

# debug aaa through debug xdmcp Commands

### debug aaa

To show debug messages for AAA, use the **debug aaa** command in privileged EXEC mode. To stop showing AAA messages, use the **no** form of this command.

debug aaa [ accounting | authentication | authorization | internal | vpn [ level ] ]

no debug aaa

Syntax Description	accounting						
	authentication	(Optional) Show					
	authorization(Optional) Show debug messages for authorization only.						
	internal	nternal (Optional) Show debug messages for AAA functions supported by the local database only.					
	level	(Optional) Specif	ies the debug leve	el. Valid wi	th the <b>vpn</b> key	word only.	
	vpn	(Optional) Show	debug messages f	or VPN-rel	ated AAA fun	ctions only.	
Defaults Command Modes	The default <i>level</i> is T The following table	1. shows the modes in wh	ich you can enter	the comma	und:		
		Firewall	Security Context				
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	
Command History	Release	Modification					
	7.0(1)	This command w	as modified to inc	lude new k	eywords.		
Usage Guidelines Examples	undebug all comma	amand displays detailed ands turn off all enabled aple enables debugging f	debugs.		-		
zampies	-		IOI AAA IUNCUON	s supported	i by the local d	atabase:	
	hostname(config)# debug aaa internal	debug aaa internal					

Related Commands	Command	Description
	show running-config	Displays running configuration related to AAA.
	aaa	

### debug appfw

To display detailed information about application inspection, use the **debug appfw** command in privileged EXEC mode. To disable debugging, Use the **no** form of this command.

debug appfw [chunk | event | eventverb | regex]

no debug appfw [chunk | event | eventverb | regex]

Syntax Description	chunk		nal) Displays er encoded pa	s runtime inform ckets.	ation abou	t processing of	chunked	
	event	(Option	(Optional) Displays debug information about packet inspection events.					
	eventverb	(Optional) Displays the action taken by the security appliance in response to an event.						
	regex	(Option signatu	· • •	s information ab	out matchin	ng patterns wit	h predefined	
Defaults	All options are ena	ıbled by defaul	lt.					
Command Modes	The following table	e shows the mo	odes in whic	h you can enter	the comma	nd:		
			Firewall M	ode	Security C	ontext		
						Multiple		
	<b>Command Mode</b>		Routed	Transparent	Single	Context	System	
	Privileged EXEC		•	•	•	•	_	
Command History	Release Modification							
	7.0(1)This command was introduced.							
Usage Guidelines	The <b>debug appfw</b> <b>debug all</b> or <b>unde</b> l					application ins	pection. The <b>n</b>	
Examples	The following exar	mple enables th	he display of	detailed inform	ation about	t application i	nspection:	
Examples	The following example of the following example	-	he display of	detailed inform	ation about	t application i	nspection:	
Examples Related Commands	-	-		detailed inform	ation about	t application i	nspection:	
	hostname# <b>debug a</b>	appfw Descri	ption	detailed inform				

### debug arp

To show debug messages for ARP, use the **debug arp** command in privileged EXEC mode. To stop showing debug messages for ARP, use the **no** form of this command.

debug arp

no debug arp

Syntax Description	This command has no arguments or keywords.
--------------------	--

**Defaults** No default behavior or values.

**Command Modes** The following table shows the modes in which you can enter the command:

	Firewall N	Security Context			
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	_

Command History	Release	Modification
Preexisting		This command was preexisting.

**Usage Guidelines** Using **debug** commands might slow down traffic on busy networks.

Examples The following example enables debug messages for ARP: hostname# debug arp

<b>Related Commands</b>	Command	Description
	arp	Adds a static ARP entry.
	show arp statistics	Shows ARP statistics.
	show debug	Shows all enabled debuggers.

### debug arp-inspection

To show debug messages for ARP inspection, use the **debug arp-inspection** command in privileged EXEC mode. To stop showing debug messages for ARP inspection, use the **no** form of this command.

debug arp-inspection

no debug arp-inspection

Syntax Description	This command has no arguments	or keywords.
--------------------	-------------------------------	--------------

**Defaults** No default behavior or values.

**Command Modes** The following table shows the modes in which you can enter the command:

	Firewall M	Firewall Mode		Security Context		
				Multiple		
Command Mode	Routed	Transparent	Single	Context	System	
Privileged EXEC		•	•	•	_	

<b>Command History</b>	Release	Modification
	7.0(1)	This command was introduced.

**Usage Guidelines** Using **debug** commands might slow down traffic on busy networks.

**Examples** The following example enables debug messages for ARP inspection: hostname# debug arp-inspection

<b>Related Commands</b>	Command	Description
	arp	Adds a static ARP entry.
	arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
	show debug	Shows all enabled debuggers.

## debug asdm history

To view debug information for ASDM, use the **debug asdm history** command in privileged EXEC mode.

debug asdm history level

Syntax Description	<i>level</i> (Optional) Specifies the debug level.					
		(optional) specific				
Defaults	The default <i>level</i> is 1.					
Command Modes	The following table show	ws the modes in whic	h you can enter	the comma	nd:	
		Firewall N	lode	Security C	Context	
					Multiple	
	Command Mode	Routed	Transparent	Single	Context	System
	Privileged EXEC	•	•	•	•	•
Command History	Release	Modification				
	7.0(1)	This command was debug asdm histo	-	ne uebug p		
Usage Guidelines	Because debugging outp unusable. For this reason troubleshooting sessions during periods of lower likelihood that increased	n, use <b>debug</b> comman with Cisco technical network traffic and for	nds only to troub support staff. M ewer users. Debu	bleshoot spe foreover, it agging duri	ecific problems is best to use <b>d</b> ng these period	s or during e <b>bug</b> commands
Examples	The following example of	enables level 1 debug	ging of ASDM:			
	hostname# <b>debug asdm</b> : debug asdm history en					
	hostname#					
Related Commands	Command	Description				
	show asdm history	Displays the content	nts of the ASDN	I history bu	ıffer.	
				•		

### debug context

To show debug messages when you add or delete a security context, use the **debug context** command in privileged EXEC mode. To stop showing debug messages for contexts, use the **no** form of this command.

debug context [level]

no debug context [level]

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.								
Defaults	The default level is 1	Ι.							
Command Modes	The following table :	shows the modes in whic	h you can enter	the comma	ınd:				
		Firewall N	lode	Security (	Context				
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•		—	•			
Commond History	Release	Modification							
Command History	ReleaseModification7.0(1)This command was introduced.								
Jsage Guidelines	Using <b>debug</b> comma	ands might slow down tra	affic on busy net	works.					
Examples	The following examp hostname# <b>debug co</b>	ple enables debug messa <sub>:</sub> ntext	ges for context n	nanagemen	t:				
Related Commands	Command	Description							
Related Commands	Command context	Creates a security		stem config	guration and er	nters context			
Related Commands		-	e.	stem config	guration and er	nters context			

### debug cplane

To show debug messages about the control plane that connects internally to an SSM, use the **debug cplane** command in privileged EXEC mode. To stop showing debug messages for the control plane, use the **no** form of this command.

debug cplane [level]

no debug cplane [level]

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.								
Defaults	The default level is 1.								
Command Modes	The following table sho	ows the modes in whic	ch you can enter	the comma	and:				
		Firewall N	Node	Security (	Context				
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•		•			
Command History	Release Modification								
	7.0(1)This command was introduced.								
Usage Guidelines Examples	Using <b>debug</b> command The following example	enables debug messa							
	hostname# <b>debug cpla</b>	ne							
Related Commands	Command	Description							
	hw-module module recover	Recovers an intelli server.	gent SSM by loa	ading a reco	overy image fr	om a TFTP			
	hw-module module reset	Shuts down an SSI	M and performs	a hardware	reset.				
	hw-module module	Reloads the intelli	( 0 0 ) ( C						

Command	Description
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

### debug crypto ca

To show debug messages for PKI activity (used with CAs), use the **debug crypto ca** command in privileged EXEC mode. To stop showing debug messages for PKI, use the **no** form of this command.

debug crypto ca [messages | transactions] [level]

no debug crypto ca [messages | transactions] [level]

