the egress interface. What makes this most confusing is the implementation of ACLs on the interface of a router that faces an external network. Look back at Figure 1. In that example, the ingress side is coming from the outside network and those addresses are considered to be sources, while all internal network addresses are destinations. On the egress side, your internal network addresses are now source addresses and the external addresses are now destinations. As you add ports in extended ACLs, confusion can mount. We will cover more of these implementations later in ACL configuration articles. Summary Access control lists are a principle element in securing your networks and understanding their function and proper placement is essential to achieving their best effectiveness. Certification training covers ACLs and there are several questions on exams that concern them. As we continue in this series, it would be wise to test some of the concepts on network simulators or unused router ports to gain a better perspective using ACLs and how they may be represented in actual implementations and on the exams. Ready to test your skills in Computer Networking? See how they stack up with this assessment from Smarterer. If this message remains, it may be due to cookies being disabled or to an ad blocker.

Chapter 4 : How To Secure Your Cisco Router Using Cisco AutoSecure Feature

Securing and Controlling Cisco Routers demonstrates proven techniques for strengthening network security. The book begins with an introduction to Cisco technology and the TCP/IP protocol suite.

Posted on November 11, by Demch Routers are a key component in our network. Controlling access to the router and monitoring or reporting on activity going on the router is essential in maintaining security of our network. And for Cisco routers, we have different options on securing access to the router. Below are some of our choices: Do we want to use aaa new-model or not. To use line passwords or use the local database. Use views to control administrative access to the router. For most cases, local database is preferred to secure the router instead of line passwords. And views can be used if you want to give access to a junior network administrator and limit the commands you allow them to access. Note that if you want to use views, then you also need to use aaa new-model. It may not be the best, but it works for me. I would set the hostname and domain name of the router and disable ip look up which could make the router unresponsive when entering wrong commands. When your computers use the router as their DNS server, the DNS queries are passed to the name server you configure as below: Router-HK config ip name-server 4. I would set the privileged mode secret and enable password encryption. I would create at least 2 users, one with privilege level 15 as admin and another ordinary user. Usually I set the admin secret same as enable secret as it is easier to remember. Creating the local user database before enabling the aaa new-model is important. If you forgot, you might be locked out of your router. We can further enhance the security of the router by logging synchronously with the console and set a time out if the user is idle for a certain number of minutes and seconds. We can also apply this to the aux and vty lines. Notice that since we are using aaa new-model, local user database is use and any line password or login setting we set before we issue the aaa new-model has now been removed. Below, we set the timeout for the console, aux and vty lines to be 5 minutes and 0 seconds. We also specify ssh as the secure login for the vty and telnet will not be used as it is not as secure and connect in the clear text. Router-HK config line console 0.

Chapter 5 : Practical Cisco Routers (Practical series) - PDF Free Download

Summary Securing and Controlling Cisco Routers demonstrates proven techniques for strengthening network security. The book begins with an introduction to Cisco technology and the TCP/IP protocol suite.

Follow these steps first Before you change your settings, follow these steps: Make sure that your Wi-Fi devices support the settings this article recommends. Forget or remove the Wi-Fi settings for your network from any devices that connect to your Wi-Fi router. This will prevent the devices from attempting to connect to your network with the old configuration. Configure all Wiâ€”Fi routers on the same network with the same settings. Otherwise, devices could have difficulty connecting to your network, or your network could become unreliable. It is case sensitive. Some common default SSID names to avoid are linksys, netgear, dlink, wireless, 2wire, and default. This could cause them to fail to automatically connect to your network, or to connect to other networks that share the same SSID. It might also prevent Wi-Fi devices from using all routers in your network, or prevent them from using all available bands of a router. This option might be incorrectly referred to as a closed network, and the corresponding nonhidden state might be referred to as broadcast. You should always enable security on your Wi-Fi router. Disabled When enabled, this feature allows a user to configure a list of MAC addresses for the Wi-Fi router, and restrict access to devices with addresses that are on the list. Security The security setting controls the type of authentication and encryption used by your Wi-Fi router, which allows you to control access to the network and specify the level of privacy for data you send over the air. For compatibility, reliability, performance , and security reasons, WEP is not recommended. WEP is insecure and functionally obsolete. Anyone can join your Wi-Fi network, use your Internet connection, access any shared resource on your network, and read any traffic you send over the network. Using an unsecured network is not recommended. Different Wi-Fi routers support different radio modes, so the setting varies depending on the router. In general, enable support for all modes. Devices can then automatically select the fastest commonly supported mode to communicate. Choosing a subset of the available modes prevents some devices from connecting. Also, choosing a subset of the available modes might cause interference with nearby legacy networks, and nearby legacy devices might interfere with your network. Newer standards support faster transfer rates, and older standards provide compatibility with older devices and additional range. Choosing a subset of the available modes prevents older devices from connecting. Channel This setting controls which channel your Wi-Fi router uses to communicate. Auto For best performance, choose "Auto" mode and let the Wi-Fi router select the best channel. Read about possible sources of interference. However, larger channels are more subject to interference and more likely to interfere with other devices. A 40MHz channel is sometimes called a wide channel, and a 20MHz channel is a narrow channel. Using 40MHz channels in the 2. A 40MHz channel might also cause interference and issues with other devices that use this band, such as Bluetooth devices, cordless phones, and neighboring Wi-Fi networks. Larger channels are more susceptible to interference, and more likely to interfere with other devices. Interference is less of an issue in the 5GHz band than in the 2. Once assigned, devices use these addresses to communicate with each other and with computers on the Internet. The functionality of a DHCP server can be thought of as similar to a phone company handing out phone numbers, which customers then use to call other people. If more than one device has DHCP enabled, you will likely see address conflicts and have issues accessing the Internet or other resources on your network. The functionality of a NAT provider is like that of a worker in an office mail room who takes a business address and an employee name on incoming letters and replaces them with the destination office number in a building. This allows people outside the business to send information to a specific person in the building. This is usually your cable modem, your DSL modem, or your standalone router, which might also act as your Wi-Fi router. Disabling WMM can cause issues for the entire network, not just Apple products on the network. Location Services Some countries or regions have regulations that affect wireless signal strength and the use of Wi-Fi channels. When you travel to other countries or regions, make sure that your devices have Location Services turned on so that you can connect to Wi-Fi networks in that country or region. Click in the corner of the window, then enter your password. Scroll

