

*Cisco ASA firewall basics. Last updated with new videos! In the course you will learn everything needed to install and configure a brand new Cisco ASA firewall with outbound internet access.*

Example shows a summary of the boot process for an ASA appliance whose factory settings have not been changed yet. Following a successful load of the OS image, a prompt offering an interactive preconfiguration of the device using menus is presented. You do not need to analyze this option because it provides little flexibility. The use of the question mark? This CLI help is useful, quickly becoming part of everyday life for anyone who works with Cisco equipment. Mon Aug 21 Boot configuration file contains 1 entry. Cisco ASA on-board accelerator revision 0x0 Boot microcode: Displaying all the commands available on the EXEC mode with a "? Display information about disk0: Display information about flash: The data returned after its execution includes OS version and hardware components, licensed features, the serial number, and even the uptime since the last reboot. The enable command with a BLANK password for a device with no initial configuration provides access to the privileged mode, recognized by the symbol after the device hostname. This is illustrated in Example , which also shows the access to config mode through the configure terminal command. Some of the specific config modes aaa, interface, ip, router, and so on are included in the example. NOTE At this point, you are encouraged to sequentially explore the help? In a similar fashion, it is also worth it to start playing with the show command parameters accessible from the ASA privileged mode. NOTE It is naturally advisable to use the enable password command at configuration level to change the default BLANK password into a new one defined by the device administrator. This simple action restricts access to the privileged mode and consequently the right to issue any configuration command. Sample show version Command for ASA! Entering configuration config mode and displaying available options ciscoasa configure terminal ciscoasa config? Other user databases are analyzed in Chapter 14, "Identity on Cisco Firewalls. The first sample uses the begin filter and instructs the OS to start displaying the line of configuration or show command where the keyword being searched snmp in this case first appears. The second exemplified filter uses the include option, which determines that all lines of the command output that include a match for the searched string should be displayed. The show running-configuration command displays the active configuration of the device and typically results in a large amount of data. More recent versions of ASA OS enable the output of this command to be broken in configuration blocks related to a specific topic. Example illustrates how to employ this resource to restrict the output only to the commands related to timeout information. NOTE Another classic filter is the combination exclude, which displays only the lines that do not contain the searched string. Even more complex regular expressions may also be constructed, and a whole chapter could be devoted to this subject, which is not the plan for this book. The book starting at this chapter brings numerous examples of practical usage, but an investigative spirit is the main asset that you must possess to benefit from these powerful resources. Establishing the point where the display should begin ciscoasa show running-config begin snmp no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart crypto ipsec security-association lifetime seconds crypto ipsec security-association lifetime kilobytes telnet timeout 5! Searching for all matches of a certain string case sensitive ciscoasa show running-config include icmp icmp unreachable rate-limit 1 burst-size 1 timeout conn 1: Delimiting the section of the running configuration to be displayed ciscoasa show running-config timeout timeout xlate 3: It makes life a lot easier by reducing the time you spend typing commands. It is certainly worth the investment. Basic Configuration for ASA Appliances Other Than Having powered up an ASA appliance and knowing the basics about command execution modes, it is time to examine some of the fundamental interface configuration tasks: Enter interface configuration mode and enable the interface for transmitting and receiving traffic: This mode is indicated by the prompt config-if. At this phase the no shutdown command needs to be issued to remove the interface from the administratively down state. If logical subinterfaces have been configured, the pertinent VLAN information to match that of the switch to which the firewall connects to should be added. You can also change the speed and duplex. Assign a logical name to the

interface: This is accomplished with the `nameif` command, and the configured name is used in any future reference to the interface. It is typically easier to remember the logical meaning of an interface than the physical. Assign a security-level to the interface: To reflect the degree of trustworthiness of a given firewall interface, Cisco introduced in the early days of the PIX Firewalls the concept of Security Level. The value of the Security Level or simply `sec-lvl` ranges from 0 to 15, in which the highest possible value, 15, is used for the most trusted network under the firewall control, which is, by default, called inside. Conversely, the name outside is reserved for the less trusted network frequently the connection to the Internet and, by default, the value 0 is assigned to its `sec-lvl`. Assign an IP Address to the interface: You can do this either through static or dynamic means using the `ip address` command. Figure shows the physical and logical reference topologies for the analysis of an ASA basic setup. Example assembles the typical configuration commands, and Example displays some commands to obtain information about the ASA interfaces. Testing the reachability of local hosts with the `ping` command `ASA1 ping` The other ASA models have only routed interfaces. The operational aspects that deserve special attention are discussed in this section. Figure shows a sample topology that serves as the base for exploring the ASA platform. Physical interfaces can be configured in either access or trunk mode, as registered in Example This is much like any Cisco Catalyst switch configuration. On Catalyst switches, the L2 portion must be defined by means of the `Vlan` command. Example relates to Figure and documents the commands employed to verify the existent VLANs and their assigned ports. The typical outputs of the `show interface options physical interface` and `interface vlan` are registered in this example, which also displays a changed hostname for the appliance ASA instead of the default `ciscoasa`. **Baseline ASA Configuration!** Physical Interface operating as a This is accomplished with the command `copy running-config startup-config` or with the well-known old version `write memory`.