(Optional) Shows only debug messages for PKI transactions.         level       (Optional) Sets the debug messages level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number. Level 1 (the default) shows messages only when errors occur. Level 2 shows warnings. Level 3 shows informational messages. Levels 4 and up show additional information for troubleshooting.         Defaults       By default, this command shows all debug messages. The default level is 1.         Command Modes       Firewall Mode       Security Context         Multiple       Context       System         Privileged EXEC       •       •       •         Command History       Release       Modification         Prexisting       This commands might slow down traffic on busy networks.       Examples         Using debug commands might slow down traffic on busy networks.       Examples       Examples         Releated Commands       Description       debug messages for PKI: hostname# debug crypto ca         Releated Commands       Description       debug messages for the crypto engine. debug messages for the crypto engine. debug crypto engine	Syntax Description	messages	(Optional) Shows	(Optional) Shows only debug messages for PKI input and output messages.						
default is 1. To display additional messages at higher levels, set the level to         a higher number. Level 1 (the default) shows messages only when errors         occur. Level 2 4 and up show additional information for troubleshooting.         Defaults       By default, this command shows all debug messages. The default level is 1.         Command Modes       The following table shows the modes in which you can enter the command:         Image: Command Mode       Firewall Mode       Security Context         Command Mode       Routed       Transparent       Single         Privileged EXEC       •       •       •         Viewed EXEC       •       •       •       •         Viewed EXEC       •       •       •       •       •         Using debug commands might slow down traffic on busy networks.       Image: Security context       Image: Security context         Release       Modification       Prexisting       This command was preexisting.       Image: Security context         Using debug commands might slow down traffic on busy networks.       Image: Security context       Image: Security context       Image: Security context         Related Commands       Command Description       Image: Security context       Image: Security context       Image: Security context         Related Commands       Command Description       Sec		transactions	(Optional) Shows	only debug mess	ages for Pk	XI transactions	•			
a higher number. Level 1 (the default) shows messages only when errors occur. Level 2 shows warnings. Level 3 shows informational messages. Levels 4 and up show additional information for troubleshooting.         Defaults       By default, this command shows all debug messages. The default level is 1.         Command Modes       The following table shows the modes in which you can enter the command:		level								
occur. Level 2 shows warnings. Level 3 shows informational messages. Levels 4 and up show additional information for troubleshooting.         Defaults       By default, this command shows all debug messages. The default level is 1.         Command Modes       The following table shows the modes in which you can enter the command:         Image: Command Mode       Firewall Mode         Release       Multiple         Command History       Release         Prexisting       This command was preexisting.         Using debug commands might slow down traffic on busy networks.       Image: Command might slow down traffic on busy networks.         Examples       The following example enables debug messages for PKI: hostname# debug crypto ca         Related Commands       Command Description         debug crypto engine       Shows debug messages for the crypto engine.										
Levels 4 and up show additional information for troubleshooting.         Defaults         By default, this command shows all debug messages. The default level is 1.         Command Modes         The following table shows the modes in which you can enter the command:         Image: Security Context         Multiple         Command Mode         Privileged EXEC       •       •       •       -         Command History         Release       Modification       Prexisting       This command was preexisting.         Using debug commands might slow down traffic on busy networks.         Examples       The following example enables debug messages for PKI: hostname# debug crypto ca       Description         debug crypto engine       Shows debug messages for the crypto engine.       debug crypto engine										
Command Modes       The following table shows the modes in which you can enter the command:         Firewall Mode       Security Context         Command Mode       Routed       Transparent       Single       Multiple         Command Mode       Routed       Transparent       Single       Context       System         Privileged EXEC       •       •       •       •       -         Command History       Release       Modification       Preexisting       This command was preexisting.         Usage Guidelines       Using debug commands might slow down traffic on busy networks.       Examples       The following example enables debug messages for PKI: hostname# debug crypto ca         Related Commands       Command       Description       debug crypto ca         Related Commands       Command       Description       debug crypto engine         Gebug crypto engine       Shows debug messages for IPSec.       Shows debug messages for IPSec.										
Command Modes       The following table shows the modes in which you can enter the command:         Firewall Mode       Security Context         Command Mode       Routed       Transparent       Single       Multiple         Command Mode       Routed       Transparent       Single       Context       System         Privileged EXEC       •       •       •       •       -         Command History       Release       Modification       Preexisting       This command was preexisting.         Usage Guidelines       Using debug commands might slow down traffic on busy networks.       Examples       The following example enables debug messages for PKI: hostname# debug crypto ca         Related Commands       Command       Description       debug crypto ca         Related Commands       Command       Description       debug crypto engine         Gebug crypto engine       Shows debug messages for IPSec.       Shows debug messages for IPSec.										
Command Modes       The following table shows the modes in which you can enter the command:         Firewall Mode       Security Context         Command Mode       Routed       Transparent       Single       Multiple         Command Mode       Routed       Transparent       Single       Context       System         Privileged EXEC       •       •       •       •       -         Command History       Release       Modification       Preexisting       This command was preexisting.         Usage Guidelines       Using debug commands might slow down traffic on busy networks.       Examples       The following example enables debug messages for PKI: hostname# debug crypto ca         Related Commands       Command       Description       debug crypto ca         Related Commands       Command       Description       debug crypto engine         Gebug crypto engine       Shows debug messages for IPSec.       Shows debug messages for IPSec.	Defeute		. 1 . 1	<b>TI</b> 1.(		. 1				
Firewall Mode       Security Context         Command Mode       Routed       Transparent       Single       Multiple         Privileged EXEC       •       •       •       •       •         Command History       Release       Modification       •       •       •       •         Prexisting       This command was preexisting.       •       •       •       •       •         Usage Guidelines       Using debug commands might slow down traffic on busy networks.       •	Detaults	By default, this comman	nd shows all debug m	lessages. The def	ault level is	s 1.				
Firewall Mode       Security Context         Command Mode       Routed       Transparent       Single       Multiple         Privileged EXEC       •       •       •       •       •         Command History       Release       Modification       •       •       •       •         Prexisting       This command was preexisting.       •       •       •       •       •         Usage Guidelines       Using debug commands might slow down traffic on busy networks.       •										
Command Mode       Routed       Transparent       Single       Multiple         Privileged EXEC       •	Command Modes	The following table sho	ws the modes in which	ch you can enter	the comma	nd:				
Command Mode       Routed       Transparent       Single       Multiple         Privileged EXEC       •										
Command Mode       Routed       Transparent       Single       Context       System         Privileged EXEC       •<			Firewall N	Node	Security C	ontext				
Privileged EXEC       •						Multiple				
Command History       Release       Modification         Preexisting       This command was preexisting.         Usage Guidelines       Using debug commands might slow down traffic on busy networks.         Examples       The following example enables debug messages for PKI: hostname# debug crypto ca         Related Commands       Command       Description debug crypto engine         Shows debug messages for the crypto engine.       debug crypto ipsec		Command Mode	Routed	Transparent	Single	Context	System			
Preexisting       This command was preexisting.         Using debug commands might slow down traffic on busy networks.         Examples       The following example enables debug messages for PKI: hostname# debug crypto ca         Related Commands       Command       Description         debug crypto engine       Shows debug messages for the crypto engine.         debug crypto ipsec       Shows debug messages for IPSec.		Privileged EXEC	•	•	•	•				
Preexisting       This command was preexisting.         Using debug commands might slow down traffic on busy networks.         Examples       The following example enables debug messages for PKI: hostname# debug crypto ca         Related Commands       Command       Description         debug crypto engine       Shows debug messages for the crypto engine.         debug crypto ipsec       Shows debug messages for IPSec.										
Usage Guidelines       Using debug commands might slow down traffic on busy networks.         Examples       The following example enables debug messages for PKI: hostname# debug crypto ca         Related Commands       Command       Description debug crypto engine         Shows debug messages for the crypto engine. debug crypto ipsec       Shows debug messages for IPSec.	Command History	Release	Modification							
Examples       The following example enables debug messages for PKI:         hostname# debug crypto ca         Related Commands       Command       Description         debug crypto engine       Shows debug messages for the crypto engine.         debug crypto ipsec       Shows debug messages for IPSec.										
Examples       The following example enables debug messages for PKI:         hostname# debug crypto ca         Related Commands       Command       Description         debug crypto engine       Shows debug messages for the crypto engine.         debug crypto ipsec       Shows debug messages for IPSec.										
Examples       The following example enables debug messages for PKI:         hostname# debug crypto ca         Related Commands       Command       Description         debug crypto engine       Shows debug messages for the crypto engine.         debug crypto ipsec       Shows debug messages for IPSec.										
Mostname# debug crypto ca         Related Commands       Command       Description         debug crypto engine       Shows debug messages for the crypto engine.         debug crypto ipsec       Shows debug messages for IPSec.	Usage Guidelines	Using <b>debug</b> command	s might slow down tr	affic on busy net	works.					
Mostname# debug crypto ca         Related Commands       Command       Description         debug crypto engine       Shows debug messages for the crypto engine.         debug crypto ipsec       Shows debug messages for IPSec.										
Mostname# debug crypto ca         Related Commands       Command       Description         debug crypto engine       Shows debug messages for the crypto engine.         debug crypto ipsec       Shows debug messages for IPSec.	Fxamples	The following example enables debug messages for PKI.								
Related Commands       Command       Description         debug crypto engine       Shows debug messages for the crypto engine.         debug crypto ipsec       Shows debug messages for IPSec.	Exampleo		-	505 IOI I III.						
debug crypto engineShows debug messages for the crypto engine.debug crypto ipsecShows debug messages for IPSec.										
debug crypto engineShows debug messages for the crypto engine.debug crypto ipsecShows debug messages for IPSec.										
debug crypto engineShows debug messages for the crypto engine.debug crypto ipsecShows debug messages for IPSec.	Rolatod Commande	Command	Description							
debug crypto ipsec Shows debug messages for IPSec.			•	sages for the crys	nto engine					
					no engine.					

### debug crypto engine

To show debug messages for the crypto engine, use the **debug crypto engine** command in privileged EXEC mode. To stop showing debug messages for the crypto engine, use the **no** form of this command.

debug crypto engine [level]

no debug crypto engine [level]

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.						
Defaults	The default level is 1.						
Command Modes	The following table show	ws the modes in whic	h you can enter	the comma	ind:		
		Firewall N	lode	Security (	Context		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	_	
Command History	<b>Release</b> 7.0(1)	Modification This command was	introduced.				
Jsage Guidelines	Using <b>debug</b> commands	s might slow down tra	ffic on busy net	works.			
_	Using <b>debug</b> commands The following example of hostname# <b>debug</b> crypt	enables debug messag					
Examples	The following example of	enables debug messag					
Examples	The following example of hostname# <b>debug crypt</b>	enables debug messag o engine	ges for the crypt	o engine:			
Usage Guidelines Examples Related Commands	The following example of hostname# <b>debug crypt</b>	enables debug messag o engine Description	ges for the crypt	o engine:			

10-13

### debug crypto ipsec

To show debug messages for IPSec, use the **debug crypto ipsec** command in privileged EXEC mode. To stop showing debug messages for IPSec, use the **no** form of this command.

**debug crypto ipsec** [*level*]

no debug crypto ipsec [level]

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.							
Defaults	The default level is 1.							
Command Modes	The following table sho	ws the modes in whic	h you can enter	the comma	ınd:			
		Firewall N	lode	Security (	Context			
				-	Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•				
		·	,					
Command History	Release Modification							
	Preexisting	This command was	s preexisting.					
Jsage Guidelines	Using <b>debug</b> commands	s might slow down tra	uffic on busy net	works.				
xamples	The following example	enables debug messa	ges for IPSec:					
	hostname# <b>debug crypt</b>	o ipsec						
Related Commands	Command	Description						
nenateu commanus	debug crypto ca         Shows debug messages for the CA.							
	debug crypto ca							
	debug crypto ca debug crypto engine	-	-					

### debug crypto isakmp

To show debug messages for ISAKMP, use the **debug crypto isakmp** command in privileged EXEC mode. To stop showing debug messages for ISAKMP, use the **no** form of this command.

debug crypto isakmp [timers] [level]

no debug crypto isakmp [timers] [level]

Syntax Description	timers	(Optional) Shows d	ebug messages	for ISAKM	IP timer expira	tion.			
	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The								
		default is 1. To display additional messages at higher levels, set the level to a higher number. Level 1 (the default) shows messages only when errors							
		occur. Levels 2 thro							
		decrypted ISAKMI	-			vel 255 shows			
		hexadecimal dump	s of decrypted is	SAKMP pa	ckets.				
Defaults	The default level is 1.								
Command Modes	The following table sho	ws the modes in whic	h you can enter	the comma	nd:				
		Firewall M	ode	Security C	ontext				
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•					
Command History	Release Modification								
	Preexisting     This command was preexisting.								
Usage Guidelines	Using <b>debug</b> commands	s might slow down tra	ffic on busy netw	works.					
-		-							
	The following example	enables debug messag							
Usage Guidelines Examples		enables debug messag							
	The following example	enables debug messag							
Examples	The following example hostname# <b>debug crypt</b>	enables debug messag o isakmp	es for ISAKMP						
Examples	The following example hostname# <b>debug crypt</b>	enables debug messag o isakmp Description	tes for ISAKMP	:					

### debug ctiqbe

To show debug messages for CTIQBE application inspection, use the **debug ctiqbe** command in privileged EXEC mode. To stop showing debug messages for CTIQBE application inspection, use the **no** form of this command.

debug ctiqbe [level]

no debug ctiqbe [level]

Syntax Description	level	(Optional) Sets the default is 1. To dis a higher number.									
Defaults	The default value for <i>le</i>	vel is 1.									
Command Modes	The following table sho	ows the modes in whic	h you can enter	the comma	ind:						
		Firewall N	lode	Security C	ontext						
					Multiple						
	Command Mode	Routed	Transparent	Single	Context	System					
	Privileged EXEC	•	•	•	•						
	<u></u>	<b>BA</b> 11/2									
Command History	Release	Modification	• .•								
	Preexisting	Preexisting This command was preexisting.									
Usage Guidelines	To see the current debug enter the <b>no debug</b> com command.										
Note	Enabling the <b>debug cti</b>	<b>qbe</b> command may sl	ow down traffic	on busy ne	tworks.						
Examples	The following example inspection:	enables debug messaş	ges at the defaul	t level (1) f	or CTIQBE ap	plication					
	hostname# <b>debug ctiq</b>	be									

#### **Related Commands**

Command	Description
inspect ctiqbe	Enables CTIQBE application inspection.
show ctiqbe	Displays information about CTIQBE sessions established through the security appliance.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

### debug dhcpc

To enable debugging of the DHCP client, use the **debug dhcpc** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug dhcpc {detail | packet | error} [level]

no debug dhcpc {detail | packet | error} [level]

Syntax Description	detail	Display	s detail eve	ent information th	hat is assoc	iated with the	DHCP client.			
- ,	error Displays error messages that are associated with the DHCP client.									
	<i>level</i> (Optional) Specifies the debug level. Valid values range from 1 to 255.									
	packet									
Defaults	The default debug le	vel is 1.								
Command Modes	The following table s	hows the mo	des in whic	h you can enter	the comma	nd:				
			Firewall N	lode	Security C	Context				
						Multiple				
	Command Mode		Routed	Transparent	Single	Context	System			
	Privileged EXEC		•	—	•	•				
Command History	Release	Modific	ation							
communa motory	Preexisting									
				· · · · · · · · · · · · · · · · · · ·						
Usage Guidelines	Displays DHCP clier	it debug infor	mation.							
	Because debugging of unusable. For this rea troubleshooting sessi during periods of low likelihood that increa	ason, use <b>deb</b> ons with Cisc ver network tr	<b>ug</b> comman to technical caffic and for	nds only to troub support staff. M ewer users. Debu	oleshoot spo oreover, it i ugging duri	ecific problems is best to use <b>d</b> ng these period	s or during ebug comman			
Examples										

#### **Related Commands**

Command	Description
show ip address dhcp	Displays detailed information about the DHCP lease for an interface.
show running-config interface	Displays the running configuration of the specified interface.

