Cheatography

Cisco Device Security Cheat Sheet

by River L. (Tamaranth) via cheatography.com/42882/cs/14448/

Login Enhancements

Command	Function
`login block-for 120 attempts 3 within 30`	blocks login attempts for 120 secs if 3 fail within 30 secs (`login local` must be configured)
`login quiet-mode access-class [acl-name | acl-number]`	maps to an ACL so only authorized hosts can attempt to login
`login delay seconds`	wait-time between login attempts
`login on-success log`	records successful logins
`login on-failure log`	records failed login attempts

> Login enhancements don't apply to console connections
> `login block-for` must be configured before any others

Role-Based CLI Views

Command	Mode	Function
`aaa new-model`	global	enables AAA
`parser view view-name`	global	creates a new view (must be in root view)
`secret password`	view	assigns view password (required)
`commands parser-mode [include|exclude] [command|interface]`	view	assigns command or interface to view
`enable view view-name`	priv. EXEC	enters view (enable secret for root password)
`parser view view-name superview`	global	creates a new superview
`secret password`	superview	assigns superview password (required)
`view view-name`	superview	assigns existing view to superview

IPsec VPNs (Site-to-Site)

	Command	Mode
----- Phase 1 -----		
`cry is en`	`crypto isakamp enable`	global
`cry is pol 10`	`crypto isakmp policy 10`	global
`h sha`	`hash sha`	(config-isakmp)
`a p (auth pre)`	`authentication pre-share`	(-isakmp)
`g 14`	`group [DH group #]`	(-isakmp)
`l 3600`	`lifetime [secs]`	(-isakmp)
`enc a 256`	`encryption aes 256`	(-isakmp)
`cry is key vpnpass add 10.2.2.2`	`crypto isakmp key [key] address [peer IP]`	global
----- Phase 2 -----		
`cry ip t VPN-SET esp-a 256 esp-sha-`	`crypto ipsec transform-set [tag] [encry.] [bits] [hash]`	global

By **River L.** (Tamaranth)
cheatography.com/tamaranth/

IPsec VPNs (Site-to-Site) (cont)

`cry ip s l s`	`crypto ipsec security-association lifetime seconds 1800`	global
`cry map CMAP 10 ipsec-i`	`crypto map [name] [seq #] ipsec-isakmp`	global
`m add 101`	`match address 101`	(-crypto-map)
`s pe 10.2.2.2`	`set peer [peer IP]`	(-crypto-map)
`s pfs group14`	`set pfs [group#]`	(-crypto-map)
`s t VPN-SET`	`set transform-set [tag]`	(-crypto-map)
`s s li s 900`	`set security-association lifetime seconds [secs]`	(-crypto-map)
`desc [text]`	`description [text]`	(-crypto-map)
`cry m CMAP`	`crypto map [name]`	interface

Line Config Mode

Command	Line	Function
`no exec`	any unused	disables EXEC mode for the line (outgoing connections only)
`login local`	all	forces username/password authentication from local database
`logging synchronous`	all	prevents logging from interrupting commands
`exec-timeout 5 0`	all	logs out after 5 mins inactive

Informational/Show Commands

Short Command	Full Command	What It Displays
`sh login`	`show login`	configured login settings
`sh login f`	`show login failures`	details about login failures (src IP, count, time/date, etc)
`sh cry key mypubkey r`	`show crypto key mypubkey rsa`	current RSA keys
`sh ip ssh`	`show ip ssh`	SSH configuration
`sh ssh`	`show ssh`	current SSH connections
`sh p v a`	`show parser view all`	summary of all configured views (asterisk indicates superview)
`sh sec b`	`show secure bootset`	verification of the archive
`sh logg`	`show logging`	logging configuration & buffered syslog messages
`sh us`	`show users`	users connected to the device
`sh cr is po`	`show crypto isakmp policy`	ISAKMP policy configuration
`sh cr ip sa`	`show crypto ipsec sa`	IPsec security association
`sh cr map`	`show crypto map`	crypto map configuration

Logging & Monitoring

Command	Mode	Function
`service timestamps log datetime msec`	global	enables timestamps service
`logging host` *ip-address*	global	specifies syslog server
`logging trap` *level*	global	sets log severity level
`logging source-interface` *ip-address*	global	identifies the device sending the log info
`logging on`	global	turns on logging

Secure Bootset

Command	Mode	Function
`secure boot-image`	global	secures IOS image & enables Cisco IOS image resilience
`secure boot-config`	global	takes snapshot of running-config to save in persistent storage
--- To Restore Secure Configuration ---		
`reload`-> ROMmon mode		
`dir`	ROMmon	lists contents of device where secure bootset is stored
`boot flash:`*filename*	ROMmon	boots route with secure IOS image
`secure boot-config restore flash:`*filename*	global	restores secure config

SSH Configuration

Command	Function
`user` *Bob* `algorithm-type scrypt secret` *password*	creates user in local database
`ip domain-name span.com`	sets network domain name
`crypto key zeroize rsa`	removes any existing RSA key pairs
`cry key gen rsa gen mod 1024`	creates RSA encryption key (max: 4096 bits)
`transport input ssh`	enables SSH (line config, vty)
`ip ssh time-out` *seconds*	sets SSH timeout length
`ip ssh authentication-retries 2`	sets number of login attempts before user is disconnected
`ip ssh version 2`	sets SSH version to v2

Miscellaneous Configurations

Command	Function
`license boot module c1900 technology-package securityk9`	*Adds security package to 1941 routers!*
`no service password-recovery`	prevents an attacker from recovering the router password

By **River L.** (Tamaranth)
cheatography.com/tamaranth/