Continue

cisco asa 9.12 download للعمليات العامة من سلسلة cli دليل تكوين

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. In this post I have gathered the most useful Cisco ASA Firewall Commands and created a Cheat Sheet list that you can download also as PDF at the end of the article. I have been working with Cisco firewalls since 2000 where we had the legacy PIX models before the introduction of the ASA 5500 and the newest ASA 5500-X series. The biggest changes in command syntax happened of course at the transition between PIX and ASA models and also after the changes in ASA version 8.3 and later (especially on NAT configuration commands). From ASA versions 8.3 and later (including 9.x) the command syntax does change a little bit on some commands at every new version update but the majority of core configurations remain the same. There are hundreds of commands and configuration features of the Cisco ASA firewall. The official Cisco command reference guide for ASA firewalls is more than 1000 pages. Therefore it's not possible to cover the whole commands' range in a single post. For this reason I have selected the most important commands and the ones used most frequently by ASA administrators to set up the firewall appliance. You can download the ASA commands cheat sheet in PDF format plus two more cheat sheet documents (for Routers and Switches) by subscribing below: Also, if you are interested for Cisco Routers and Switches Commands Cheat Sheet documents, have a look at the links below: Cisco Switch Commands Cheat Sheet Cisco Router Commands Cheat Sheet Most Important Cisco ASA Firewall Commands Start Configuring the firewall ciscoasa> enable Password: [Enter into "Privileged Mode". This will require to enter the "enable" password] ciscoasa# configure terminal ciscoasa(config)# [Enter into "Global Configuration Mode" to start configuring the device] Viewing and Saving the configuration ciscoasa# show running-config [Show the currently running configuration] ciscoasa# show startup-config [Show the configuration which is stored on the device. This is the one which will be loaded if you reboot the firewall] ciscoasa# copy run start or ciscoasa# write memory [Save the running configuration so it won't be lost if you reboot] Image Software Management ciscoasa# copy tftp flash [Copy image file from TFTP to Flash of ASA] ciscoasa#config term ciscoasa(config)# boot system flash:/asa911-k8.bin [At next reboot, the firewall will use the software image "asa911-k8.bin" from flash] Passwords and Users ciscoasa(config)# enable password Gh4w7$-s39fg#(! [You must create a strong "enable" password which gives access to the configuration mode of the device] ciscoasa(config)#username ciscoadmin password adminpassword privilege 15 [Create a local user account and assign privilege level 15 which means administrator access] Change Device Hostname ciscoasa(config)# hostname DATA-CENTER-FW DATA-CENTER-FW(config)# MORE READING: Using Interfaces with Same Security Levels on Cisco ASAConfigure Secure Management Access to the Firewall ciscoasa(config)# crypto key generate rsa modulus 2048 [Create SSH keys] ciscoasa(config)#aaa authentication ssh console LOCAL [The device will authenticate SSH user access from the LOCAL user database] ciscoasa(config)#username admin password adminpassword privilege 15 [Create local administrator user] ciscoasa(config)#ssh 192.168.1.10 255.255.255.255 inside [Allow SSH access only from host 192.168.1.10 from the "inside" interface] Interface Configuration and Security Levels ciscoasa(config)# interface GigabitEthernet0/1 ciscoasa(config-if)# nameif DMZ ciscoasa(config-if)# ip address 192.168.1.2 255.255.255.0 ciscoasa(config-if)# security-level 50 ciscoasa(config-if)# no shutdown The absolutely necessary Interface Sub-commands that you need to configure in order for the interface to pass traffic are the following: nameif "interface name": Assigns a name to an interface ip address "ip_address" "subnet_mask" : Assigns an IP address to the interface security-level "number 0 to 100" : Assigns a security level to the interface no shutdown : By default all interfaces are shut down, so enable them. Static and Default Routes ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 100.1.1.1 [Configure a default route via the "outside" interface with gateway IP of 100.1.1.1] ciscoasa(config)# route inside 192.168.2.0 255.255.255.0 192.168.1.1 [Configure a static route via the "inside" interface. To