Click to verify

دليل التكوين الأساسي cisco asa 5525 xp

12-23Cisco ASA 5500 Series Configuration Guide using ASDMChapter12 Starting Interface Configuration (ASA 5510 and Higher) Starting Interface Configuration (ASA 5510 and Higher)Step12 Close the Command Line Interface dialog box, and choose File > Refresh ASDM with the Running Configuration.Step13 Reenable failover by choosing Configuration > Device Management > High Availability > Failover, and checking the Enable failover check box. Click Apply, and click No when prompted if you want to configure basic failover settings.Enabling the Physical Interface and Configuring Ethernet ParametersThis section describes how to:•Enable the physical interface•Set a specific speed and duplex (if available)•Enable pause frames for flow controlPrerequisitesFor multiple context mode, complete this procedure in the system execution space. If you are not already in the System configuration mode, in the Configuration > Device List pane, double-click System under the active device IP address.Detailed StepsStep1 Depending on your context mode:•For single mode, choose the Configuration > Device Setup > Interfaces pane.•For multiple mode in the System execution space, choose the Configuration > Context Management > Interfaces pane.By default, all physical interfaces are listed.Step2 Click a physical interface that you want to configure, and click Edit.The Edit Interface dialog box appears.Page 267-10Cisco ASA 5500 Series Configuration Guide using ASDMChapter67 Configuring Active/Active Failover Configuring Active/Active Failovermanager. For both types of failover, you need to provide system-level failover settings in the system context, and context-level failover settings in the individual security contexts. For more information about configuring failover in general, see Chapter65, “Information About High Availability.”.Seethe following topics for more information:•Failover > Setup Tab•Failover> C riteria Tab•Failover> Active/Active Tab•Failover> MAC Addresses TabFailover > Setup TabUse this tab to enable failover on an ASA in multiple context mode. You also designate the failover link and the state link, if using Stateful Failover, on this tab.Note During a successful failover event on the ASA, the interfaces are brought down, roles are switched (IP addresses and MAC addresses are swapped), and the interfaces are brought up again. However, the process is transparent to users. The ASA does not send link-down messages or system log messages to notify users that interfaces were taken down during failover (or link-up messages for interfaces brought up by the failover process).Fields•Enable Failover—Checking this check box enables failover and lets you configure a standby ASA.Note The speed and duplex settings for an interface cannot be changed when Failover is enabled. To change these settings for the failover interface, you must configure them in the Configuration > Interfaces pane before enabling failover.•Use 32 hexadecimal character key—Check this check box to enter a hexadecimal value for the encryption key in the Shared Key field. Uncheck this check box to enter an alphanumeric shared secret in the Shared Key field.•Shared Key—Specifies the failover shared secret or key for encrypted and authenticated communications between failover pairs. If you checked the Use 32 hexadecimal character key check box, then enter a hexadecimal encryption key. The key must be 32 hexadecimal characters (0-9, a-f). If you cleared the Use 32 hexadecimal character key check box, then enter an alphanumeric shared secret. The shared secret can be from 1 to 63 characters. Valid character are any combination of numbers, letters, or punctuation. The shared secret is used to generate the encryption key.•LAN Failover—Contains the fields for configuring LAN Failover.–Interface—Specifies the interface used for failover communication. Failover requires a dedicated interface, however, you can use the same interface for Stateful Failover. Only unconfigured interfaces or subinterfaces that have not been assigned to a context are displayed in this list and can be selected as the LAN Failover interface. Once you specify an interface as the LAN Failover interface, you cannot edit that interface in the Configuration> Interfaces pane or assign that interface to a context.Page 367-11Cisco ASA 5500 Series Configuration Guide using ASDMChapter67 Configuring Active/Active Failover Configuring Active/Active Failover–Active IP—Specifies the IP address for the failover interface on the active unit. The IP address can be an IPv4 or an IPv6 address.–Subnet Mask/Prefix Length—Depending upon the type of address specified for the Active IP, enter a subnet mask (IPv4 addresses) or a prefix length (IPv6 address) for the failover interface on the primary and secondary unit.