Click to verify

دليل إعداد cisco asa 5516-xt

All Cisco ASA series models configurations are same. Cisco ASA devices allow for configuration to be made via a Java application. In order to set the ASA up to use the Java application, you will need to complete some basic configuration from the CLI of the ASA. Please make sure that Java is installed on your laptop prior to completing the below. This is written under the assumption that the ASA has been factory reset. Connect your console cable to the ASA and connect to it via Putty. Once the ASA has finished loading, go into enable mode. The default password is cisco with no username. We will set up the management interface for connecting our laptop to ASDM. Ciscoasa# conf t Ciscoasa# (config) int management0/0 Ciscoasa#(config-if)ip address 192.168.1.1 255.255.255.0 Ciscoasa#(config-if) nameifManageASDM Ciscoasa#(config-if)no shut Ciscoasa#(config-if) Security-level 100 This sets the management interface IP address and names it for later use. Now we can set up the web server that we will connect to. Ciscoasa#(config) http server enable Ciscoasa#(config) http 192.168.1.0 255.255.255.0 ManageASDM(matches management int name) Now we need to set an “enable username” for connecting to the ASDM interface. Ciscoasa#(config)enable password firewall level 15 Next, connect the Ethernet port of your laptop to the management port of the ASA and set a static IP on the laptop, in the 192.168.1.0/24 range (but not 192.168.1.1). On your laptop, open a browser and go to to get to the Cisco ASDM page. Accept the certificate error and continue to the webpage. The last step is to click Install ASDM Launcher and Run ASDM from the webpage. The installer will then run through the process of installing. You’ll then need to go to the install location and create a shortcut to your desktop. Open the shortcut and fill in the IP address (192.168.1.1), leave the username blank and put in the password firewall. The ASDM will then connect to the ASA and load the java interface. You can now configure the ASA as per your requirements.Here and another Here In order to download the version of cisco asa software you need a cisco support contract in place. please do not forget to rate. > Obtaining Documentation and Submitting a Service Request 4 Introduction to Cisco ASA Firewall Services 5 How to Implement Firewall Services 5 Network Address Translation 8 Use Case: Expose a Server to the Public 9 Objects for Access Control 13 Guidelines for Objects 13 Configure Network Objects and Groups 14 Configure a Network Object Group 15 Configure Service Objects and Service Groups 16 Configure a Service Object 16 Configure a Service Group 17 Configure Local User Groups 19 Configure Security Group Object Groups 20 Access Control Entry Order 27 Permit/Deny Vs. Match/Do Not Match 27 Access Control Implicit Deny 27 IP Addresses Used for Extended Acls When You Use NAT 28 Basic ACL Configuration and Management Options 30 Configure Extended Acls 31 Add an Extended ACE for TCP or UDP-Based Matching, with Ports 33 Add an Extended ACE for ICMP-Based Matching 34 Add an Extended ACE for User-Based Matching (Identity Firewall) 34 Add an Extended ACE for Security Group-Based Matching (Cisco Trustsec) 35 Example of Converting Addresses to Objects for Extended Acls 37 Configure Standard Acls 37 Configure Webtype Acls 38 Add a Webtype ACE for URL Matching 38 Adding a Webtype ACE for IP Address Matching 39 Examples for Webtype Acls 40 Configure Ethertype Acls 41 Examples for Ethertype Acls 42 Edit Acls in an Isolated Configuration Session 42 Controlling Network Access 47 General Information about Rules 48 Interface Access Rules and Global Access Rules 48 Inbound and Outbound Rules 48 Extended Access Rules for Returning Traffic 51 Management Access Rules 51 Guidelines for Access Control 53 Configure Access Control 53 Configure an Access