### debug dhcpd

To enable debugging of the DHCP server, use the **debug dhcpd** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug dhcpd {event | packet} [level]

no debug dhcpd {event | packet} [level]

Syntax Description	<b>event</b> Displays event information that is associated with the DHCP server.									
	<i>level</i> (Optional) Specifies the debug level. Valid values range from 1 to 255.									
	packet         Displays packet information that is associated with the DHCP server.									
Defaults	The default debug leve	el is 1.								
Command Modes	The following table sh	nows the modes in whic	ch you can enter	the comma	and:					
		Firewall M	lode	Security (	Context					
					Multiple					
	Command Mode	Routed	Transparent	Single	Context	System				
	Privileged EXEC	•	•	•	•	—				
Command History	Release Modification									
	Preexisting	This command was	s preexisting.							
Usage Guidelines	ē -	<b>nt</b> command displays ev lays packet information			OHCP server. T	he <b>debug dhcpo</b>				
	Use the <b>no</b> form of the	Use the <b>no</b> form of the debug dhcpd commands to disable debugging.								
	unusable. For this reas troubleshooting sessio during periods of lowe	ttput is assigned high p son, use <b>debug</b> comman ns with Cisco technical er network traffic and for ed <b>debug</b> command pro-	nds only to troub support staff. M ewer users. Debu	oleshoot sp oreover, it ugging duri	ecific problematis best to use <b>d</b> ing these period	s or during ebug command				
Examples	The following shows a	an example of enabling	DHCP event de	bugging:						
	hostname# <b>debug dhcpd event</b> debug dhcpd event enabled at level 1									

Related Commands	Command	Description
	show dhcpd	Displays DHCP binding, statistic, or state information.
	show running-config dhcpd	Displays the current DHCP server configuration.

### debug dhcprelay

To enable debugging of the DHCP relay server, use the **debug dhcpreleay** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug dhcprelay {event | packet | error } [level]

no debug dhcprelay {event | packet | error} [level]

Syntax Description	error	Displays	s error mess	sages that are as	sociated w	ith the DHCP	relay agent.	
	event	Displays	s event info	rmation that is a	associated	with the DHCF	relay agent.	
	<i>level</i> (Optional) Specifies the debug level. Valid values range from 1 to 255.							
	packet	Displays	s packet inf	ormation that is	associated	l with the DHC	P relay agent.	
Defaults	The default debug lev	vel is 1.						
Command Modes	The following table s	shows the mod	les in whic	h you can enter	the comma	and:		
			Firewall M	ode	Security (	Context		
						Multiple		
	Command Mode		Routed Transpar	Transparent	Single	Context	System	
	Privileged EXEC		•	—	•	•	—	
Command History	Release Modification							
	Preexisting			preexisting.				
Usage Guidelines	Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use <b>debug</b> commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use <b>debug</b> command during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased <b>debug</b> command processing overhead will affect system use.					s or during e <b>bug</b> commands		
Examples	The following examp hostname# <b>debug dho</b> debug dhcprelay err	cprelay erro	r		HCP relay	agent error me	essages:	

#### **Related Commands**

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
show dhcprelay statistics	Displays DHCP relay agent statistic information.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

10-23

### debug disk

To display file system debug information, use the **debug disk** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug disk {file | file-verbose | filesystem} [level]

no debug disk {file | file-verbose | filesystem}

Syntax Description	file Enables file-level disk debug messages.							
	file-verbose Enables verbose file-level disk debug messages							
	filesystem	Enable	es file system	n debug message	s.			
	level	defaul		debug message play additional n				
Defaults	The default value for	or <i>level</i> is 1.						
Command Modes	The following table	shows the m	odes in whic	h you can enter	the comma	nd:		
			Firewall M	lode	Security (	Context		
						Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	
	Privileged EXEC		•	•	•		•	
Command History	Release Modification							
	7.0(1)	This c	ommand was	s introduced.				
Usage Guidelines	Because debugging unusable. For this r troubleshooting ses during periods of lo likelihood that incre	eason, use <b>de</b> sions with Cis ower network	<b>bug</b> commar sco technical traffic and fe	nds only to troub support staff. M ewer users. Debu	oleshoot spo oreover, it ugging duri	ecific problems is best to use <b>d</b> ng these perior	s or during ebug commands	
Examples	The following example enables file-level disk debug messages. The <b>show debug</b> command reveals that file-level disk debug messages are enabled. The <b>dir</b> command causes several debug messages.							
	hostname# <b>debug disk file</b> debug disk file enabled at level 1 hostname# <b>show debug</b> debug vpn-sessiondb enabled at level 1 hostname# <b>dir</b>							

```
IFS: Opening: file flash:/, flags 1, mode 0
IFS: Opened: file flash:/ as fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
Directory of flash:/
IFS: Close: fd 3
IFS: Opening: file flash:/, flags 1, mode 0
                        14:42:27 Apr 04 2005 cdisk.binIFS: Opened: file flash:/ as fd 3
4
       -rw- 5124096
9
       -rw- 5919340
                        14:53:39 Apr 04 2005 ASDMIFS: Getdent: fd 3
                        15:18:56 Apr 21 2005 syslog
11
       drw- 0
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Close: fd 3
16128000 bytes total (5047296 bytes free)
```

<b>Related Commands</b>	Command	Description
	show debug	Displays current debug configuration.

### debug dns

To show debug messages for DNS, use the **debug dns** command in privileged EXEC mode. To stop showing debug messages for DNS, use the **no** form of this command.

debug dns [resolver | all] [level]

no debug dns [resolver | all] [level]

Syntax Description	level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.						
	resolver	(Optional) Shows only DNS resolver messages.						
	all	(Default) Shows a	ll messages, inclu	uding mess	ages about the	DNS cache.		
Defaults	The default level is 1	. If you do not specify a	any keywords, the	e security a	ppliance show	s all mesages.		
Command Modes	The following table s	hows the modes in whi	ch you can enter	the comma	ind:			
		Firewall I	Node	Security (	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	_		
			·					
Command History	Release Modification							
	7.0(1)	This command wa	introduced.					
Usage Guidelines		nds might slow down tr		works.				
Examples	The following example enables debug messages for DNS:							
	hostname# <b>debug dn:</b>	3						
Related Commands	Command	Description						
	class-map	Defines the traffic	class to which to	o apply sec	urity actions.			
	inspect dns	Enables DNS appl	lication inspectio	n.				
	policy-map	Associates a class		•				
	service-policy	Applies a policy n	nan to one or mor	ra interface				

### debug entity

To display management information base (MIB) debug information, use the **debug entity** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug entity [level]

no debug entity

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level a higher number.							
Defaults	The default value for <i>lev</i>	<i>el</i> is 1.						
Command Modes	The following table show	vs the modes in whic	h you can enter	the comma	nd:			
		Firewall N	lode	Security (	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	•		
Command History	Release Modification							
-	7.0(1)This command was introduced.							
Usage Guidelines	Because debugging outp unusable. For this reasor troubleshooting sessions during periods of lower likelihood that increased	n, use <b>debug</b> comman with Cisco technical network traffic and for	nds only to troub support staff. M ewer users. Debu	oleshoot spo loreover, it lgging duri	ecific problems is best to use <b>d</b> ng these period	s or during ebug commands		
Examples	The following example of debug messages are enal hostname# <b>debug entity</b> debug entity enabled hostname# <b>show debug</b> debug entity enabled hostname#	oled. / at level 1	nessages. The <b>sh</b>	ow debug	command reve	als that MIB		

#### **Related Commands**

Command	Description
show debug	Displays current debug configuration.

### debug fixup

To display detailed information about application inspection, use the **debug fixup** command in privileged EXEC mode. To disable debugging, Use the **no** form of this command.

debug fixup

no debug fixup

**Defaults** All options are enabled by default.

#### **Command Modes** The following table shows the modes in which you can enter the command:

	Firewall Mode Security Context				
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	

# Release Modification Preexisting This command was preexisting.

# Usage Guidelines The debug fixup command displays detailed information about application inspection. The no debug all or undebug all commands turn off all enabled debugs.

**Examples** The following example enables the display of detailed information about application inspection: hostname# debug fixup

<b>Related Commands</b>	Commands	Description
	class-map	Defines the traffic class to which to apply security actions.
	inspect protocol	Enables application inspection for specific protocols.
	policy-map	Associates a class map with specific security actions.

### debug fover

To display failover debug information, use the **debug fover** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug fover {cable | fail | fmsg | ifc | open | rx | rxdmp | rxip | switch | sync | tx | txdmp | txip | verify}

no debug fover {cable | fail | fmsg | ifc | open | rx | rxdmp | rxip | switch | sync | tx | txdmp | txip | verify}

Syntax Description	cable	Failover LAN s	tatus or serial cable	e status.			
	fail	Failover interna	l exception.				
	fmsg	fmsg     Failover message.       ifc     Network interface status trace.					
	ifc						
	open	Failover device	open.				
	rx	Failover messag	ge receive.				
	rxdmp	Failover receive	message dump (se	erial consol	e only).		
	rxip	IP network faile	over packet receive.	•			
	switch Failover switching status.						
	sync	Failover configu	eplication.				
	tx Failover message transmit.						
	txdmpFailover transmit message dump (serial console only).txipIP network failover packet transmit.						
	verify Failover message verify.						
Defaults Command Modes	No default behavior of The following table s	or values. shows the modes in w	hich you can enter	the comma	ind:		
		Firewa	ll Mode	Security (	ırity Context		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	
	Privileged EXEC		•	•	•		
Command History	Privileged EXEC Release	• Modification	•	•	•		

Usage Guidelines	unusable. For this re troubleshooting sess during periods of low	output is assigned high priority in the CPU process, it can render the system ason, use <b>debug</b> commands only to troubleshoot specific problems or during ions with Cisco technical support staff. Moreover, it is best to use <b>debug</b> commands wer network traffic and fewer users. Debugging during these periods decreases the ased <b>debug</b> command processing overhead will affect system use.
Examples	The following exam hostname# <b>debug fc</b> fover event trace	-
Related Commands	Command	Description
	show failover	Displays information about the failover configuration and operational statistics.

### debug fsm

To display FSM debug information, use the **debug fsm** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug fsm [level]

no debug fsm

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.						
Defaults	The default value for	level is 1.					
Command Modes	The following table s	hows the modes in whic	ch you can enter	the comma	und:		
		Firewall N	lode	Security Context			
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	
Command History	Release Modification						
	7.0(1)This command was introduced.						
Usage Guidelines	unusable. For this rea troubleshooting session during periods of low	utput is assigned high p ason, use <b>debug</b> comman ons with Cisco technical ver network traffic and for ased <b>debug</b> command pro-	nds only to troub support staff. M ewer users. Debu	oleshoot sp loreover, it ugging duri	ecific problem is best to use <b>d</b> ing these perio	s or during ebug commands	
Examples	debug messages are e hostname# debug fsm debug fsm enabled hostname# show debu	<b>n</b> at level 1	nessages. The <b>sh</b>	now debug	command reve	eals that FSM	

#### **Related Commands**

Command	Description
show debug	Displays current debug configuration.

# debug ftp client

To show debug messages for FTP, use the **debug ftp client** command in privileged EXEC mode. To stop showing debug messages for FTP, use the **no** form of this command.

debug ftp client [level]

no debug ftp client [level]

yntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. Th default is 1. To display additional messages at higher levels, set the level to a higher number.						
Defaults	The default value for <i>level</i>	The default value for <i>level</i> is 1.					
ommand Modes	The following table shows	the modes in whic	h you can enter	the comma	nd:		
		Firewall Mode		Security Context			
	Command Mode				Multiple		
		Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	_	
ommand History							
ommand History	Release         Modification           Preexisting         This command was preexisting.						
			, preenisting.				
sage Guidelines	To see the current debug conter the <b>no debug</b> command.	-		-	-	• •	
Note	Enabling the <b>debug ftp cl</b>	ient command may	y slow down traf	fic on busy	networks.		
Note	Enabling the <b>debug ftp cl</b>			<u> </u>			

#### **Related Commands**

Command	Description
сору	Uploads or downloads image files or configuration files to or from an FTP server.
ftp mode passive	Configures the mode for FTP sessions.
show running-config ftp mode	Displays FTP client configuration.

