Cisco asa 8.2 config guide

Some links below may open a new browser window to display your chosen document. Firepower Center Configuration Guide, 6.6 31/aug/2020Updated Firepower Management Center Configuration Guide, Version 6.5 18/Sep/2020Updated Firepower Management Center Configuration Guide, Version 6.4 18/Sep/2020Updated Firepower Management Center Configuration Guide, Version 6.2.3 18/Sep/2020Updated FirePower Center Configuration Guide, Version 6.2.2 16/Apr/2020 Center for FirePower Control Configuration Guide, Version 6.2.1 16/Apr/2020 FirePower Control Center Configuration Guide, Version 6.1 16/Apr/2020 FirePower Control Center Guide, Version 6.2 16/Apr/2020 Center for Firepower Management Guide to Configuration, Version 6.2 16/Apr/2020 Center for FirePower Control Guide to Configuration Guide, Version 6.2 16/Apr/2020 Center for FirePower Control Guide to Configuration Guide, Version 6.2 1 6.0.1 06/May/2020 FirePower Control Center Configuration Guide, Version 6.0 25/Apr/2019 FireSIGHT System User Version 5 .4.1 02/Feb/2017 ASA FirePOWER User Guide Module , ASA5506H-X, ASA5506W-X, ASA5508-X, and ASA5516-X , Version 5.4.1 26/Feb/2015 FMC and FTD Network Management Administration 22/Apr/2020 Cisco Fire Threat Defense Exercise Guide, Version 6.4 10/May/2019 Cisco AnyConnect Deployment Guide for Cisco Jabber This chapter describes how to access the command-line interface, adjust the firewall mode, and work with the configuration. This chapter includes the following sections: Starting with your platform model ,Default Configuration Factory Access to the command-line interface Installing a transparent or route firewall mode Working with configuration This guide extends to several platforms and security models: the PIX 500 series of security devices and the ASA 5500 series of adaptive security devices. There are some hardware differences between PIX and asa security device. In addition, the ASA 5505 includes a built-in switch, and requires some special configuration. For these hardware differences, supported platforms or models are marked directly in each section. Some models don't support all of the features covered in this guide. For example, the ASA 5505 adaptive security device does not support security contexts. This guide may not list every model you support when discussing the feature. To identify the features that are supported for the model before the configuration starts, see the Supported Platforms and Feature License section on page A-1 for a detailed list of features supported for each model. The default factory configuration is a configuration that Cisco applies to new security devices. The default configuration is supported on all models, with the exception of the PIX 525 and PIX 535 security devices. For PIX 515/515E and ASA 5510 and High-security factory configuration by default customizes interface interface control so you can connect to it with ASDM, with which you can complete the configuration. For an adaptive security device, the ASA 5505 factory configuration adjusts the interfaces and NAT by default so that the security device is ready for immediate use on your network. The default factory configuration is only available for the firewall route mode and the single-context mode. Read more about the multiple context mode in Chapter 3 Of The Multiple Context Mode. For more information on the route and transparent mode of the firewall, please visit the Installing Transparent or Route Firewall Mode section. This section includes the following themes: Restore the default factory configuration of ASA 5505 Default Configuration ASA 5510 and higher default configuration PIX 515/515E Default Configuration to restore the default configuration of the plant, Enter the following command: host name (configuration) sets up the default plant (ip_address mask) If you specify ip_address, you will set the ip address of the internal or management interface, depending on your model, instead of using the default IP address 192.168.1.1. The http team uses this subnet. Similarly, the range of dhcpd commands consists of addresses in the subnet that you specify. Once the configuration is restored by default, save it in the internal flash memory with the recording memory command. The record memory team keeps the execution configuration in place by default for the startup configuration, even if you've previously set up a download configuration command to establish a different location; When the configuration was cleared, this path was also cleared. Please note that this command also cleans the download system command, if present, along with the rest of the configuration. The download team allows you to download from a specific image, including an image on the external Flash memory card. The next time you restart your security device after restoring the plant configuration, it is loaded from the first image into the internal flash memory; If you don't have an image in your internal flash, the security device doesn't load. To set up additional settings useful for the full configuration, see the default factory configuration for the