Group 53 Configure ICMP Access Rules 54 Monitoring Access Rules 56 Evaluating Syslog Messages for Access Rules 56 History for Access Rules 58 About the Identity Firewall 61 Architecture for Identity Firewall Deployments 62 Features of the Identity Firewall 63 Guidelines for the Identity Firewall 67 Prerequisites for the Identity Firewall 69 Configure the Identity Firewall 70 Configure the Active Directory Domain 70 Configure Active Directory Agents 73 Configure Identity Options 74 Configure Identity-Based Security Policy 78 Collect User Statistics 79 Examples for the Identity Firewall 79 VPN with IDFW Rule -1 Example 81 VPN with IDFW Rule -2 Example 81 Monitoring the Identity Firewall 81 History for the Identity Firewall 82 ASA and Cisco Trustsec 83 About SGT and SXP Support in Cisco Trustsec 84 Roles in the Cisco Trustsec Feature 85 Security Group Policy Enforcement 85 How the ASA Enforces Security Group-Based Policies 86 Effects of Changes to Security Groups on the ISE 87 Speaker and Listener Roles on the ASA 88 IP-SGT Manager Database 90 Features of the ASA-Cisco Trustsec Integration 90 Register the ASA with the ISE 92 Create a Security Group on the ISE 92 Guidelines for Cisco Trustsec 93 Configure the AAA Server for Cisco Trustsec Integration 95 Configure the Security Exchange Protocol 99 Add an SXP Connection Peer 101 Refresh Environment Data 102 Configure the Security Policy 102 Layer 2 Security Group Tagging Imposition 104 Configure a Security Group Tag on an Interface 106 Configure IP-SGT Bindings Manually 107 Example for Cisco Trustsec 108 Anyconnect VPN Support for Cisco Trustsec 108 Typical Steps for a Remote User Connecting to a Server 108 Add an SGT to Local Users and Groups 109 Monitoring Cisco Trustsec 109 History for Cisco Trustsec 110 About the ASA Firepower Module 111 How the ASA Firepower Module Works with the ASA 111 ASA Firepower Inline Mode 112 ASA Firepower Passive Monitor-Only Traffic Forwarding Mode 114 ASA Firepower Management 115 Compatibility with ASA Features 115 Licensing Requirements for the ASA Firepower Module 115 Guidelines for ASA Firepower 115 Defaults for ASA Firepower 116 Perform Initial ASA Firepower Setup 117 Deploy the ASA Firepower Module in Your Network 117 Access the ASA Firepower CLI 119 Configure ASA Firepower Basic Settings 119 Configure the ASA Firepower Module 120 Configure the Security Policy on the ASA Firepower Module 120 Redirect Traffic to the ASA Firepower Module 120 Configure Inline or Inline Tap Monitor-Only Modes 121 Configure Passive Traffic Forwarding 122 Managing the ASA Firepower Module 123 Install or Reimage the Module 123 Install or Reimage the Software Module 124 Reimage the ASA 5585-X ASA Firepower Hardware Module 126 Reload or Reset the Module 128 Uninstall a Software Module Image 129 Session to the Software Module from the ASA 130 Upgrade the System Software 130 Monitoring the ASA Firepower Module 131 Showing Module Status 131 Showing Module Statistics 132 Monitoring Module Connections 132 Examples for the ASA Firepower Module 133 History for the ASA Firepower Module 134 ASA and Cisco Cloud Web Security 137 Information about Cisco Cloud Web Security 137 User Identity and Cloud Web Security 138 How Groups and the Authentication Key Interoperate 140 Failover from Primary to Backup Proxy Server 140 Licensing Requirements for Cisco Cloud Web Security 140 Guidelines for Cloud Web Security 141 Configure Cisco Cloud Web Security 142 Configure Communications with the Cloud Web Security Proxy Server 142 Identify Whitelisted Traffic 144 Configure a Service Policy to Send Traffic to Cloud Web Security 145 Configure the User Identity Monitor 149 Configure the Cloud Web Security Policy 150 Monitoring Cloud Web Security 150 Examples for Cisco Cloud Web Security 151 Cloud Web Security Example with Identity Firewall 151 Active Directory Integration Example for Identity