### debug generic

To display miscellaneous debug information, use the **debug generic** command in privileged EXEC mode. To disable the display of miscellaneous debug information, use the **no** form of this command.

debug generic [level]

no debug generic

Syntax Description	level       (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.         The default value for level is 1.					
Defaults						
Command Modes	The following table shows	s the modes in whic	h you can enter	the comma	ınd:	
		Firewall N	lode	Security Context		
				Single	Multiple	
	Command Mode	Routed	Transparent		Context	System
	Privileged EXEC	•	•	•	•	•
Command History	<b>Release</b> 7.0(1)	<b>Modification</b> This command was	s introduced.			
Usage Guidelines	Because debugging outpu unusable. For this reason, troubleshooting sessions w during periods of lower no likelihood that increased o	use <b>debug</b> commany with Cisco technical etwork traffic and for	nds only to troub support staff. M ewer users. Debu	bleshoot sp loreover, it ugging duri	ecific problematis best to use <b>d</b> and these period	s or during ebug commands
Examples	The following example en miscellaneous debug mess hostname# <b>debug generic</b> debug generic enabled hostname# <b>show debug</b> debug generic enabled hostname#	sages are enabled. ; at level 1	s debug message	es. The <b>sho</b> v	w debug comn	and reveals that

#### **Related Commands**

Command	Description
show debug	Displays current debug configuration.
# debug gtp

To display detailed information about GTP inspection, use the **debug gtp** command in privileged EXEC mode. To disable debugging, Use the **no** form of this command.

debug gtp [ error | event | ha | parser ]

no debug gtp [ error | event | ha | parser ]

yntax Description	error	error (Optional) Displays debug information on errors encountered while processing the GTP message.						
	event	(Optional) Di	splays debug in	formation on GT	P events.			
	ha option	(Optional) De	ebugs information	on on GTP HA e	vents.			
	parser(Optional) Displays debug information for parsing the GTP messages.							
efaults	All options are enabl	ed by default.						
ommand Modes	The following table s	shows the modes in	which you can	enter the comma	and:			
		Firew	Context					
					Multiple			
	Command Mode	Route	ed Transp	arent Single	Context	System		
	Privileged EXEC	•	•	•	•			
		I	I		I			
ommand History	Release	Release Modification						
-	7.0(1)	This comman	d was introduce	ed.				
Isage Guidelines <u>Note</u>	The <b>debug gtp</b> comr <b>undebug all</b> comman GTP inspection requ	nds turn off all enab	bled debugs.	about GTP insp	ection. The <b>no</b>	debug all o		
Examples	The following exam	ple enables the disp	lay of detailed i	information abou	ıt GTP inspecti	on.		

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.
show running-config gtp-map	Shows the GTP maps that have been configured.

## debug h323

To show debug messages for H.323, use the **debug h323** command in privileged EXEC mode. To stop showing debug messages for H.323, use the **no** form of this command.

debug h323 {h225 | h245 | ras} [asn | event]

no debug h323 {h225 | h245 | ras} [asn | event]

Syntax Description	h225	Specifies H.225 signaling.						
	h245	Specifi	ies H.245 sig	gnaling.				
	ras	Specifi	ies the regist	ration, admissio	n, and statu	us protocol.		
	<b>asn</b> (Optional) Displays the output of the decoded protocol data units (PDU)s.							
	event (Optional) Displays the events of the H.245 signaling or turns on both traces.							
Defaults	No default behavior of	or values.						
Command Modes	The following table s	hows the m	odes in whic	h you can enter	the comma	ind:		
			Firewall N	lode	Security (	Context		
						Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	
	Privileged EXEC		•	•	•	•		
Command History	Release	Release Modification						
	Preexisting	This co	ommand was	preexisting.				
Usage Guidelines	To see the current del enter the <b>no debug</b> co command.	-	-		-	-	• •	
<u>Note</u>	Enabling the <b>debug h323</b> command may slow down traffic on busy networks.							
Examples	The following examp	ole enables d	lebug messag	ges at the defaul	t level (1) f	For H.225 signa	aling	
	hostname# <b>debug h3</b>	23 h225						

Command	Description			
inspect h323	Enables H.323 application inspection.			
show h225	Displays information for H.225 sessions established across the security appliance.			
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.			
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.			
timeout h225   h323	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.			

# debug http

To display detailed information about HTTP traffic, use the **debug http** command in privileged EXEC mode. To disable debugging, Use the **no** form of this command.

debug http [ level ]

no debug http [ level ]

Syntax Description	level	(Optional) Sets the default is 1. To disp a higher number.										
Defaults	The defafult for <i>level</i>	is 1.										
command Modes	The following table sl	hows the modes in whic	h you can enter	the comma	nd:							
		Firewall N	lode	Security C	ontext							
					Multiple							
	Command Mode	Routed	Transparent	Single	Context	System						
	Privileged EXEC	•	•	•	•							
Command History	Release Modification											
	7.0(1)This command was introduced.											
Usage Guidelines	undebug all comman	mand displays detailed i ds turn off all enabled d	lebugs.			-						
xamples			detailed inform	ation abou	t HTTP traffic	The following example enables the display of detailed information about HTTP traffic:						
	hostname# <b>debug htt</b>	P										
Related Commands	Commands	Description										
Related Commands	<b>Commands</b> http	<b>Description</b> Specifies hosts that appliance.	t can access the	HTTP serve	er internal to th	ne security						
Related Commands		Specifies hosts that		HTTP serve	er internal to t	ne security						
Related Commands	http	Specifies hosts that appliance.	TP proxy server.	HTTP serve	er internal to tl	ne security						

#### debug http-map

To show debug messages for HTTP application inspection maps, use the **debug http-map** command in privileged EXEC mode. To stop showing debug messages for HTTP application inspection, use the **no** form of this command.

debug http-map

no debug http-map

**Defaults** The default value for *level* is 1.

**Command Modes** The following table shows the modes in which you can enter the command:

	Firewall N	Security Context				
			Multiple			
Command Mode	Routed	Transparent	Single	Context	System	
Privileged EXEC	•	•	•	•		

 Release
 Modification

 7.0(1)
 This command was introduced.

#### **Usage Guidelines**

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note

Enabling the debug http-map command may slow down traffic on busy networks.

**Examples** The following example enables debug messages at the default level (1) for HTTP application inspection: hostname# debug http-map

Command	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about HTTP application inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

#### debug icmp

To display detailed information about ICMP inspection, use the **debug icmp** command in privileged EXEC mode. To disable debugging, Use the **no** form of this command.

debug icmp trace [ level ]

no debug icmp trace [ level ]

Syntax Description	trace Displays debug information about ICMP trace activity.							
	level (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.							
efaults	All options are enabled.							
Command Modes	The following table sho	ws the modes in whic	h you can enter	the comma	nd:			
		Firewall M	lode	Security C	ontext			
					Multiple	T		
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
ommand History	Release Modification							
	7.0(1)This command was introduced.							
lsage Guidelines	The <b>debug icmp</b> comma <b>undebug all</b> commands			ut ICMP in	spection. The	no debug all		
xamples	The following example hostname# <b>debug icmp</b>	enables the display of	f detailed inform	nation abou	t ICMP inspec			
	hostname# <b>debug icmp</b>	Description		nation abou	t ICMP inspec			
	hostname# debug icmp Commands clear configure icmp	<b>Description</b> Clears the ICMP co	onfiguration.			tion:		
Examples Related Commands	hostname# <b>debug icmp</b>	Description	onfiguration. rules for ICMP t			tion:		

Commands	Description
show icmp	Displays ICMP configuration.
timeout	Configures idle timeout for ICMP.

## debug igmp

To display IGMP debug information, use the **debug igmp** command in privileged EXEC mode. To stop the display of debug information, use the **no** form of this command.

**debug igmp** [**group** *group\_id* | **interface** *if\_name*]

**no debug igmp** [group group\_id | interface if\_name]

Syntax Description	<b>group</b> <i>group_id</i> Displays IGMP debug information for the specified group.						
	<b>interface</b> <i>if_name</i>	Display IGN	IP debu	g information f	for the spec	cified interface	
Defaults	No default behavior or	values.					
Command Modes	The following table sho	ows the modes i	n which	i you can enter	the comma	und:	
		Fire	wall M	ode	Security (		
	Command Mode	Rou	ted	Transparent	Single	Multiple Context	System
	Privileged EXEC	•			•		
Command History	Release	Modification	1				
ooniniunu motory	Preexisting	This comma		preexisting.			
Usage Guidelines	Because debugging out unusable. For this reaso troubleshooting session during periods of lower likelihood that increase	on, use <b>debug</b> co is with Cisco tec r network traffic	ommane chnical s c and fev	ds only to troub support staff. M wer users. Debu	oleshoot sp loreover, it ugging duri	ecific problematis best to use <b>d</b> ing these period	s or during ebug commands ds decreases the
Examples	The following is sample output from the <b>debug igmp</b> command:						
	IGMP debugging is on IGMP: Received v2 Qua IGMP: Send v2 general IGMP: Received v2 Qua IGMP: Send v2 general IGMP: Received v2 Qua IGMP: Received v2 Qua IGMP: Received v2 Rep IGMP: Updating EXCLUT	l Query on dmz ery on dmz fro l Query on out ery on outside l Query on ins ery on inside port on inside	z om 192. side from 1 from 1 e from 1	168.4.1 192.168.3.1 92.168.1.1 192.168.1.6 fo	or 224.1.1	1	

<b>Related Commands</b>	Command	Description
	show igmp groups	Displays the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP.
	show igmp interface	Displays multicast information for an interface.

## debug ils

To show debug messages for ILS, use the **debug ils** command in privileged EXEC mode. To stop showing debug messages for ILS, use the **no** form of this command.

debug ils [level]

no debug ils [level]

Syntax Description	level	(Optional) Sets the default is 1. To dis a higher number.						
Defaults	The default value for	level is 1.						
Command Modes	The following table s	shows the modes in whic	ch you can enter	the comma	and:			
		Firewall N	lode	Security (	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
			ľ	÷		·		
Command History	Release Modification							
	Preexisting This command was preexisting.							
Usage Guidelines		bug command settings, e ommand. To stop all deb						
Note	Enabling the <b>debug ils</b> command may slow down traffic on busy networks.							
Examples	The following examp hostname# <b>debug il</b>	ple enables debug messa; s	ges at the defaul	t level (1) f	for ILS applica	tion inspection:		
Related Commands	Command	Description						
	class-map	Defines the traffic	class to which to	apply sec	urity actions.			
	inspect ils	Enables ILS applic	ation inspection					

Command	Description
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

# debug imagemgr

To display Image Manager debug information, use the **debug imagemgr** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug imagemgr [level]

no debug imagemgr

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255 default is 1. To display additional messages at higher levels, set the level a higher number.						
Defaults	The default value for <i>leve</i>	<i>l</i> is 1.					
Command Modes	The following table show	s the modes in whic	ch you can enter	the comma	and:		
		Firewall N	Node	Security (	Context		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	
Usage Guidelines	7.0(1) Because debugging output unusable. For this reason, troubleshooting sessions during periods of lower n likelihood that increased	use <b>debug</b> comma with Cisco technical etwork traffic and f	riority in the CP nds only to trout l support staff. M ewer users. Debu	oleshoot sp foreover, it ugging duri	ecific problematis best to use <b>d</b> ing these period	s or during <b>ebug</b> commands	
Examples	The following example en Image Manager debug me hostname# <b>debug imagem</b> e debug imagemgr enable hostname# <b>show debug</b> debug imagemgr enable hostname#	essages are enabled. gr d at level 1		es. The <b>sho</b>	w debug comn	nand reveals that	

Command	Description
show debug	Displays current debug configuration.

#### debug ipsec-over-tcp

To display IPSec-over-TCP debug information, use the **debug ipsec-over-tcp** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug ipsec-over-tcp [level]

no debug ipsec-over-tcp

Syntax Description	level	(Optional) Sets the default is 1. To dis a higher number.	0 0		1 V ·			
Defaults	The default value for <i>leve</i>	<i>l</i> is 1.						
Command Modes	The following table show	s the modes in whic	h you can enter	the comma	ind:			
		Firewall N	lode	Security (	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	•		
Command History	Release Modification							
	7.0(1)     This command was introduced.							
Usage Guidelines	Because debugging outpu unusable. For this reason, troubleshooting sessions v during periods of lower no likelihood that increased o	use <b>debug</b> comma with Cisco technical etwork traffic and f	nds only to troub support staff. M ewer users. Debu	oleshoot sp foreover, it ugging duri	ecific problems is best to use <b>d</b> ng these perio	s or during ebug command		
Examples	The following example er that IPSec-over-TCP debu hostname# <b>debug ipsec-o</b> debug ipsec-over-tcp of hostname# <b>show debug</b> debug ipsec-over-tcp of hostname#	ng messages are ena pver-tcp enabled at level	bled.	ages. The s	how debug co	mmand reveals		

Command	Description
show debug	Displays current debug configuration.

