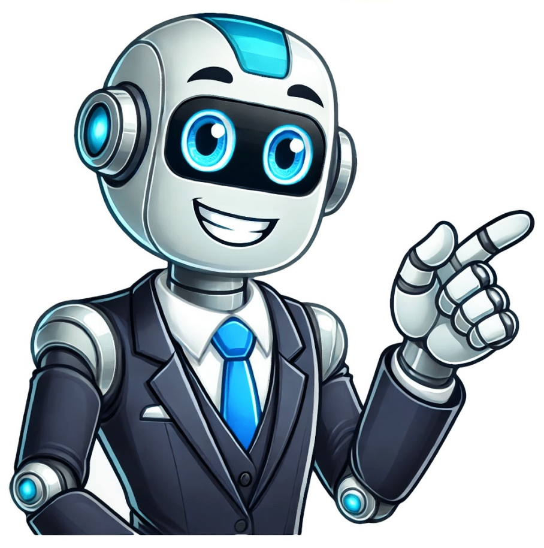
Click to prove you're human



Guide مستخدم cisco asa 5506

Initial configuration for management interface IP and which subnets are allowed to manage the device can be done through CLI. For the actual access policy configuration you would need access to the GUI. I have never tried connecting a PC directly to the management interface so you might need a cross-over cable for that if you do not have a dumb switch you could use for a staging area. -- Please remember to select a correct answer and rate helpful posts --Please remember to select a correct answer and rate helpful posts View solution in original post

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 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

Throughout my professional career in networking I was lucky to work with all Cisco firewall models and therefore I have experienced the “evolution” of every firewall product developed by Cisco. For the SMB/SOHO market, Cisco’s initial offering was the PIX 501, followed by the successful Cisco ASA 5505. The latter came to an End-of-Sale in 2014 and now the replacement low-end model is the new Cisco ASA 5506-X. One of the most popular configuration guides on this blog is this basic ASA 5505 tutorial . Since these are useful posts for many people, I’ve decided to write also a configuration tutorial for the new ASA 5506-X. I will cover two popular use cases of the 5506-X. One is a simple scenario of providing internet access to an internal LAN. The second case is more advanced and will cover two DMZ zones, one with a publicly accessible Web Server and one with a Guest WiFi Access Point. Cisco ASA 5506-X Specs and Features Before starting the discussion on how to configure the 5506, let’s first see the most important specs and features of this model. It comes in two hardware “flavors”, the normal 5506-X and also the 5506W-X which has an integrated wireless access point (a/b/g/n bands). It comes in two software license “flavors”, the Base License and the Security Plus License. 8x1GE Network Interfaces (these are routed ports, not switch ports like the previous 5505 model). 1 Management Interface (for the FirePOWER module). Performance throughput varies according to what services are enabled. 300 Mbps for only firewall services, 250 Mbps for Application Visibility and Control (AVC), 125 Mbps for Application Control (AVC) and IPS/NGIPS, 100 Mbps for VPN throughput. Max 20,000 concurrent sessions with the Base License or 50,000 with the Sec.Plus License. 5 VLANs with Base License and 30 with the Security Plus License. 10 IPSEC Site-to-Site VPNs (Base License) and 50 VPNs with Sec. Plus. Unlimited internal hosts (even with the Base License). Active/Standby high availability (only with Security Plus License). Comes with FirePOWER Services (Application Visibility and Control – AVC) which supports more than 3000 application-layer and risk-based controls. With extra subscription cost you can have also Next Generation IPS, Advanced Malware Protection and URL filtering. Note Regarding Licenses and Subscriptions: You should contact your local reseller and ask about License cost, “right-to-use” subscriptions needed etc. They made licensing too complex in my opinion so you must conduct your reseller for more details and to avoid any “surprises”. For example, Anyconnect needs extra license, IPS requires subscription etc. How to connect the ASA 5506-X in your network for Initial Configuration As you can see in the specs section above, there are 8x1G network interfaces and also one Management interface (Management 1/1) which belongs to the FirePOWER module. In order to deploy the device in your network and be able to start its initial configuration, connect it as following: NOTES: The Management 1/1 interface belongs to the separate FirePOWER module and NOT to the ASA. DO NOT configure an IP address for the Management 1/1 interface inside the ASA configuration. The default “inside” IP address for managing the ASA is 192.168.1.1 (interface GE1/2). You must configure an IP address for Management1/1 in the 192.168.1.x subnet (e.g 192.168.1.2) inside the FirePOWER module (or via the ASDM GUI as we’ll see below). You must connect both GE1/2 (inside) and Management1/1 interfaces on the same Layer2 LAN switch. The outside interface (GE1/1) must be connected to the WAN (ISP) device and will receive IP address dynamically by default (via DHCP). The quickest way to manage initially the device is using ASDM. Launch a web browser on your Management PC and go to . Select “Startup Wizard”, leave username/password fields empty and hit OK. When the wizard takes you to the FirePOWER network settings, enter IP address 192.168.1.2, Mask 255.255.255.0 and Gateway 192.168.1.1 (see below). MORE READING: Cisco ASA Firewall in Transparent Layer2 Mode After you finish the above, quit the ASDM application and then relaunch it. This time you will see new FirePOWER tabs on the GUI home page which means you can now configure also FirePOWER settings in addition to ASA settings. ASA 5506-X Basic Configuration Tutorial The ASA 5506-X has a default configuration out-of-the-box. This default configuration has the following characteristics: Internal LAN: 192.168.1.0/24 Internal LAN can access the Internet. The WAN (outside) interface (GE1/1) is configured to receive IP address from DHCP. The LAN (inside) interface (GE1/2) has IP address 192.168.1.1 DHCP is enabled for providing IP address to internal hosts. In this section we will describe how to change this default configuration to suit your network topology. We assume that you already have network connectivity (or console connectivity) to the device so that you can start configuring with Command Line Interface (CLI). This is our network topology for the basic configuration. Internal user LAN: 10.1.1.0/24 ASA inside IP: 10.1.1.1 ASA outside IP (static): 50.1.1.1 NAT: Dynamic overload (PAT) using the outside interface. Step 1: Configure the Internal LAN interface interface GigabitEthernet1/2   description LAN   nameif inside   security-level 100