Firewall 153 History for Cisco Cloud Web Security 155 Network Address Translation 157 Network Address Translation (NAT) 159 Network Object NAT and Twice NAT 161 Comparing Network Object NAT and Twice NAT 162 Firewall Mode Guidelines for NAT 165 Ipv6 NAT Recommendations 165 Additional Guidelines for NAT 166 Network Object NAT Guidelines for Mapped Address Objects 167 Twice NAT Guidelines for Real and Mapped Address Objects 168 Twice NAT Guidelines for Service Objects for Real and Mapped Ports 169 Dynamic NAT Disadvantages and Advantages 171 Configure Dynamic Network Object NAT 172 Configure Dynamic Twice NAT 174 Dynamic PAT Disadvantages and Advantages 177 PAT Pool Object Guidelines 177 Configure Dynamic Network Object PAT 178 Configure Dynamic Twice PAT 180 Configure Per-Session PAT or Multi-Session PAT 183 Static NAT with Port Translation 185 One-To-Many Static NAT 187 Other Mapping Scenarios (Not Recommended) 189 Configure Static Network Object NAT or Static NAT-With-Port-Translation 190 Configure Static Twice NAT or Static NAT-With-Port-Translation 192 Configure Identity Network Object NAT 195 Configure Identity Twice NAT 197 NAT Examples and Reference 205 Examples for Network Object NAT 205 Providing Access to an Inside Web Server (Static NAT) 205 Examples for Twice NAT 210 Different Translation Depending on the Destination (Dynamic Twice PAT) 210 Example: Twice NAT with Destination Address Translation 213 NAT in Routed and Transparent Mode 213 NAT in Transparent Mode 214 Mapped Addresses and Routing 216 Addresses on the same Network as the Mapped Interface 216 Addresses on a Unique Network 216 The same Address as the Real Address (Identity NAT) 217 Transparent Mode Routing Requirements for Remote Networks 218 Determining the Egress Interface 218 NAT and Remote Access VPN 219 NAT and Site-To-Site VPN 221 NAT and VPN Management Access 223 Troubleshooting NAT and VPN 225 DNS Reply Modification, DNS Server on Outside 226 DNS Reply Modification, DNS Server on Host Network 228 DNS64 Reply Modification Using Outside NAT 229 PTR Modification, DNS Server on Host Network 231 Service Policies and Application Inspection 233 About Service Policies 235 The Components of a Service Policy 235 Features Configured with Service Policies 238 Feature Matching Within a Service Policy 239 Order in Which Multiple Feature Actions Are Applied 240 Incompatibility of Certain Feature Actions 240 Feature Matching for Multiple Service Policies 242 Guidelines for Service Policies 242 Defaults for Service Policies 243 Default Service Policy Configuration 243 Default Class Maps (Traffic Classes) 244 Configure Service Policies 245 Identify Traffic (Layer 3/4 Class Maps) 247 Create a Layer 3/4 Class Map for through Traffic 247 Create a Layer 3/4 Class Map for Management Traffic 249 Define Actions (Layer 3/4 Policy Map) 250 Apply Actions to an Interface (Service Policy) 251 Monitoring Service Policies 252 Examples for Service Policies (Modular Policy Framework) 252 History for Service Policies 255 Application Layer Protocol Inspection 257 How Inspection Engines Work 257 When to Use Application Protocol Inspection 258 Inspection Policy Maps 259 Replacing an In-Use Inspection Policy Map 259 How Multiple Traffic Classes Are Handled 260 Guidelines for Application Inspection 261 Defaults for Application Inspection 262 Default Inspections and NAT Limitations 262 Default Inspection Policy Maps 265 Configure Application Layer Protocol Inspection 265 Choosing the Right Traffic Class for Inspection 270 Configure Regular Expressions 271 Create a Regular Expression 271 Create a Regular Expression Class Map 273 History for Application Inspection 274 DNS Inspection Actions 276 Defaults for DNS Inspection 276 Configure DNS Inspection 276 Configure DNS Inspection Policy Map 277 Configure the DNS Inspection Service Policy 280 Monitoring DNS Inspection 282 ICMP Error