## debug ipsec-pass-thru

To show debug messages for ipsec-pass-thru, use the **debug ipsec-pass-thru** command in privileged EXEC mode. To stop showing debug messages for DNS, use the **no** form of this command.

debug ipsec-pass-thru level

no debug ipsec-pass-thru

Syntax Description	level	(Optional) Sets the default is 1. To dis a higher number.	0 0		1 .			
Defaults	The default level is 1.	If you do not specify a	ny keywords, the	e security a	ppliance show	s all mesages.		
Command Modes	The following table sh	ows the modes in whic	ch you can enter	the comma	ind:			
		Firewall N	Node	Security (	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
Command History	Release Modification							
	7.1This command was introduced.							
Jsage Guidelines	Using <b>debug</b> comman	ds might slow down tra	affic on busy net	works.				
xamples	The following example enables debug messages for DNS:							
	hostname# <b>debug ipsec-pass-thru</b>							
Related Commands	Command	Description						
	inspect ipsec-pass-thru	Enables IPSec pas	s-thru application	n inspectio	n.			

## debug ipv6

To display ipv6 debug messages, use the **debug ipv6** command in privileged EXEC mode. To stop the display of debug messages, use the **no** form of this command.

debug ipv6 {icmp | interface | nd | packet | routing}

no debug ipv6 {icmp | interface | nd | packet | routing}

Syntax Description	icmp		-	ssages for IPv6 transactions.	ICMP trans	sactions, exclu	ding ICMPv6	
	interface	Displays	debug inf	ormation for IPv	6 interface	s.		
	nd	Displays	debug me	ssages for ICMI	Pv6 neighb	or discovery tr	ansactions.	
	packetDisplays debug messages for IPv6 packets.							
	routing	Displays updates.	debug me	ssages for IPv6	routing tab	le updates and	route cache	
Defaults	No default behavio	or or values.						
Command Modes	The following tabl	le shows the mod	les in whic	h you can enter	the comma	nd:		
			Firewall N	lode	Security C	ontext		
						Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	
	Privileged EXEC		•	—	•	•	—	
Command History	Release	Modifica	ation					
	7.0(1)	7.0(1)This command was introduced.						
Usage Guidelines	Because debuggin unusable. For this troubleshooting se during periods of l likelihood that inc	reason, use <b>deb</b> essions with Cisco lower network tr	<b>ig</b> comman o technical affic and fe	nds only to troub support staff. M ewer users. Debu	oleshoot spe oreover, it igging duri	ecific problems is best to use <b>d</b> ng these period	s or during ebug commands	
Examples	hostname# <b>debug</b> 13:28:40:ICMPv6: 13:28:45:ICMPv6: 13:28:50:ICMPv6:	reased <b>debug</b> command processing overhead will affect system use. ample output for the <b>debug ipv6 icmp</b> command: <b>ipv6 icmp</b> Received ICMPv6 packet from 2000:0:0:3::2, type 136 Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135 Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 136 Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135						

<b>Related Commands</b>	Command	Description
	ipv6 icmp	Defines access rules for ICMP messages that terminate on a security appliance interface.
	ipv6 address	Configures an interface with an IPv6 address or addresses.
	ipv6 nd dad attempts	Defines the number of neighbor discovery attempts performed during duplicate address detection.
	ipv6 route	Defines a static entry in the IPv6 routing table.

## debug iua-proxy

To display individual user authentication (IUA) proxy debug information, use the **debug iua-proxy** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug iua-proxy [level]

no debug iua-proxy

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.						
Defaults	The default value for <i>le</i>	<i>vel</i> is 1.					
Command Modes	The following table sho	ows the modes in whic	h you can enter	the comma	ınd:		
		Firewall N	lode	Security (	Context		
				-	Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	
Usage Guidelines	7.0(1) Because debugging out unusable. For this reaso troubleshooting session during periods of lower likelihood that increase	on, use <b>debug</b> comman s with Cisco technical network traffic and for	riority in the CP nds only to trout support staff. M ewer users. Debu	oleshoot sp oreover, it ugging duri	ecific problems is best to use <b>d</b> ng these period	s or during <b>ebug</b> commands	
Examples	The following example IUA-proxy debug mess hostname# <b>debug iua-p</b> debug iua-proxy enal hostname# <b>show debug</b> debug iua-proxy enal hostname#	ages are enabled. proxy pled at level 1	ebug messages. '	The show o	<b>lebug</b> commar	nd reveals that	

Related Commands	Command	Description
	show debug	Displays current debug configuration.

### debug kerberos

To display Kerberos authentication debug information, use the **debug kerberos** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug kerberos [level]

no debug kerberos

Syntax Description         level         (Optional) Sets the debug message level to default is 1. To display additional message a higher number.							
Defaults	The default value for <i>le</i>	evel is 1.					
Command Modes	The following table sho	ows the modes in whic	h you can enter	the comma	ınd:		
		Firewall N	lode	Security (	Context		
					Multiple	1	
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	
Commond Illiotom	Deleges	Madifiantian					
Command History	Release         Modification           7.0(1)         This command was introduced.						
Usage Guidelines	Because debugging out unusable. For this reaso troubleshooting session during periods of lower likelihood that increase	on, use <b>debug</b> command s with Cisco technical r network traffic and for	nds only to troub support staff. M ewer users. Debu	bleshoot sp loreover, it lgging duri	ecific problems is best to use <b>d</b> ng these period	s or during <b>ebug</b> commands	
Examples	The following example Kerberos debug messag hostname# <b>debug kerb</b> debug kerberos enab hostname# <b>show debug</b> debug kerberos enab hostname#	ges are enabled. eros led at level 1	ug messages. Tł	ne show de	bug command	reveals that	

Command	Description
show debug	Displays current debug configuration.

## debug Idap

To display LDAP debug information, use the **debug ldap** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug ldap [level]

no debug ldap

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255 default is 1. To display additional messages at higher levels, set the le a higher number.						
Defaults	The default value for <i>lev</i>	eel is 1.					
Command Modes	The following table show	ws the modes in whic	ch you can enter	the comma	nd:		
		Firewall N	lode	Security C	Context		
			Transparent	Single •	Multiple		
	Command Mode Privileged EXEC	Routed			Context •	System •	
Command History	ReleaseModification7.0(1)This command was introduced.						
Usage Guidelines	Because debugging outp unusable. For this reason troubleshooting sessions during periods of lower likelihood that increased	n, use <b>debug</b> comman with Cisco technical network traffic and for	nds only to troub support staff. M ewer users. Debu	bleshoot spe loreover, it i ugging duri	ecific problems is best to use <b>d</b> ng these period	s or during <b>ebug</b> command	
Examples	The following example of debug messages are enal hostname# <b>debug ldap</b> debug ldap enabled ar hostname# <b>show debug</b> debug ldap enabled ar hostname#	bled. t level 1	messages. The s	show debu	g command rev	veals that LDAI	

Command	Description
show debug	Displays current debug configuration.

### debug mac-address-table

To show debug messages for the MAC address table, use the **debug mac-address-table** command in privileged EXEC mode. To stop showing debug messages for the MAC address table, use the **no** form of this command.

debug mac-address-table [level]

no debug mac-address-table [level]

<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.							
The default level is 1.							
The following table sh	lows the modes in whic	h you can enter	the comma	nd:			
	Firewall N	ode	Security C	ontext			
				Multiple			
Command Mode	Routed	Transparent	Single	Context	System		
Privileged EXEC		•	•	•			
Release Modification							
7.0(1)This command was introduced.							
Using <b>debug</b> command	ds might slow down tra	ffic on busy net	works.				
The following example	e enables debug messag	ges for the MAC	address ta	ble:			
hostname# <b>debug mac-address-table</b>							
noschance debug mac	-address-table						
Command	-address-table Description						
		r dynamic MAC	address en	tries.			
Command mac-address-table	Description	-					
	The default level is 1. The following table sh Command Mode Privileged EXEC Release 7.0(1) Using debug comman The following example	default is 1. To disg a higher number.         The default level is 1.         The following table shows the modes in whice         Firewall M         Command Mode       Routed         Privileged EXEC       —         Release       Modification         7.0(1)       This command was         Using debug commands might slow down training	default is 1. To display additional r         a higher number.         The default level is 1.         The following table shows the modes in which you can enter         Firewall Mode         Command Mode         Privileged EXEC         Privileged EXEC         Addition         7.0(1)         This command was introduced.         Using debug commands might slow down traffic on busy net	default is 1. To display additional messages at a higher number.         The default level is 1.         The following table shows the modes in which you can enter the comma         Firewall Mode       Security C         Command Mode       Routed         Privileged EXEC       -         Release       Modification	default is 1. To display additional messages at higher levels, a higher number.         The default level is 1.         The following table shows the modes in which you can enter the command:         Image: Command Mode       Firewall Mode         Routed       Transparent         Single       Context         Privileged EXEC       —         Image: The command was introduced.       This command was introduced.		

Command	Description
show debug	Shows all enabled debuggers.
show mac-address-table	Shows MAC address table entries.

### debug menu

To display detailed debug information for specific features, use the **debug menu** command in privileged EXEC mode.

debug n	nenu
---------	------

Caution	The <b>debug menu</b> co	ommand should be us	ed only under the su	pervision	of Cisco techni	cal support staf	
Syntax Description	This command should be used only under the supervision of Cisco technical support staff.						
Defaults	No default behavior	r or values.					
Command Modes	The following table	e shows the modes in	which you can enter	the comma	and:		
		Firew	all Mode	Security	Context		
				Single	Multiple		
	Command Mode	Route	d Transparent		Context	System	
	Privileged EXEC	•	•	•	•	•	
Command History	Release	Modification					
•							
	7.0(1)	This command	was introduced.				
Usage Guidelines	Because debugging unusable. For this r troubleshooting ses during periods of lo	This command output is assigned his eason, use <b>debug</b> con sions with Cisco tech ower network traffic a eased <b>debug</b> comman	gh priority in the CP nmands only to trout nical support staff. M nd fewer users. Debu	oleshoot sp loreover, it ugging dur	ecific problem is best to use <b>d</b> ing these perio	s or during <b>ebug</b> commands	
Usage Guidelines Examples	Because debugging unusable. For this r troubleshooting ses during periods of lo likelihood that incre	output is assigned hireason, use <b>debug</b> consions with Cisco tech	gh priority in the CP nmands only to trout nical support staff. M nd fewer users. Debu d processing overhea	bleshoot sp foreover, it ugging dur ad will affe	ecific problem is best to use <b>d</b> ing these perio ect system use.	s or during ebug commands ds decreases the	
	Because debugging unusable. For this r troubleshooting ses during periods of lo likelihood that incre	output is assigned hireason, use <b>debug</b> consions with Cisco tech ower network traffic a	gh priority in the CP nmands only to trout nical support staff. M nd fewer users. Debu d processing overhea	bleshoot sp foreover, it ugging dur ad will affe	ecific problem is best to use <b>d</b> ing these perio ect system use.	s or during ebug commands ds decreases the	

#### debug mfib

To display MFIB debug information, use the **debug mfib** command in privileged EXEC mode. To stop displaying debug information, use the **no** form of this command.

**debug mfib** {**db** | **init** | **mrib** | **pak** | **ps** | **signal**} [group]

no debug mfib {db | init | mrib | pak | ps | signal} [group]

	11	(0	• •	1.1			
Syntax Description	db(Optional) Displays debug information for route database operations.group(Optional) IP address of the multicast group.						
	mrib(Optional) Displays debug information for communication with MRIB.pak(Optional) Displays debug information for packet forwarding operations.						
	pak			-	-		
	ps			debug informa	-		*
	signal	protocols.	isplays	debug informa	tion for MF	IB signaling to	o routing
Command Modes	The following table sh	nows the modes in	n which	you can enter	the comma	nd:	
		Firewall Mode		Security Context			
						Multiple	
	Command Mode	D4	hat	Transparent	Single	Context	System
		Rout	leu	mansparent	0		
	Privileged EXEC	•	leu		•	_	
Command History	. <u></u>						
Command History	Privileged EXEC	•					
Command History Usage Guidelines	Privileged EXEC Release	• Modification This commar utput is assigned H son, use debug co ons with Cisco tecl er network traffic	nd was i high pri- ommand hnical s and fev	ntroduced. ority in the CP ls only to troub upport staff. M wer users. Debu	• U process, leshoot spe oreover, it i lgging durin	it can render the cific problems s best to use <b>de</b> ng these period	ne system s or during e <b>bug</b> command
	Privileged EXEC          Release         7.0(1)         Because debugging ou         unusable. For this reast troubleshooting session         during periods of lower	• Modification This comman This comman atput is assigned H son, use <b>debug</b> co ons with Cisco tech er network traffic sed <b>debug</b> comman	nd was i bigh prio ommand hnical s and fev and proc	ntroduced. ority in the CP s only to troub upport staff. M ver users. Debu cessing overhea	• U process, leshoot spe oreover, it i lgging durin id will affeo	it can render the cific problems s best to use <b>d</b> ang these period ct system use.	ne system s or during e <b>bug</b> command

Related Commands	Command	Description
	show mfib	Displays MFIB forwarding entries and interfaces.