ADAPTIVE security device ASA 5505: Inside the VLAN 1 interface, which includes Ethernet 0/1 switch ports in 0/7. If you haven't installed an IP address in the default factory setting team, the IP address and the VLAN 1 mask are 192.168.1.1 and 255.255.255.0. The external interface of VLAN 2, which includes the switch port Of Ethernet 0/0. VLAN 2 receives its IP address using DHCP. The default route is also derived from the DHCP. All IP addresses are translated when accessing the outside using the PAT interface. By default, inside users can access the outside with an access list, and users can't access the inside. The DHCP server is enabled on the security device, so the computer connected to the VLAN 1 interface receives an address between 192.168.1.2 and 192.168.1.254. The HTTP server is enabled for ASDM and is available to users on the 192.168.1.0 network. The configuration consists of the following commands: interface Ethernet 0/0 switchport access vlan 2 no interface shutdown Ethernet 0/1 switchport access vlan 1 no interface shutdown Ethernet 0/2 switchport access vlan 1 no interface shutdown Ethernet 0/3 switchport access vlan 1 interface no interface there is no shutdown of Ethernet 0/4 switchport access vlan 1 no shutdown interface Ethernet 0/5 switchport access vlan 1 no shutdown interface Ethernet 0/6 switchport access vlan 1 no interface shutdown Ethernet 0/7 switchport access vlan 1 no shutdown interface vlan2 nameif outside not turning off IP address dhcp setroute interface vlan The 1st nameif within the ip address 192.168.1.1 255.255.255.0 security level 100 is not turned off global (out) 1 interface nat (inside) 1 0 0 http server allows http 192.168.1.0 255.25 5.255.0 in dhcpd address 192.168.1.2-192.168.1.254 in dhcpd auto_config outside of dhcpd allow in the asdm of the default plant information configuration for ASA 5510 and above adaptive security device adjusts the following : Management interface, 0/0 management. If you don't set the IP address in the default factory setting team, the IP address and mask are 192.168.1.1 and 255.255.255.0. The DHCP server is enabled on the security device, so the computer connected to the interface receives an address between 192.168.1.2 and 192.168.1.254. The HTTP server is enabled for ASDM and is available to users on the 192.168.1.0 network. The configuration consists of the following commands: control interface 0/0 IP address 192.168.1 255.255.0 nameif security control level 100 non-stop asdm registration information 100 asdm history allow the server http to turn on http 192.168.1.0 255.255.5.5.5 5.5 255.0 management dhcpd address 192.168.1.2-192.1.254 management dhcpd lease 3600 dhcpd ping_timeout 750 dhcpd include plant configuration management for default 515/515E security device adjusts the following: Internal Interface Ethernet1. If you don't set the IP address in the default factory setting team, the IP address and mask are 192.168.1.1 and 255.255.255.0. The DHCP server is enabled on the security device, so the computer connected to the interface receives an address between 192.168.1.2 and 192.168.1.254. The HTTP server is enabled for ASDM and is available to users on the 192.168.1.0 network. The configuration consists of the following commands: the interface 1 IP address 192.168.1.1 255.255.255.0 nameif security level management 100 no shutdown asdm log information history 100 asdm allow http server to include 255.255.255.0 Management dhcpd address 192.168.1.2-192.168.1.254 management dhcpd lease 3600 dhcpd ping_timeout 750 dhcpd include control for the original configuration, access to the command-line interface directly from the port console. Later, you can set up remote access using Telnet or SSH according to Chapter 40 Office of System Access. If your system is already in multi-context mode, access to the console port puts you in the system execution space. Read more about the multiple context mode in Chapter 3 Of The Multiple Context Mode. Please note that if you want to use ASDM to set up a security device instead of a command line interface, you can connect to the default control address 192.168.1.1 (if your security device includes a factory default configuration. On ASA 5510 and higher adaptive security devices, the interface you connect to with ASDM is Management 0/0. For an adaptive security device, the ASA 5505 switch port you connect to with ASDM is any port except Ethernet 0/0. For the PIX 515/515E security device, the interface you connect to with ASDM is Ethernet 1. If you don't have a factory configuration by default, follow the steps in this section to access the command line interface. You can then set up minimum settings to access ASDM by entering the settings command. To access the command line interface, follow the following steps: Step 1 Connect your computer to the console port with the console cable provided and connect to the console with an emulator terminal installed for 9600 bods, 8 bits of data, no parity, 1 stop-bit, no flow control. For more information about the console cable, you can find the hardware guide that came with your security