Inspection 295 Instant Messaging Inspection 295 Configure an Instant Messaging Inspection Policy Map 296 Configure the IM Inspection Service Policy 298 IP Options Inspection 300 IP Options Inspection Overview 300 What Happens When You Clear an Option 300 Supported IP Options for Inspection 301 Defaults for IP Options Inspection 301 Configure IP Options Inspection 301 Configure an IP Options Inspection Policy Map 302 Configure the IP Options Inspection Service Policy 302 Monitoring IP Options Inspection 304 Ipsec Pass through Inspection 304 Ipsec Pass through Inspection Overview 304 Configure Ipsec Pass through Inspection 304 Configure an Ipsec Pass through Inspection Policy Map 305 Configure the Ipsec Pass through Inspection Service Policy 306 Defaults for Ipv6 Inspection 307 Configure Ipv6 Inspection 308 Configure an Ipv6 Inspection Policy Map 308 Configure the Ipv6 Inspection Service Policy 309 Configure the Netbios Inspection Service Policy 312 SMTP and Extended SMTP Inspection 313 SMTP and ESMTP Inspection Overview 314 Defaults for ESMTP Inspection 315 Configure ESMTP Inspection 316 Configure an ESMTP Inspection Policy Map 316 Configure the ESMTP Inspection Service Policy 318 Inspection for Voice and Video Protocols 321 Limitations for CTIQBE Inspection 321 Verifying and Monitoring CTIQBE Inspection 322 Limitations for H.323 Inspection 325 Configure H.323 Inspection 326 Configure H.323 Inspection Policy Map 326 Configure the H.323 Inspection Service Policy 329 Verifying and Monitoring H.323 Inspection 330 Monitoring H.225 Sessions 330 Monitoring H.245 Sessions 331 Monitoring H.323 RAS Sessions 332 MGCP Inspection Overview 332 Configure MGCP Inspection 333 Configure the MGCP Inspection Service Policy 335 Configuring MGCP Timeout Values 336 Verifying and Monitoring MGCP Inspection 336 RTSP Inspection Overview 337 Realplayer Configuration Requirements 338 Limitations for RSTP Inspection 338 Configure RTSP Inspection 338 Configure RTSP Inspection Policy Map 339 Configure the RTSP Inspection Service Policy 341 SIP Inspection Overview 343 Limitations for SIP Inspection 343 Default SIP Inspection 344 Configure SIP Inspection 344 Configure SIP Inspection Policy Map 344 Configure the SIP Inspection Service Policy 348 Configure SIP Timeout Values 349 Verifying and Monitoring SIP Inspection 349 Skinny (SCCP) Inspection 350 SCCP Inspection Overview 350 Supporting Cisco IP Phones 351 Limitations for SCCP Inspection 351 Default SCCP Inspection 351 Configure SCCP (Skinny) Inspection 352 Configure the SCCP Inspection Service Policy 353 Verifying and Monitoring SCCP Inspection 355 History for Voice and Video Protocol Inspection 355 Inspection of Database, Directory, and Management Protocols 357 Configure DCERPC Inspection 358 GTP Inspection Overview 361 Defaults for GTP Inspection 362 Configure GTP Inspection 362 Configure a GTP Inspection Policy Map 363 Configure the GTP Inspection Service Policy 365 Verifying and Monitoring GTP Inspection 367 RADIUS Accounting Inspection 369 RADIUS Accounting Inspection Overview 369 Configure RADIUS Accounting Inspection 369 Configure a RADIUS Accounting Inspection Policy Map 370 Configure the RADIUS Accounting Inspection Service Policy 371 Sun RPC Inspection Overview 375 Managing Sun RPC Services 375 Verifying and Monitoring Sun RPC Inspection 376 History for Database, Directory, and Management Protocol Inspection 378 Connection Management and Threat Detection 379 What Are Connection Settings 381 Configure Connection Settings 382 Configure Global Timeouts 383 Protect Servers from a SYN Flood Dos Attack (TCP Intercept) 384 Customize Abnormal TCP Packet Handling (TCP Maps, TCP Normalizer) 387 Bypass TCP State Checks for Asynchronous Routing (TCP State Bypass) 390 The Asynchronous Routing Problem 390 Guidelines for TCP State Bypass 391 Configure TCP State Bypass 392 Disable TCP Sequence Randomization 