### Chapter 2 : How to configure DNS on ASA firewall ? - Cisco Community

*Basic ASA Configuration. Before dealing with any specific configuration procedure for the Adaptive Security Appliance (ASA), you need to understand a set of basic concepts.*

We are going to use three of the interfaces in this network – inside, dmz1 50 and outside 0. You do not need an ACL because all outbound traffic is traversing from higher security level inside and dmz1 to lower security level outside. The reason we want to give it the least preference is to avoid possible conflict with other NAT rules. Next is configuring a default gateway and route all traffic to the upstream ISP. It allows icmp return traffic to pass the ASA while the Ping is initiated from inside hosts. Configure static NAT to web servers, grant Internet inbound access to web servers First we define two objects for the web server, one for its internal IP and one for its public facing IP. Now the IP address translation has been done. We will need to configure ACL and allow Internet inbound traffic to access the web server. And apply the ACL to the outside interface. For troubleshooting and demonstration purpose, we also allow ICMP ping traffic. In a real-world network, I recommend disallow Ping for higher security. Specify a DHCP address pool and the interface for the client to connect. We reserve a few address before and after the pool for future network devices or appliances that require static IP. It is always a good idea to have the secondary DNS server in case the primary fails. This lease equals the amount of time in seconds the client can use its allocated IP address before the lease expires. Enter a value between 0 to 1,, The default value is seconds. The subscription based licenses can be purchased annually, 3 or 5 years with discount. Here are list of licenses available: Do you really want to replace them? Configure time and enable logging It is important to enable logging so we know what happened in case there was an incident. Make sure time is set correctly and timestamp is enabled while logging. The maximum log size can grow up to MB and then the oldest logs are overwritten. ASA1 clock set For a more comprehensive, multi-DMZ network configuration example please read: You may use it on any compatible ASA devices. It is fully configured lab based on the requirements in the article. As part of our documentation effort, we maintain current and accurate information we provided. Documentations are routinely reviewed and updated. We ask for your email address to keep you notified when the article is updated.

## Chapter 3 : 6 Steps Cisco ASA Basic Configuration Tutorial

*ASA Firewall Course Description In these lessons you will learn how to configure everything the Cisco ASA firewall has to offer NAT, IPSEC/SSL vpns, Anyconnect remote VPN, failover, and many other things.*

Testimonials I am using it everyday! I recommend it to everyone. All the topics are explained with various configuration examples, which is very useful to understand the technologie. I recommend it to everyone! I have no doubt in saying that signing up for membership was the best investment I have spent on learning networking. I only wish I would have started reading NetworkLessons. Every lesson is set up in a way that makes learning interesting and fun. He has a genuine desired to help others to grasp all network concepts. The one aspect I enjoy the most are the live demonstrations he includes with each lesson. The labs presented in his lessons are easily reproducible in GNS3 which has allowed me to hone my skills. Nice drawings of the scenarios. Their courses are ordered in a way that you can find answers to questions you got fast. I really recommend their materials! I used their lessons as part of my CCNA certification preparation and look there: Thanks a lot for a great learning experience! All topics are explained very well in an understandable language. I will also use it for my CCNP preparation. It looks like his videos on NetworkLessons. He is just that kind of guy the greatest. The tutorials here are easy to understand and straight to the point! I recommend starting your networking career with NetworkLessons. It gives basic and advanced knowledge in all networking and security topics. A great tool to gain, upgrade or refresh your knowledge. I look forward to using this site for many future certifications.