device. Step 2 Click Enter to see the following query: host's name is indicated that you are in EXEC user mode. Step 3 To gain access to the privileged EXEC mode, enter the following command: host's name: Password: Password: Step 4 Enter the password on request. The default password is empty and you can press the Enter key to continue. See the inclusion password change section on page 8-1 to change your password. Fast changes to: the host's name to exit the privileged mode, type unplugged, exit or exit the team. Step 5 To access the global configuration mode, enter Team: The host-name sets up the Terminal Fast changes to the following: host name (configuration) to get out of global configuration mode, enter output, exit or finish the team. You can set up a security device to work in the route mode of the firewall (default) or transparent firewall mode. For The For contextual mode, you can only use one firewall mode for all contexts. You need to set up the mode in the system execution space. When you change modes, the security device clears the configuration because many commands are not supported for both modes. If you already have a completed configuration, be sure to make a backup time for backup configuration time before changing the mode; you can use this backup to help you create a new configuration. See the Backup Configuration Files section on page 41-8. For multiple context, the configuration of the system is erased. This action removes any context from the startup. If you then re-add a context that has an existing configuration that was created for the wrong mode, the context configuration won't work properly. Be sure to recreate context configurations for the correct mode before re-adding them, or add new contexts with new ways for new configurations. If you're uploading a text configuration to a security device that changes mode with a transparent firewall command, be sure to place the command at the top of the configuration; The security device changes mode as soon as it reads the command and then continues to read the configuration you downloaded. If the command is later in the configuration, the security device clears all previous lines in the configuration. For information about downloading text files, see Download software or flash configuration files on page 41-3. To set the mode transparent, enter the following command in the system execution space: host name (configuration) firewall Transparent This command also appears in each context configuration only for informational purposes; you can't get into this team in context. To set up the mode on the route, enter the following command in the system execution space: host name (configuration) The security device loads the configuration from a text file called a startup configuration. This file is by default like a hidden file in an internal flash memory. However, you can specify a different path for the startup configuration. (For more information, see Chapter 41 Software Management, Licenses, and Configurations.) When you log in to the team, the change in is made only in the configuration to work in memory. You have to manually keep the configuration running in the startup configuration so that your changes remain after the restart. The information in this section extends to both individual and several security contexts, with the exception of those noted. More information about contexts is in the chapter Incorporating a multiple context mode. Here are the topics in this section: Saving Configuration Changes, Copying the Startup Configuration in a Running Configuration Configuration, View ConfigurationCleaning and Deleting Removal Settings Creating text configuration files offline This section describes how to save the configuration, and includes the following themes: Keeping configuration changes in one context mode Keeping configuration changes in multiple context To save the running configuration in the start-up configuration enter the next command: host name, write a Memory Note Copy of the Start-configuration configuration command equivalent to the record memory team. You can save each context configuration (and system) separately, or keep all context configurations at the same time. This section includes the following topics: Keep each context and system separateSaving all context configurations at the same time to save the system or context configuration, enter the next command in the system or context: hostname write a Note Note Copy of the Start-up Configuration configuration command equivalent to the record memory command. For multiple contextual modes, context start-up configurations may be on external servers. In this case, the security device keeps the configuration back to the server that you identified in the URL context, except for the HTTP or HTTPS URL, which does not allow you to keep the configuration on the server. To save all context configurations at the same time as well as the configuration of the system, enter the following command in the system execution space: hostname' write the memory all if you do not enter the keyword /noconfirm, you see