393 Monitoring Connections 397 History for Connection Settings 398 Supported Qos Features 402 What Is a Token Bucket 402 How Qos Features Interact 403 DSCP (Diffserv) Preservation 403 Determine the Queue and TX Ring Limits for a Priority Queue 404 TX Ring Limit Worksheet 405 Configure the Priority Queue for an Interface 406 Configure a Service Rule for Priority Queuing and Policing 407 Qos Police Statistics 409 Qos Priority Statistics 410 Qos Priority Queue Statistics 410 Configuration Examples for Priority Queuing and Policing 411 Class Map Examples for VPN Traffic 411 Priority and Policing Example 412 Basic Threat Detection Statistics 416 Advanced Threat Detection Statistics 416 Scanning Threat Detection 417 Guidelines for Threat Detection 417 Defaults for Threat Detection 418 Configure Threat Detection 418 Configure Basic Threat Detection Statistics 419 Configure Advanced Threat Detection Statistics 419 Configure Scanning Threat Detection 421 Monitoring Threat Detection 422 Monitoring Basic Threat Detection Statistics 422 Monitoring Advanced Threat Detection Statistics 423 Evaluating Host Threat Detection Statistics 424 Monitoring Shunned Hosts, Attackers, and Targets 426 Examples for Threat Detection 427 History for Threat Detection 428 Hi Mahesh, firewall is a huge technology and you will specifically let us know what you are looking for. I would suggest to go through configuration guide of specific version and see what you exactly need. Here is the link to enable your license Note ASA version 9.16 is the final supported version for the ASA 5508-X and 5516-X. Is This Chapter for You? This chapter describes how to deploy the ASA 5508-X or 5516-X in your network with the ASA FirePOWER module and how to perform initial configuration. This chapter does not cover the following deployments, for which you should refer to the ASA configuration guide: Failover Clustering (ASA 5516-X only) CLI configuration This chapter also walks you through configuring a basic security policy; if you have more advanced requirements, refer to the configuration guide. The ASA 5508-X and 5516-X hardware can run either ASA software or FTD software. Switching between ASA and FTD requires you to reimage the device. See Reimage the Cisco ASA or Firepower Threat Defense Device. Privacy Collection Statement—The ASA 5508-X or 5516-X do not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP. The ASA provides advanced stateful firewall and VPN concentrator functionality in one device, and with the included ASA FirePOWER module, next-generation firewall services including Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP). You can manage the ASA using one of the following managers: ASDM (covered in this guide)—A single device manager included on the device. CLI Cisco Defense Orchestrator—A simplified, cloud-based multi-device manager Cisco Security Manager—A multi-device manager on a separate server. You can manage the ASA FirePOWER module using one of the following managers: ASDM (Covered in this guide)—A single device manager included on the device. Firepower Management Center (FMC)—A full-featured, multidevice manager on a separate server. You can also access the FirePOWER CLI for troubleshooting purposes. The following figure shows a typical edge deployment for the ASA 5508-X and 5516-X using the default configuration. In this deployment, the ASA acts as the internet gateway for the ASA FirePOWER module, which needs internet access for database updates. You can connect the Management 1/1 interface to the same network (through a switch) as the inside interface if you do not set the Management 1/1 IP address for the ASA. (You can set the Management 1/1 IP address for the ASA FirePOWER module to be on the same network as inside because it is a separate system from the ASA.) If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the ASA performs