to the bottom of the list of apps and services, then click the Details button next to System Services. In the Details dialog, select Wi-Fi Networking. On your iPhone, iPad, or iPod touch: Wireless carrier Wi-Fi networks Wireless carrier Wi-Fi networks are networks configured by your carrier and their partners. Your iPhone treats them as known networks and automatically connects to them. Tap next to the network name and then turn off Auto-Join. Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. Risks are inherent in the use of the Internet. Contact the vendor for additional information. Other company and product names may be trademarks of their respective owners. Mon Jul 23

Chapter 6 : calendrierdelascience.com: Customer reviews: Securing and Controlling Cisco Routers

Securing A Cisco Router: The Basics Take these steps for basic security. While installing a new Cisco router for a client recently, I was a bit surprised that there was no firewall.

Share on Facebook Cisco manufactures a wide range of hardware products including wireless routers. Your Cisco wireless router plays a big role in how well the internet works on your devices, so it may be necessary to access and tweak the router settings from time to time. Depending on the type of reset you perform, you can fix settings that were misconfigured and reset an internet connection that has suddenly slowed down or cut out entirely. There are two types of resets you can perform: You perform a soft reset by unplugging the power adapter from the router and the outlet. Leave it unplugged for a couple of minutes and then plug it back in. Wait 5 to 10 minutes for the router to reset and then try to use the internet on your device. If everything is working, your router is fixed. Press the small "Reset" button on the back of the router and hold it down for 30 seconds. You may need to use a pen, pencil or paperclip to do this as the button is tiny. The router completely resets at this point, and you have a clean slate to configure the router as you want. Cisco Linksys Router Login Cisco owned Linksys from to , so if you have a Linksys router in your home, there is a chance that it is a Cisco model. You can log in to your Cisco wireless router control panel to change things such as the wireless password and network name, the parental controls, the firewall and IP settings. Open your internet browser of choice and type the address http: Type in the username and password for your router. If you never set a username and password, use the default settings by leaving the username field blank and entering the password "admin. Cisco Wireless Router Login When Cisco sold Linksys in , it moved to manufacture small business and enterprise products. You may have a Cisco business router in your home that comes with advanced settings and features that are appealing in residential applications. In this case, you log in to your Cisco business router by opening an internet browser and going to Click the "OK" button to log in. You can change all the same settings as in the Cisco Linksys router control panel plus advanced settings such as port forwarding and more.

Chapter 7 : How to Secure Your Wireless Router | calendrierdelascience.com

Cisco Wireless Router Login When Cisco sold Linksys in , it moved to manufacture small business and enterprise products. You may have a Cisco business router in your home that comes with advanced settings and features that are appealing in residential applications.

Deny all other ip traffic explicitly and log it. Non-commented lines are the actual configuration syntax as it would be entered on the Cisco router. The information supplied in this configuration is in no way guaranteed or supported by the author to "secure" your network. This is meant to provide an example of generally accepted configuration practices when securing routers that provide access to untrusted networks. This access-list should be applied inbound on your choke router to what is considered your internal or inside interface. In most cases, this will be some sort of ethernet interface. This filters traffic that is going towards the Internet or untrusted network "inbound on that interface. Deny RFC private source addresses from going outbound. It is not wise! This is the primary way that hackers learn about the configuration of private! These packets can not be responded to anyway, since these networks are! Keep any errant request for private addresses inside your network! Just in case your internal routing table for some reason does not contain a route! This is another way that hackers! Deny all netbios traffic going outbound since this is one of the top 3 most hacked! Users should not access netbios services on! Permit everything else from the "external network" and build the! This command allows all other traffic to pass through the interface and! I recommend at least a series! If this router is not being used as a firewall but more for just a choke device! You should specifically define your networks that should!

Chapter 8 : News, Tips, and Advice for Technology Professionals - TechRepublic

Securing and Controlling Cisco Routers. Uploaded by. Juan JosÃ© Castro. Download with Google Download with Facebook or download with email. Securing and Controlling.

Chapter 9 : Securing and Controlling Cisco Routers | Juan JosÃ© Castro - calendrierdelascience.com

Securing Administrative Access to a Cisco Router Configuring administrative access on the Cisco router is an important step toward network security. You can access all Cisco routers in various ways.