the following query: You are sure that Y/N: After entering Y, the security device retains the configuration of the system and each context. Start context configurations can be on external servers. In this case, the security device keeps the configuration back to the server that you identified in the URL context, except for the HTTP or HTTPS URL, which does not allow you to keep the configuration on the server. Once the security device saves each context, the following message appears: Saving the 'b' context... Sometimes the context is not saved because of an error. See the following error information: For contexts that are not saved due to low memory, the following message appears: Context A context cannot be saved due to unavailability of resources For contexts that are not saved because the remote destination is not available, the following message appears: Context A context cannot be saved due to the inaccessibility of the destination For contexts that are not saved because the context appears, because the context appears, the next message appears. 'a' context, 'x' context, 'z' context. Context is only blocked if another user is already saving or in the process of removing the context. For contexts that don't persist because a startup read only (for example, on the HTTP server), the next message report is printed at the end of all other messages: You can't save the configuration for the following contexts because these contexts only have to read the urls configuration: context 'a', context 'b', context 'c'. For contexts that are not saved due to bad sectors in flash memory, the following message appears: context context a cannot be saved due to unknown errors Copy the new launch configuration to the launch configuration using one of these options: Combine the launch configuration with the run configuration, enter the following command: host-name (configuration) copying the start-up configuration If the configurations are the same. If teams disagree, or if teams affect the context, the impact of the merger depends on the team. You can get bugs, or you may have unexpected results. To download the launch configuration and opt out of the running configuration, restart the security device by entering the following command: host name reboot Alternatively, you can use the following commands to download the launch configuration and opt out of the running configuration without requiring a reboot: hostname/contexta (config) Enter the following command: host name show a running configuration To view the running configuration of a particular team, enter the following command: host name show the command To view the configuration of the startup, enter the next command: host name show the startup configuration to erase the settings, enter one of the following commands. To clear the entire configuration for the specified command, enter the following command: host name (configuration) clear configuration and level2configurationcommand This team cleans the entire current configuration for the specified configuration command. If you want to clear the configuration only for a specific version of the command, you can enter the value for level2configurationcommand. For example, to clear the configuration for all aaa commands, enter the following command: host name (configuration) clearly customize aaa To clear the configuration only for aaa authentication commands, Enter the following command: hostname (config) clearly adjust aaa authentication To disable specific settings or command settings, enter the following command: host name (configuration)no configurationcommand level2configurationcommand qualifier in this case, you do not use For example, to remove a certain command nat, enter enough to define it unequivocally as follows: host name (configuration) no nat (inside) 1 To erase the launch configuration, enter the following command: host name (configuration) write to erase To erase the running configuration, enter the following command: host name (configuration) clearly adjust the entire Note In multiple contexts, if you enter a clear configuration of all of the configuration of the system, you also remove all the contexts. This guide describes how to use CLI to set up a security device; if you save commands, the changes are recorded in a text file. Instead of using CLI, however, you can edit the text file directly on your computer and insert the configuration into the command-line query configuration mode in full, or line by line. You can also download a text file into the internal flash memory of your security device. For more information about downloading the configuration file to a security device, visit Chapter 41, Managing Software, Licenses, and Configurations. In most cases, the commands described in this guide are preceded by a CLI request. The hint in the following example is hostname (config): hostname (config) - Context a In a text configuration file you are not asked to enter commands, so the request is omitted as follows: context A For more information about file formatting see Appendix C, Using the command-line interface. Interface.