all routing and NAT for your inside networks. If you need to configure PPPoE for the outside interface to connect to your ISP, you can do so as part of the ASDM Startup Wizard. Note If you cannot use the default inside IP address for ASDM access, you can set the inside IP address at the ASA CLI. See (Optional) Change the IP Address. For example, you may need to change the inside IP address in the following circumstances: If the outside interface tries to obtain an IP address on the 192.168.1.0 network, which is a common default network, the DHCP lease will fail, and the outside interface will not obtain an IP address. This problem occurs because the ASA cannot have two interfaces on the same network. In this case you must change the inside IP address (and later, the ASA FirePOWER IP address) to be on a new network. If you add the ASA to an existing inside network, you will need to change the inside IP address (and later, the ASA FirePOWER IP address) to be on the existing network. The default factory configuration for the ASA 5506-X series, 5508-X, and 5516-X configures the following: inside --> outside traffic flow—GigabitEthernet 1/1 (outside), GigabitEthernet 1/2 (inside) outside IP address from DHCP inside IP address—192.168.1.1 (ASA 5506W-X) wifi inside, wifi --> outside traffic flow—GigabitEthernet 1/9 (wifi) (ASA 5506W-X) wifi IP address—192.168.10.1 DHCP server on inside and wifi. The access point itself and all its clients use the ASA as the DHCP server. Default route from outside DHCP Management 1/1 interface is Up, but otherwise unconfigured. The ASA FirePOWER module can then use this interface to access the ASA inside network and use the inside interface as the gateway to the Internet. ASDM access—inside and wifi hosts allowed. NAT—Interface PAT for all traffic from inside, wifi, and management to outside. The configuration consists of the following commands: interface Management1/1 management-only no nameif no security-level no ip address no shutdown interface GigabitEthernet1/1 nameif outside security-level 0 ip address dhcp setroute no shutdown interface GigabitEthernet1/2 nameif inside security-level 100 ip address 192.168.1.1 255.255.255.0 no shutdown ! object network obj_any subnet 0.0.0.0 0.0.0.0 nat (any,outside) dynamic interface ! http server enable http 192.168.1.0 255.255.255.0 inside ! dhcpd auto_config outside dhcpd address 192.168.1.5-192.168.1.254 inside dhcpd enable inside ! logging asdm informational For the ASA 5506W-X, the following commands are also included: same-security-traffic permit inter-interface ! interface GigabitEthernet 1/9 security-level 100 nameif wifi ip address 192.168.10.1 255.255.255.0 no shutdown ! http 192.168.10.0 255.255.255.0 wifi ! dhcpd address 192.168.10.2-192.168.10.254 wifi dhcpd enable wifi System power is controlled by a rocker power switch located on the rear of the device. Step 1 Attach the power cord to the device, and connect it to an electrical outlet. Step 2 Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord. Step 3 Check the Power LED on the front or rear of the device; if it is solid green, the device is powered on. Figure 1. Rear Panel Figure 2. Front Panel Step 4 Check the Status LED on the front or rear of the device; after it is solid green, the system has passed power-on diagnostics. I too found that any stencils or even any photographs of the 5516x to be oddly elusive among all of Cisco's appliance offerings. I found nothing at all in any of Cisco's documentation. The closest I got was the back panel. Eventually I located one picture from CDW's website of the front of the 5508x which looks identical to the 5516x. I saved it and converted it to a vss file I could use. Unfortunately, this site does not allow me to upload *.vss files, so enjoy this *.png file. I used "Png to Vss Converter 5.3" and had it output to My Shapes folder. Easy pleasy.