#### debug mgcp

#### debug mgcp

To display detailed information about MGCP application inspection, use the **debug mgcp** command in privileged EXEC mode. To disable debugging, Use the **no** form of this command.

debug mgcp {messages | parser | sessions}

no debug mgcp {messages | parser | sessions}

messages	Displays debug information about MGCP messages.
parser	Displays debug information for parsing MGCP messages.
sessions	Displays debug information about MGCP sessions.

#### **Defaults** All options are enabled.

-

**Command Modes** The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	_

Command History	Release	Modification
	7.0(1)	This command was introduced.

Usage Guidelines The debug mgcp command displays detailed information about mgcp inspection. The no debug all or undebug all commands turn off all enabled debugs.

**Examples** The following example enables the display of detailed information about MGCP application inspection: hostname# debug mgcp

Related Commands	Commands	Description		
	class-map	Defines the traffic class to which to apply security actions.		
	inspect mgcp	Enables MGCP application inspection.		
	mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.		
	show mgcp	Displays information about MGCP sessions established through the security appliance.		
	show conn	Displays the connection state for different connection types.		

# debug module-boot

To show debug messages about the SSM booting process, use the **debug module-boot** command in privileged EXEC mode. To stop showing debug messages for the SSM booting process, use the **no** form of this command.

**debug module-boot** [*level*]

no debug module-boot [level]

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. Th default is 1. To display additional messages at higher levels, set the level t a higher number.								
Defaults	The default level is 1.								
Command Modes	The following table shows the modes in which you can enter the command:								
		Firewall N	lode	Security Context					
				Single	Multiple				
	Command Mode	Routed	Transparent		Context	System			
	Privileged EXEC	•	•	•		•			
Command History	Release Modification								
	7.0(1)     This command was introduced.								
Usage Guidelines Examples	Using <b>debug</b> command								
examples	The following example hostname# <b>debug modu</b>		ges for the SSM	booting pr	ocess:				
Related Commands	Command Description								
	hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.							
	<b>hw-module module</b> Shuts down an SSM and performs a hardware reset. <b>reset</b>								
	hw-module module Reloads the intelligent SSM software.								

Command	Description				
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.				
show module	Shows SSM information.				

#### debug mrib

To display MRIB debug information, use the **debug mrib** command in privileged EXEC mode. To stop the display of debug information, use the **no** form of this command.

**debug mrib** {**client** | **io** | **route** [*group*] | **table**}

**no debug mrib** {**client** | **io** | **route** [*group*] | **table**}

Syntax Description									
eyntax beeenption	client	client Enables debugging for MRIB client management activity.							
	io Enables debugging of MRIB I/O events.								
	route Enables debugging of MRIB routing entry activity.								
	group	Enables	debugging	of MRIB routin	g entry act	ivity for the sp	ecified group.		
	tableEnables debugging of MRIB table management activity.								
Defaults	No default behavior o	or values.							
Command Modes	The following table s	hows the mod	les in whic	h you can enter	the comma	nd:			
			Firewall Mode		Security Context				
						Multiple			
	Command Mode		Routed	Transparent	Single	Context	System		
	Privileged EXEC		•		•				
Command History	Release Modification								
Command History	Kelease	Modifica							
Command History	<b>Release</b> 7.0(1)			introduced.					
Command History				introduced.					
Command History Usage Guidelines		This con utput is assign son, use <b>debu</b> ons with Cisco er network tra	nmand was ned high pr ig commar o technical affic and fe	riority in the CP ids only to troub support staff. M ewer users. Debu	oleshoot spe oreover, it i ugging duri	cific problems s best to use <b>d</b> ng these period	s or during e <b>bug</b> command		
	7.0(1) Because debugging o unusable. For this rea troubleshooting sessio during periods of low	This com utput is assign son, use <b>debu</b> ons with Cisco er network tra sed <b>debug</b> com	nmand was ned high pr g commar o technical affic and fe mmand pro	riority in the CP ids only to troub support staff. M ewer users. Debu ocessing overhea	oleshoot spe oreover, it i agging duri ad will affe	ecific problems s best to use <b>d</b> ng these period ct system use.	s or during e <b>bug</b> command		

Command	Description				
show mrib client	Displays information about the MRIB client connections.				
show mrib route	Displays MRIB table entries.				

### debug ntdomain

To display NT domain authentication debug information, use the **debug ntdomain** command in privileged EXEC mode. To disable the display of NT domain debug information, use the **no** form of this command.

debug ntdomain [level]

no debug ntdomain

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.						
Defaults	The default value for <i>leve</i>	<i>el</i> is 1.					
Command Modes	The following table show	s the modes in whic	h you can enter	the comma	nd:		
		Firewall Mode		Security Context			
				Single •	Multiple		
	Command Mode	Routed	Transparent		Context	System	
	Privileged EXEC	•	•		•	•	
Command History	Release	Modification					
	7.0(1)     This command was introduced.						
Usage Guidelines	Because debugging output unusable. For this reasons troubleshooting sessions during periods of lower n likelihood that increased	, use <b>debug</b> comman with Cisco technical etwork traffic and fo	nds only to troub support staff. M ewer users. Debu	oleshoot spo loreover, it ugging duri	ecific problems is best to use <b>d</b> ng these period	s or during <b>ebug</b> command	
Examples	The following example er domain debug messages a hostname# <b>debug ntdoma</b> debug ntdomain enable hostname# <b>show debug</b> debug ntdomain enable hostname#	are enabled. in d at level 1	ebug messages. T	The show do	e <b>bug</b> command	l reveals that N	
Related Commands	Command	Description					
------------------	------------	---------------------------------------					
	show debug	Displays current debug configuration.					

#### debug ntp

To show debug messages for NTP, use the **debug ntp** command in privileged EXEC mode. To stop showing debug messages for NTP, use the **no** form of this command.

debug ntp {adjust | authentication | events | loopfilter | packets | params | select | sync | validity }

no debug ntp {adjust | authentication | events | loopfilter | packets | params | select | sync | validity}

Syntax Description	adjust	Shows	messages a	bout NTP clock a	adjustment	s.	
	authentication	Shows	messages a	bout NTP authen	tication.		
	eventsShows messages about NTP events.loopfilterShows messages about NTP loop filter.						
	packetsShows messages about NTP packets.						
	params	Shows	messages a	bout NTP clock	parameters		
	select	Shows	messages a	bout NTP clock	selection.		
	sync	Shows	messages a	bout NTP clock s	synchroniz	ation.	
	validity	Shows	messages a	bout NTP peer cl	ock validit	y.	
Defaults	No default behavior o	or values.					
Command Modes	The following table sl	hows the mo	odes in whic	ch you can enter	the comma	.nd:	
				-			
			Firewall N	Node	Security (	Context	
				Node	Security (	context Multiple	
	Command Mode			Node Transparent	Security ( Single		System
	<b>Command Mode</b> Privileged EXEC		Firewall N			Multiple	System —
Command History	Privileged EXEC	Modifie	Firewall N Routed •	Transparent	Single	Multiple Context	System —
Command History	Privileged EXEC Release	Modific This so	Firewall N Routed •	Transparent •	Single	Multiple Context	System —
Command History	Privileged EXEC		Firewall N Routed •	Transparent	Single	Multiple Context	System —
Command History	Privileged EXEC Release		Firewall N Routed •	Transparent •	Single	Multiple Context	System —
	Privileged EXEC Release Preexisting	This co	Firewall N Routed • cation	s preexisting.	Single •	Multiple Context	System —
Command History Usage Guidelines	Privileged EXEC Release	This co	Firewall N Routed • cation	s preexisting.	Single •	Multiple Context	System 
	Privileged EXEC Release Preexisting	This co	Firewall N Routed • cation	s preexisting.	Single •	Multiple Context	System —
	Privileged EXEC Release Preexisting	This co	Firewall M Routed • cation mmand was	s preexisting.	Single •	Multiple Context	System 
Usage Guidelines	Privileged EXEC Release Preexisting Using debug comman	This co nds might slo le enables do	Firewall M Routed • cation mmand was	s preexisting.	Single •	Multiple Context	System 

#### Related Commands C

Command	Description
ntp authenticateEnables NTP authentication.	
ntp server	Identifies an NTP server.
show debug Shows all enabled debuggers.	
show ntp associations	Shows the NTP servers with which the security appliance is associated.
show ntp status	Shows the status of the NTP association.

### debug ospf

To display debug information about the OSPF routing processes, use the **debug ospf** command in privileged EXEC mode.

debug ospf [adj | database-timer | events | flood | lsa-generation | packet | retransmission | spf [external | inter | intra] | tree]

no debug ospf [adj | database-timer | events | flood | lsa-generation | packet | retransmission | spf [external | inter | intra] | tree]

Command Modes	The following table sl Command Mode Privileged EXEC	hows the modes in white Firewall I Routed	-	Security C		System		
Command Modes		Firewall I	Mode	Security C	Context Multiple	System		
Command Modes	The following table s		-		Context			
Command Modes	The following table s		-					
Command Modes	The following table s	hows the modes in whi	ch you can enter	the comma	nd:			
Defaults	Displays all OSPF de	bug information if no k	eyword is provid	led.				
	tree	tree       (Optional) Enables the debugging of OSPF database events.						
		You can limit the SPF debug information by using the <b>external</b> , <b>inter</b> , and <b>intra</b> keywords.						
	spf	(Optional) Enable						
	retransmission	(Optional) Enable	66 6					
	packet	(Optional) Enable	s the debugging o	of received	OSPF packets			
	lsa-generation	(Optional) Enable	s the debugging o	of OSPF su	mmary LSA ge	eneration.		
	intra	(Optional) Limits	SPF debugging t	o intra-area	events.			
	inter	ood     (Optional) Enables the debugging of OSPF flooding.						
	flood							
	external							
	database-timer events	(Optional) Enable	66 6					
		(Onfional) Enable	s the debugging of	of OSPF tir	ner events			

# Usage GuidelinesBecause debugging output is assigned high priority in the CPU process, it can render the system<br/>unusable. For this reason, use debug commands only to troubleshoot specific problems or during<br/>troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands<br/>during periods of lower network traffic and fewer users. Debugging during these periods decreases the<br/>likelihood that increased debug command processing overhead will affect system use.

Examples	The following is sample output from the <b>debug ospf events</b> command:				
	hostname# <b>debug ospf events</b> ospf event debugging is on				
	OSPF:hello with invalid timers on interface Ethernet0 hello interval received 10 configured 10				

hello interval received 10 configured 10 net mask received 255.255.0 configured 255.255.0 dead interval received 40 configured 30

<b>Related Commands</b>	Command	Description
	show ospf	Displays general information about the OSPF routing process.

#### debug parser cache

To display CLI parser debug information, use the **debug parser cache** command in privileged EXEC mode. To disable the display of CLI parser debug information, use the **no** form of this command.

debug parser cache [level]

no debug parser cache

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.						
Defaults	The default value for	t level is 1.					
Command Modes	The following table	shows the modes in whic	ch you can enter	the comma	ind:		
		Firewall N	Node	Security (	Context		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	
Command History	Release     Modification       7.0(1)     This command was introduced.						
Usage Guidelines	unusable. For this re troubleshooting sess during periods of low	output is assigned high p ason, use <b>debug</b> comma ions with Cisco technical wer network traffic and f ased <b>debug</b> command pr	nds only to troub l support staff. M ewer users. Debu	bleshoot sp loreover, it ugging duri	ecific problems is best to use <b>d</b> ing these perio	s or during ebug commands	
Examples	current debug config show debug comma hostname# debug pa debug parser cache hostname# show deb parser cache: try	rser cache e enabled at level 1 vug to match 'show debug' e enabled at level 1	debug messages				

Related Commands	Command	Description
	show debug	Displays current debug configuration.