## Chapter 4 : How to Configure a Cisco ASA Firewall - Basic Configuration Tutorial

*Cisco ASA firewall basics ASA models There are two flavors, physical and virtual. The virtual one is relatively new, and is known as the ASA v ('v' for virtual, it makes sense). The physical range of ASA firewalls ( series) has been around for a number of years and replaced the PIX firewalls.*

This step is essential and will help the ASA Firewall understand which interface is connected to the trusted private and untrusted public network: Security level for "inside" set to by default. Security level for "outside" set to 0 by default. The ASA Firewall will automatically set the security level to for inside interfaces and 0 to outside interfaces. Traffic can flow from higher security levels to lower private to public , but not the other way around public to private unless stated by an access-lists. To change the security-level of an interface use the security-level xxx command by substituting xxx with a number from 0 to The higher the number, the higher the security level. DMZ interfaces are usually configured with a security level of In case the public interface VLAN2 is configured using the ip address dhcp setroute command, configuration of the default gateway is not required. ASA config route outside 0. ASA config ping Usually these networks can be reached via a Layer3 switch or an internal router. These additional networks are contactable via a Layer3 device with IP address ASA config route outside Network Address Translation is essential to masquerade our internal network using the single IP address our Public interface has been configured with. Network Address Translation, along with all its variations Static, Dynamic etc , is covered in great depth in our popular Network Address Translation section. We will provide both commands to cover installations with software version up to v8. The following commands apply to ASA appliances with software version up to 8. Another method of configuring NAT is with the use of access lists. With software version 8. The following commands software version 8. ASA config object network network1 ASA config-network-object nat inside,outside dynamic interface!

### Chapter 5 : HOW TO: ASA Firewall basic configuration lab â€“ NetFixPro

*The Cisco ASA Firewall is the smallest model in the new Cisco series of hardware appliances. Although this model is suitable for small businesses, branch offices or even home use, its firewall security capabilities are the same as the biggest models ( , , etc).*

Testimonials Comprehensive Networking Foundation One of my favorite features of the site in general is the context sensitive keyword search feature in the upper right hand corner. This is my first favorite resource when looking for information on a topic I am unclear of. The site provides comprehensive coverage of all the CCNA topics. The course material is clear and concise with Rene giving video white board explanations making abstract networking concepts appear tangible. If you are looking for an entry point into the world of Cisco routing and switching, Networklessons. I have been searching a lot for network review materials and many people make networking sound difficult. When I came across Networklessons. The course material is easy to understand even the most difficult and complicated topics. Then everything comes into light. They go straight to the point, period! Ramos Network Design September 10, Taking Network Technologies to the Street The lead instructor Rene has the ability to explain the most complex concept into very straightforward and easy to understand units. Thank you Rene and your crew , for your great work! Then started studying with NetworkLessons. You can also discuss with other members if you want or suggest to prepare lessons about some latest networking industry features like Vxlan, Segment Routing, EVPN, etc. You guys are doing a great job! Subrata Sen Ryerson University September 5, Easy To Read There are a lot of websites with content about computer networks but on networklessons I found the best and easy to read articles to help me prepare for Cisco exams. I am very happy and excited about each subject that I have learned! Accurate and very good in explaining technical networking topics materials. The network topics are very well explained, and the videos are helpful too. Questions are answered quickly and to the point. Before I became a member, it took me 3 years to come to the understanding of how multicast sparse mode works; simply because I could not find anything that explained the whole process as simple and clear as Networklessons. I will continue to use Networklessons. Since I changed job from System Engineer to Pre Sales, I have been asked to certify for CCNP and going through the official Cisco certification guides is not only a hassle but sometimes you read on difficult subjects and the way it is explained is sometimes more difficult than it actually is. Regardless of your expertise, Networklessons. Difficult topics are brought in a easy readable format and looking at the whole package, including GNS3Vault labs, makes Networklessons a must have when you want to certify or grow in the job. It is fantastic that a person is so dedicated to help others on difficult topics.

### Chapter 6 : Firewall Fundamentals

*This article gets back to the basics regarding Cisco ASA firewalls. I'm offering you here a basic configuration tutorial for the Cisco ASA security appliance. This device is the second model in the ASA series (ASA , , etc) and is fairly popular since is intended for small to medium enterprises.*

### Chapter 7 : Basic ASA Configuration > Cisco Firewall Configuration Fundamentals

*Basic firewall functionality is explained, along with VLAN and port configuration. Proper use of the console port is covered, plus the use of a USB-to-Serial adapter cable. Software version*

### Chapter 8 : Cisco ASA Erase Configuration | calendrierdelascience.com

*This Cisco ASA Tutorial gets back to the basics regarding Cisco ASA firewalls. I'm offering you here a basic configuration tutorial for the Cisco ASA security appliance but the configuration applies also to the other ASA models as well (see also this Cisco ASA Basic Configuration).*

## Chapter 9 : Basic Troubleshooting For traffic throu - Cisco Community

*Cisco ASA X Series Firewalls. This chapter describes how to configure basic settings on your ASA that are typically required for a functioning configuration.*