reach network 192.168.2.0/24 go via gateway IP 192.168.1.1] Network Address Translation (NAT) ciscoasa(config)# object network internal_lan ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0 ciscoasa(config-network-object)# nat (inside,outside) dynamic interface [Configure PAT for internal LAN (192.168.1.0/24) to access the Internet using the outside interface] ciscoasa(config)# object network obj_any ciscoasa(config-network-object)# subnet 0.0.0.0 0.0.0.0 ciscoasa(config-network-object)# nat (any,outside) dynamic interface [Configure PAT for all ("any") networks to access the Internet using the outside interface] ciscoasa(config)# object network web_server_static ciscoasa(config-network-object)# host 192.168.1.1 ciscoasa(config-network-object)# nat (DMZ , outside) static 100.1.1.1 [Configure static NAT. The private IP 192.168.1.1 in DMZ will be mapped statically to public IP 100.1.1.1 in outside zone] ciscoasa(config)# object network web_server_static ciscoasa(config-network-object)# host 192.168.1.1 ciscoasa(config-network-object)# nat (DMZ , outside) static 100.1.1.1 service tcp 80 80 [Configure static Port NAT. The private IP 192.168.1.1 in DMZ will be mapped statically to public IP 100.1.1.1 in outside zone only for port 80] Access Control Lists (ACL) ciscoasa(config)# access-list OUTSIDE_IN extended permit tcp any host 192.168.1.1 eq 80 [Create an ACL to allow TCP access from "any" source IP to host 192.168.1.1 port 80] ciscoasa(config)# access-group OUTSIDE_IN in interface outside [Apply the ACL above at the "outside" interface for traffic coming "in" the interface] ciscoasa(config)# access-list INSIDE_IN extended deny ip host 192.168.1.1 any ciscoasa(config)# access-list INSIDE_IN extended permit ip any any ciscoasa(config)# access-group INSIDE_IN in interface inside [Create an ACL to deny all traffic from host 192.168.1.1 to any destination and allow everything else. This ACL is then applied at the "inside" interface for traffic coming "in" the interface] Object Groups ciscoasa(config)# object-group network WEB_SRV ciscoasa(config-network)# network-object host 192.168.1.1 ciscoasa(config-network)# network-object host 192.168.1.2 [Create a network group having two hosts (192.168.1.1 and 192.168.1.2). This group can be used in other configuration commands such as ACLs] ciscoasa(config)# object-group network DMZ_SUBNETS ciscoasa(config-network)# network-object 10.1.1.0 255.255.255.0 ciscoasa(config-network)# network-object 10.2.2.0 255.255.255.0 [Create a network group having two subnets (10.1.1.0/24 and 10.2.2.0/24). This group can be used in other configuration commands such as ACLs] ciscoasa(config)# object-group service DMZ_SERVICES tcp ciscoasa(config-service)# port-object eq http ciscoasa(config-service)# port-object eq https ciscoasa(config-service)# port-object range 21 23 [Create a service group having several ports. This group can be used in other configuration commands such as ACLs] ciscoasa(config)# access-list OUTSIDE-IN extended permit tcp any object-group DMZ_SUBNETS object-group DMZ_SERVICES [Example of using object groups in ACLs] Subinterfaces and VLANs ciscoasa(config)# interface gigabitethernet 0/1 ciscoasa(config-if)# no nameif ciscoasa(config-if)# no security-level ciscoasa(config-if)# no ip address ciscoasa(config-if)# exit ciscoasa(config)# interface gigabitethernet 0/1.1 ciscoasa(config-subif)# vlan 10 ciscoasa(config-subif)# nameif inside1 ciscoasa(config-subif)# security-level 80 ciscoasa(config-subif)# ip address 192.168.1.1 255.255.255.0 ciscoasa(config)# interface gigabitethernet 0/1.2 ciscoasa(config-subif)# vlan 20 ciscoasa(config-subif)# nameif inside2 ciscoasa(config-subif)# security-level 90 ciscoasa(config-subif)# ip address 192.168.2.1 255.255.255.0 [In example above we have a physical interface (GE0/1) which is split into two subinterfaces (GE0/1.1 and GE0/1.2) belonging to two different VLANs with different IPs and security levels] Clock Settings ciscoasa# clock set 18:30:00 Aug 10 2016 [Set the time and date] ciscoasa(config)# clock timezone MST -7 [Set the timezone to MST with -7 hours offset from UTC] ciscoasa(config)# clock summer-time MST recurring 1 Sunday April 2:00 last Sunday October 2:00 [Set daylight saving time] Logging Commands ASA(config)# logging enable [Enable logging] ASA(config)# logging timestamp [Attach timestamp to log messages] ASA(config)# logging buffer-size 64000 [Set log buffer to 64kB] ASA(config)# logging buffered warnings [Send warning log messages to buffer log] ASA(config)# logging asdm errors [Send error log messages to ASDM management] ASA(config)# logging host inside 192.168.1.30 ASA(config)# logging trap errors [Send error log messages to syslog server 192.168.1.30] Enable Management Access with ASDM ASA(config)# asdm image disk0:/asdm-647.bin [Location of ASDM image on the ASA] ASA(config)# http server enable [Enable the http server on the device] ASA(config)# http 10.10.10.0 255.255.255.0 inside [Tell the device which IP addresses are allowed to connect with HTTP (ASDM)] ASA(config)#username admin password adminpass [Configure user/pass to login with ASDM] DHCP (Assign IP addresses to computers from the ASA device) ciscoasa(config)# dhcpd address 192.168.1.101-192.168.1.110 inside [Create a DHCP address pool to assign to clients. This address pool must be on the same subnet as the ASA interface] ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129 [The DNS servers to assign to clients via DHCP] ciscoasa(config)# dhcpd enable inside [Enable the DHCP server on the inside interface] Permit Traffic Between Same Security Levels ciscoasa(config)# same-security-traffic permit inter-interface [Permits communication between different interfaces that have the same security level.] ciscoasa(config)# same-security-traffic permit intra-interface [Permits traffic to enter and exit the same interface.] Useful Verification and Troubleshooting Commands ciscoasa# show access-list OUTSIDE-IN [Shows hit-counts on ACL with name "OUTSIDE-IN". It shows how many hits each entry has on the ACL] Sample output: access-list OUTSIDE-IN line 1 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0 255.255.255.0 eq telnet (hitcnt=15) 0xca10ca21 ciscoasa# show clock [Verify that time and date are correct on the appliance] ciscoasa# show conn [The show conn command displays the number of active TCP and UDP connections, and provides information about connections of various types.] ciscoasa# show conn all [Shows all the connections through the appliance] ciscoasa# show conn state up,http_get,h323,sip [Shows HTTP GET, H323, and SIP connections that are in the "up" state] ciscoasa# show conn count 54 in use, 123 most used [Shows overall connection counts] ciscoasa# show cpu usage [show CPU utilization] ciscoasa# show crypto ipsec sa [show details about IPSEC VPNs like packets encrypted/decrypted, tunnel peers etc] ciscoasa# show crypto isakmp sa [show details if an IPSEC VPN tunnel is up or not. MM_ACTIVE means the tunnel is up] ciscoasa# show disk [List the contents of the internal flash disk of the ASA] ciscoasa# show environment [Displays operating information about hardware system components such as CPU, fans, power supply, temperature etc] ciscoasa# show failover [Displays information about Active/Standby failover status] ciscoasa# show interface [Shows information about Interfaces, such as line status, packets received/sent, IP address etc] ciscoasa# show local-host [Displays the network states of local hosts. A local-host is created for any host that forwards traffic to, or through, the ASA.] ciscoasa# show memory [Displays maximum physical memory and current free memory] ciscoasa# show route [Displays the routing table] ciscoasa# show version [Displays the software version, hardware configuration, license key, and related uptime data] ciscoasa# show xlate [Displays information about NAT sessions] DOWNLOAD IN PDF FORMAT HERE Harris Andrea is an Engineer with more than two decades of professional experience in the fields of TCP/IP Networks, Information Security and I.T. Over the years he has acquired several professional certifications such as CCNA, CCNP, CEH, ECSA etc. He is a self-published author of two books ("Cisco ASA Firewall Fundamentals" and "Cisco VPN Configuration Guide") which are available at Amazon and on this website as well. 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 You can partition a single ASA into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management; however, some features are not supported. See the feature chapters for more information. In multiple context mode, the ASA includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the ASA. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context. The admin context is just like any other context, except that when a user logs into the admin context, then that user has system administrator rights and can access the system and all other contexts.