### debug pim

To display PI M debug information, use the **debug pim** command in privileged EXEC mode. To stop displaying debug information, use the **no** form of this command.

**debug pim** [**df-election** [**interface** *if\_name* | **rp** *rp*] | **group** *group* | **interface** *if\_name* | **neighbor**]

**no debug pim** [**df-election** [**interface** *if\_name* | **rp** *rp*] | **group** *group* | **interface** *if\_name* | **neighbor**]

df-election	(Optional) Displays debug messages for PIM bidirectional DF-election message processing.				
group group	(Optional) Displays debug information for the specified group. The value for <i>group</i> can be one of the following:				
	• Name of the multicast group, as defined in the DNS hosts table or with the domain <b>ipv4 host</b> command.				
	• IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.				
<b>interface</b> <i>if_name</i>	(Optional) When used with the <b>df-election</b> keyword, it limits the DF election debug display to information for the specified interface.				
	When used without the <b>df-election</b> keyword, displays PIM error messages for the specified interface.				
	<b>Note</b> The <b>debug pim interface</b> command does not display PIM protocol activity messages; it only displays error messages. To see debug information for PIM protocol activity, use the <b>debug pim</b> command without the <b>interface</b> keyword. You can use the <b>group</b> keyword to limit the display to the specified multicast group.				
neighbor	(Optional) Displays only the sent/received PIM hello messages.				
<b>rp</b> <i>rp</i>	(Optional) Can be either one of the following:				
	• Name of the RP, as defined in the Domain Name System (DNS) hosts table or with the domain <b>ipv4 host</b> command.				
	• IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.				
	group group interface if_name neighbor				

#### **Defaults** No default behavior or values.

#### **Command Modes** The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History	Release	Modification				
	7.0(1)	This command was introduced.				
Usage Guidelines	Logs PIM packets	received and transmitted and also PIM-related events.				
	unusable. For this troubleshooting se during periods of l	g output is assigned high priority in the CPU process, it can render the system reason, use <b>debug</b> commands only to troubleshoot specific problems or during ssions with Cisco technical support staff. Moreover, it is best to use <b>debug</b> commands lower network traffic and fewer users. Debugging during these periods decreases the reased <b>debug</b> command processing overhead will affect system use.				
Examples	The following is s	ample output from the <b>debug pim</b> command:				
	hostname# <b>debug</b>	-				
		in/Prune on Ethernet1 from 172.24.37.33				
	PIM: Received Join/Prune on Ethernet1 from 172.24.37.33					
	PIM: Received Join/Prune on Tunnel0 from 10.3.84.1 PIM: Received Join/Prune on Ethernet1 from 172.24.37.33					
	PIM: Received Join/Prune on Ethernet1 from 172.24.37.33					
	PIM: Received RP	-Reachable on Ethernet1 from 172.16.20.31				
	PIM: Update RP e	xpiration timer for 224.2.0.1				
		reachability packet for 224.2.0.1 on Tunnel0				
		in/Prune on Ethernet1 from 172.24.37.33				
		(10.221.196.51/32, 224.2.0.1)				
		lay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Ethernet1				
		in/Prune on Ethernet1 from 172.24.37.6 in/Prune on Ethernet1 from 172.24.37.33				
		in/Prune on Tunnel0 from 10.3.84.1				
		(*, 224.2.0.1) RP 172.16.20.31				
		to (*, 224.2.0.1), Forward state				
		(10.0.0/8, 224.2.0.1)				
	PIM: Add Tunnel0	to (10.0.0.0/8, 224.2.0.1), Forward state				
	PIM: Join-list:	(10.4.0.0/16, 224.2.0.1)				
		(172.24.84.16/28, 224.2.0.1) RP-bit set RP 172.24.84.16				
		on Ethernet1 to 172.24.37.6 for (172.24.84.16/28, 224.2.0.1), RP				
		ne-list: 10.9.0.0/16				
		ne-list: 10.16.0.0/16				
		ne-list: 10.49.0.0/16 ne-list: 10.84.0.0/16				
		ne-list: 10.146.0.0/16				
		.1, Join-list: 172.24.84.16/28				
		lic Join/Prune to RP via 172.24.37.6 (Ethernet1)				

<b>Related Commands</b>	Command	Description
	show pim group-map	Displays group-to-protocol mapping table.
	show pim interface	Displays interface-specific information for PIM.
	show pim neighbor	Displays entries in the PIM neighbor table.

#### debug pix pkt2pc

To show debug messages that trace packets sent to the uauth code and that trace the event where the uauth proxy session is cut through to the data path, use the **debug pix pkt2pc** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix pkt2pc

no debug pix pkt2pc

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** The following table shows the modes in which you can enter the command:

	Firewall M	Firewall Mode Security Co		ontext	itext	
Command Mode				Multiple		
	Routed	Transparent	Single	Context	System	
Privileged EXEC	•	•	•	•	•	

Command History	Release	Modification
	Preexisting	This command was preexisting.

**Usage Guidelines** Using **debug** commands might slow down traffic on busy networks.

**Examples** The following example enables debug messages that trace packets sent to the uauth code and that trace the event where the uauth proxy session is cut through to the data path: hostname# debug pix pkt2pc

## Commands Command Description debug pix process Shows debug messages for xlate and secondary connections processing. show debug Shows all enabled debuggers.

### debug pix process

To show debug messages for xlate and secondary connections processing, use the **debug pix process** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix process

no debug pix process

Syntax Description This con	nmand has no	o arguments or	keywords.
-----------------------------	--------------	----------------	-----------

**Defaults** No default behavior or values.

**Command Modes** The following table shows the modes in which you can enter the command:

	Firewall N	Firewall Mode		Security Context		
				Multiple		
Command Mode	Routed	Transparent	Single	Context	System	
Privileged EXEC	•	•	•	•	•	

Command History	Release	Modification
	Preexisting	This command was preexisting.

**Usage Guidelines** Using **debug** commands might slow down traffic on busy networks.

**Examples** The following example enables debug messages for xlate and secondary connections processing: hostname# debug pix process

Related Commands	Command	Description
	debug pix pkt2pc	Shows debug messages that trace packets sent to the uauth code and that trace the event where the uauth proxy session is cut through to the data path.
	show debug	Shows all enabled debuggers.

## debug pptp

To show debug messages for PPTP, use the **debug pptp** command in privileged EXEC mode. To stop showing debug messages for PPTP, use the **no** form of this command.

debug pptp [level]

no debug pptp [level]

Syntax Description	level	(Optional) Sets the default is 1. To disp a higher number.	0 0		1 .			
Defaults	The default value for	level is 1.						
Command Modes	The following table sh	nows the modes in whic	h you can enter	the comma	nd:			
		Firewall N	lode	Security (	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
Command History	Release Modification							
-	Preexisting	This command was	preexisting.					
Usage Guidelines		ug command settings, e mmand. To stop all deb						
Usage Guidelines <u>Note</u>	enter the <b>no debug</b> co command.		ug messages from	m being dis	splayed, enter t			
Usage Guidelines <u>Note</u> Examples	enter the <b>no debug</b> co command. Enabling the <b>debug p</b>	mmand. To stop all deb <b>ptp</b> command may slov e enables debug messag	ug messages from v down traffic o	m being dis n busy netw	splayed, enter t vorks.	he no debug al		
Note	enter the <b>no debug</b> co command. Enabling the <b>debug p</b> The following example	mmand. To stop all deb <b>ptp</b> command may slov e enables debug messag	ug messages from v down traffic o	m being dis n busy netw	splayed, enter t vorks.	he no debug al		

Enables PPTP application inspection.

inspect pptp

Command	Description
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

### debug radius

To show debug messages for AAA, use the **debug radius** command in privileged EXEC mode. To stop showing RADIUS messages, use the **no** form of this command.

debug radius [ all | decode | session | user username ] ]

no debug radius

Syntax Description	all	· •	(Optional) Show RADIUS debugging messages for all users and sessions, including decoded RADIUS messages.					
	decode	(Optional) Show decoded content of RADIUS messages. Content of all						
		RADIUS packets display, including hexadecimal values and the decoded, eye-readable versions of these values.						
	session	(Optional) Show session-related RADIUS messages. Packet types for sent and received RADIUS messages display but not the packet content.						
	user	(Optional) Show RADIUS debugging messages for a specific user.						
	username	Specifies the second of the second se		whose messages	you want t	o see. Valid wi	ith the <b>user</b>	
Defaults	No default behavior	or values.						
Command Modes	The following table	shows the modes	in which	h vou can enter	the commo	nd		
Commanu Moues	The following table	shows the modes		ii you can enter	the comma	liu.		
		Fi	Firewall Mode S			Security Context		
						Multiple		
	<b>Command Mode</b>	Ro	outed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	•	
Command History	Release	Modificatio	on					
	Preexisting	This comm	nand was	preexisting.				
Usage Guidelines	The <b>debug radius</b> of security appliance a enabled debugs.							
Examples	The following exam	ple shows decode	ed RADI	US messages, w	hich happe	en to be accour	nting packets:	
	hostname(config)# hostname(config)#			accounting red	quest)			

```
Raw packet data (length = 216).....
i
Parsed packet data....
Radius: Code = 4 (0x04)
Radius: Identifier = 105 (0x69)
Radius: Length = 216 (0x00D8)
Radius: Vector: 842E0E99F44C00C05A0A19AB88A81312
Radius: Type = 40 (0x28) Acct-Status-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.1.1.1 (0x0A010101)
Radius: Type = 14 (0x0E) Login-IP-Host
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.2.0.50 (0xD0FE1291)
Radius: Type = 16 (0x10) Login-TCP-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x50
Radius: Type = 44 (0x2C) Acct-Session-Id
Radius: Length = 12 (0x0C)
Radius: Value (String) =
30\ 78\ 31\ 33\ 30\ 31\ 32\ 39\ 66\ 65
                                                    0x130129fe
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
62 72 6f 77 73 65 72
                                                    browser
Radius: Type = 46 (0x2E) Acct-Session-Time
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 42 (0x2A) Acct-Input-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x256D
Radius: Type = 43 (0x2B) Acct-Output-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x3E1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x0000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e
                                                    ip:source-ip=10.
31 2e 31 2e 31 30
                                                       1.1.10
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 27 (0x1B)
Radius: Vendor ID = 9 (0x0000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 21 (0x15)
Radius: Value (String) =
69\ 70\ 3a\ 73\ 6f\ 75\ 72\ 63\ 65\ 2d\ 70\ 6f\ 72\ 74\ 3d\ 33
                                                    ip:source-port=3
34 31 33
                                                       413
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 40 (0x28)
Radius: Vendor ID = 9 (0x0000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 34 (0x22)
Radius: Value (String) =
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 69
                                                    | ip:destination-i
70 3d 32 30 38 2e 32 35 34 2e 31 38 2e 31 34 35
                                                    p=10.2.0.50
Radius: Type = 26 (0x1A) Vendor-Specific
```

Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x0000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 70 | ip:destination-p
6f 72 74 3d 38 30 | ort=80

<b>Related Commands</b>	Command	Description
	show running-config	Displays the configuration that is running on the security appliance.

debug rip

To display debug information for RIP, use the **debug rip** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug rip

no debug rip

Syntax Description	This command	has no arguments	or keywords.
--------------------	--------------	------------------	--------------

**Defaults** No default behavior or values.

**Command Modes** The following table shows the modes in which you can enter the command:

	Firewall N	Firewall Mode Security Context			xt	
			Transparent Single	Multiple		
Command Mode	Routed	Transparent		Context	System	
Privileged EXEC	•		•		_	

<b>Command History</b>	Release	Modification
	Preexisting	This command was preexisting.

**Usage Guidelines** Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

**Examples** The following example enables level 1 debugging of RIP: hostname# **debug rip** debug rip enabled at level 1

hostname#

Related Commands	Command	Description
	clear configure rip	Clears all RIP commands from the running configuration.

Command	Description
rip	Configures RIP on the specified interface.
show running-config rip	Displays the RIP commands in the running configuration.