–Logical Name—Specifies the logical name of the interface used for failover communication.–Standby IP—Specifies the IP address used by the secondary unit to communicate with the primary unit. The IP address can be an IPv4 or an IPv6 address.–Preferred Role—Specifies whether the preferred role for this ASA is as the primary or secondary unit in a LAN failover.•State Failover—Contains the fields for configuring Stateful Failover.–Interface—Specifies the interface used for failover communication. You can choose an unconfigured interface or subinterfaces or the LAN Failover interface. If you choose the LAN Failover interface, the interface needs enough capacity to handle both the LAN Failover and Stateful Failover traffic. Also, you do not need to specify the Active IP, Subnet Mask, Logical Name, and Standby IP values; the values specified for the LAN Failover interface are used.Note We recommend that you use two separate, dedicated interfaces for the LAN Failover interface and the Stateful Failover interface.–Active IP—Specifies the IP address for the Stateful Failover interface on the primary unit. This field is dimmed if the LAN Failover interface or Use Named option is chosen from the Interface drop-down list.–Subnet Mask/Prefix Length—Specifies the mask (IPv4 address) or prefix (IPv6 address) for the Stateful Failover interfaces on the primary and secondary units. This field is dimmed if the LAN Failover interface or Use Named option is selected in the Interface drop-down list.–Logical Name—Specifies the logical interface used for failover communication. If you chose the Use Named option in the Interface drop-down list, this field displays a list of named interfaces. This field is dimmed if the LAN Failover interface is chosen from the Interface drop-down list.–Standby IP—Specifies the IP address used by the secondary unit to communicate with the primary unit. This field is dimmed if the LAN Failover interface or Use Named option is chosen from the Interface drop-down list.–Enable HTTP replication—Checking this check box enables Stateful Failover to copy active HTTP sessions to the standby firewall. If you do not allow HTTP replication, then HTTP connections are disconnected at failover. Disabling HTTP replication reduces the amount of traffic on the state link.Failover > Criteria TabUse this tab to define criteria for failover, such as how many interfaces must fail and how long to wait between polls. The hold time specifies the interval to wait without receiving a response to a poll before unit failover. Hello, I just would like to confirm if ASA 5525-X with 9.6 will allow to create VLANS and assigned them to the interfaces. such as an example ciscoasa(config)# interface vlan 1 ciscoasa(config-if)# nameif inside ... ciscoasa(config-if)# interface vlan 2 ciscoasa(config-if)# nameif outside ... THEN ciscoasa(config)# interface Et0/0 ciscoasa(config-if)# switchport access vlan 1 ... ciscoasa(config-if)# interface Et0/1 ciscoasa(config-if)# switchport access vlan 2 What is different in ASA 5525-x and how to implement this ? The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product. Learn more about how Cisco is using Inclusive Language. User Manuals, Guides and Specifications for your Cisco ASA 5525-X Chassis, Firewall, Network Hardware, Security System. Database contains 8 Cisco ASA 5525-X Manuals (available for free online viewing or downloading in PDF): Cli configuration manual, Software manual, Installation instructions manual, Configuration manual, Quick start manual, Hardware installation manual . 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 Welcome to Cisco World 1. Should i register the product with Cisco? is this the requirement to acquire licenses or the licenses are already installed? BB - you can register the product or contact TAC - if this new unpacket might not have registered, if you have any PAK(cisco License) you can register. If the contract expired you can extend the smartnet contract contacting local Partner or Cisco 2. How to check that how many and which licences are installed on the device? BB - show license (will give you what license installed. if this new device you get basic information) 3. I have currently following images on the device i). asa922-4-smp-k8 BB - This is OS of the ASA to run as Firewall - there is latest version, but depends on the requirement you need to choose the right verison for your environment - 9.6.X is good as of now tested myself, there 9.8.X also available read the release notes before you upgrade. ii). asasfr-5500x-boot-5.4.0-763.img This is SourceFire (FirePOWER - IPS Engine) Hope this information help you to start with : here is quick start guide : What these two images represent? and should i upgrade both of them to newer versions?