## debug rtsp

To show debug messages for RTSP application inspection, use the **debug rtsp** command in privileged EXEC mode. To stop showing debug messages for RTSP application inspection, use the **no** form of this command.

debug rtsp [level]

no debug rtsp [level]

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.						
Defaults	The default value for <i>leve</i>	<i>el</i> is 1.					
Command Modes	The following table show	vs the modes in whic	h you can enter	the comma	und:		
		Firewall N	lode	Security (	Context		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•		
Command History	<b>Release</b> Preexisting	<b>Modification</b> This command was	s preexisting.				
Jsage Guidelines	To see the current debug enter the <b>no debug</b> comm command.						
	Enabling the <b>debug rtsp</b> command may slow down traffic on busy networks.						
Note	Enabling the <b>debug rtsp</b>		v down traine of	i busy netw	/01KS.		
Examples	The following example example	nables debug messag	ges at the default	level (1) fo	or RTSP applic	ation inspection	
	hostname# <b>debug rtsp</b>						

#### **Related Commands**

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect rtsp	Enables RTSP application inspection.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

#### debug sdi

To display SDI authentication debug information, use the **debug sdi** command in privileged EXEC mode. To disable the display of SDI debug information, use the **no** form of this command.

debug sdi [level]

no debug sdi

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.						
Defaults	The default value for	or <i>level</i> is 1.					
Command Modes	The following table	e shows the modes in whi	ch you can enter	the comma	nd:		
		Firewall I	Vode	Security (	ontext		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	
ommand History	Release Modification						
	7.0(1)This command was introduced.						
Jsage Guidelines	unusable. For this r troubleshooting ses during periods of lo	output is assigned high p eason, use <b>debug</b> comma sions with Cisco technica ower network traffic and p eased <b>debug</b> command p	inds only to troub l support staff. M fewer users. Debu	oleshoot spo oreover, it igging duri	ecific problems is best to use <b>d</b> ng these period	s or during e <b>bug</b> command	

#### **Related Commands**

Command	Description
show debug	Displays current debug configuration.

#### debug sequence

To add a sequence number to the beginning of all debug messages, use the **debug sequence** command in privileged EXEC mode. To disable the use of debug sequence numbers, use the **no** form of this command.

debug sequence [level]

no debug sequence

Syntax Description	level		o display ad	-			1 and 255. The , set the level to
Defaults	The defaults are as	follows:					
	• Debug messag	e sequence numbers a	re disabled				
	• The default va	lue for <i>level</i> is 1.					
Command Modes	The following tabl	e shows the modes in	which you	can enter	the comm	and:	
		Firew	all Mode		Security	Context	
					Single	Multiple	
	Command Mode	Route	d Tra	nsparent		Context	System
	Privileged EXEC	•	•		•	•	•
Command History	Release	Modification					
	7.0(1)	This command	l was introd	luced.			
Usage Guidelines	unusable. For this troubleshooting set during periods of 1	g output is assigned hi reason, use <b>debug</b> cor ssions with Cisco tech ower network traffic a reased <b>debug</b> commar	nmands onl nical support nd fewer us	y to troul rt staff. M sers. Deb	oleshoot sp loreover, it ugging dur	ecific problem is best to use <b>c</b> ing these perio	ns or during <b>lebug</b> commands ods decreases the
Examples	command enables configuration. The hostname# <b>debug</b>	enabled at level 1 parser cache	sages. The ssages show	show del	oug comma	and reveals the	e current debug

hostname# show debug
0: parser cache: try to match 'show debug' in exec mode
debug parser cache enabled at level 1
debug sequence enabled at level 1
1: parser cache: hit at index 8
hostname#

<b>Related Commands</b>	Command	Description
	show debug	Displays current debug configuration.

## debug session-command

To show debug messages for a session to an SSM, use the **debug session-command** command in privileged EXEC mode. To stop showing debug messages for sessions, use the **no** form of this command.

debug session-command [level]

no debug session-command [level]

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.					
Defaults	The default level is	s 1.				
Command Modes	The following tabl	le shows the modes in whic	h you can enter	the comma	ınd:	
		Firewall N	lode	Security (	Context	
		Devite d		o	Multiple	
	<b>Command Mode</b> Privileged EXEC	Routed •	Transparent •	•	Context	System •
ommand History	<b>Release</b> 7.0(1)	<b>Modification</b> This command was	s introduced.			
sage Guidelines	Using <b>debug</b> com	mands might slow down tra	uffic on busy net	works.		
kamples	The following examination the following examination of the second	mple enables debug messag	ges for sessions:			
Related Commands	Command	Description				

### debug sip

To show debug messages for SIP application inspection, use the **debug sip** command in privileged EXEC mode. To stop showing debug messages for SIP application inspection, use the **no** form of this command.

debug sip [level]

no debug sip [level]

Syntax Description	level	(Optional) Sets the default is 1. To dis a higher number.						
Defaults	The default value for	level is 1.						
Command Modes	The following table sh	nows the modes in whic	ch you can enter	the comma	ind:			
		Firewall N	lode	Security C	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
Command History	Release Modification							
	Preexisting							
Usage Guidelines		ug command settings, e mmand. To stop all deb		-	-			
<u>Note</u>								
Note	Enabling the <b>debug si</b>	<b>p</b> command may slow	down traffic on	busy netwo	orks.			
		e enables debug messa				tion inspection		
Examples	The following exampl	e enables debug messa				tion inspection		
Examples Related Commands	The following exampl hostname# debug sip	e enables debug messa	ges at the defaul	t level (1) f	for SIP applica	tion inspection		

Command	Description
show conn	Displays the connection state for different connection types.
show sip	Displays information about SIP sessions established through the security appliance.
timeout	Sets the maximum idle time duration for different protocols and session types.

#### debug skinny

To show debug messages for SCCP (Skinny) application inspection, use the **debug skinny** command in privileged EXEC mode. To stop showing debug messages for SCCP application inspection, use the **no** form of this command.

debug skinny [level]

no debug skinny [level]

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 25 default is 1. To display additional messages at higher levels, set the lean higher number.							
Defaults	The default value for	level is 1.						
Command Modes	The following table s	hows the modes in whic	ch you can enter	the comma	ind:			
		Firewall N	lode	Security (	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	—		
Command History	Release	Modification						
	Preexisting	Preexisting This command was preexisting.						
Usage Guidelines		oug command settings, e ommand. To stop all deb						
Note	Enabling the <b>debug s</b>	<b>kinny</b> command may s	low down traffic	on busy no	etworks.			
Examples	The following exampl hostname# <b>debug ski</b>	le enables debug messag nny	ges at the default	level (1) fo	or SCCP applic	ation inspectio		
Related Commands								

Command	Description			
<b>class-map</b> Defines the traffic class to which to apply security actions.				
inspect skinny	Enables SCCP application inspection.			
show skinny	Displays information about SCCP sessions established through the security appliance.			
show conn	Displays the connection state for different connection types.			
timeout	Sets the maximum idle time duration for different protocols and session types.			

## debug smtp

To show debug messages for SMTP/ESMTP application inspection, use the **debug smtp** command in privileged EXEC mode. To stop showing debug messages for SMTP/ESMTP application inspection, use the **no** form of this command.

debug smtp [level]

no debug smtp [level]

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. default is 1. To display additional messages at higher levels, set the leve a higher number.						
Defaults	The default value for	level is 1.					
Command Modes	The following table s	shows the modes in whic	h you can enter	the comma	nd:		
		Firewall N	lode	Security (	Context		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	—	
command History	Release Modification						
	Preexisting This command was preexisting.						
Jsage Guidelines		bug command settings, e ommand. To stop all deb					
Note	Enabling the <b>debug</b> s	smtp command may slo	w down traffic o	on busy net	works.		
Examples	The following examp inspection:	ole enables debug messa	ges at the defaul	t level (1) f	for SMTP/ESM	ITP applicatio	
Examples	• 1	-	ges at the defaul	t level (1) f	for SMTP/ESM	ITP applicatio	
	inspection:	-	ges at the defaul	t level (1) f	for SMTP/ESM	ITP applicatio	

Command	Description			
class-map	Defines the traffic class to which to apply security actions.			
inspect esmtp	Enables ESMTP application inspection.			
policy-map	Associates a class map with specific security actions.			
service-policy	Applies a policy map to one or more interfaces.			
show conn	Displays the connection state for different connection types, including SMTP.			

#### debug sqlnet

To show debug messages for SQL\*Net application inspection, use the **debug sqlnet** command in privileged EXEC mode. To stop showing debug messages for SQL\*Net application inspection, use the **no** form of this command.

debug sqlnet [level]

no debug sqlnet [level]

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. T default is 1. To display additional messages at higher levels, set the level a higher number.							
Defaults	The default value for	level is 1.						
Command Modes	The following table s	hows the modes in whic	h you can enter	the comma	ind:			
		Firewall N	lode	Security (	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
Command History	Release	Modification						
	Preexisting This command was preexisting.							
Usage Guidelines		bug command settings, e ommand. To stop all deb						
Note	Enabling the <b>debug sqlnet</b> command may slow down traffic on busy networks.							
Examples	The following exampling inspection:	le enables debug messag	ges at the defaul	t level (1) f	for SQL*Net aj	oplication		

Command	Description			
class-map	Defines the traffic class to which to apply security actions.			
inspect sqlnet	Enables SQL*Net application inspection.			
policy-map	Associates a class map with specific security actions.			
service-policy	Applies a policy map to one or more interfaces.			
show conn	Displays the connection state for different connection types, including SQL*Net.			

#### debug ssh

To display debug information and error messages associated with SSH, use the **debug ssh** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug ssh [level]

no debug ssh [level]

Syntax Description	n <i>level</i> (Optional) Specifies an optional level of debug.						
Defaults	The default <i>level</i> is 1.						
Command Modes	The following table sho	ows the modes in wh	nich you can enter	the comma	und:		
		Firewall	Mode	Security (	Context		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•		
Command History	Release	Modification					
•	Preexisting	This command w	as preexisting.				
Usage Guidelines	Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use <b>debug</b> commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use <b>debug</b> commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased <b>debug</b> command processing overhead will affect system use.						
Examples	The following is sample	e output from the <b>d</b> e	ebug ssh 255 com	mand:			
	hostname# debug ssh : debug ssh enabled at SSH2 0: send: len 64 SSH2 0: done calc MAG SSH2 0: done calc MAG SSH2 0: done calc MAG SSH2 0: done calc MAG SSH2 0: send: len 32 SSH2 0: done calc MAG SSH2 0: send: len 64 SSH2 0: done calc MAG SSH2 0: send: len 64	255 t level 255 (includes padlen C out #239 (includes padlen C out #240 (includes padlen C out #241 (includes padlen C out #242 (includes padlen C out #243	17) 7) 15) 16) 7)				

SSH2 0: send: len 64 (includes padlen 8) SSH2 0: done calc MAC out #245 SSH2 0: send: len 64 (includes padlen 18) SSH2 0: done calc MAC out #246 SSH2 0: send: len 64 (includes padlen 7) SSH2 0: done calc MAC out #247 SSH2 0: send: len 64 (includes padlen 18) SSH2 0: done calc MAC out #248 SSH2 0: send: len 64 (includes padlen 7) SSH2 0: done calc MAC out #249 SSH2 0: send: len 64 (includes padlen 18) SSH2 0: done calc MAC out #250 SSH2 0: send: len 64 (includes padlen 8) SSH2 0: done calc MAC out #251 SSH2 0: send: len 64 (includes padlen 18) SSH2 0: done calc MAC out #252 SSH2 0: send: len 64 (includes padlen 7) SSH2 0: done calc MAC out #253 SSH2 0: send: len 64 (includes padlen 18) SSH2 0: done calc MAC out #254SSH2 0: send: len 64 (includes padlen 8) SSH2 0: done calc MAC out #255 SSH2 0: send: len 64 (includes padlen 18) SSH2 0: done calc MAC out #256 SSH2 0: send: len 64 (includes padlen 7) SSH2 0: done calc MAC out #257SSH2 0: send: len 64 (includes padlen 18) SSH2 0: done calc MAC out #258

Related Commands	Command	Description
	clear configure ssh	Clears all SSH commands from the running configuration.
	show running-config ssh	Displays the current SSH commands in the running configuration.
	show ssh sessions	Displays information about active SSH sessions to the security appliance.
	ssh	Allows SSH connectivity to the security appliance from the specified client or network.

#### debug ssl

To display SSL debug information, use the **debug ssl** command in privileged EXEC mode. To disable the display of SSL debug information, use the **no** form of this command.

**debug ssl** {**cipher** | **device**} [*level*]

no debug ssl {cipher | device}

Syntax Description	cipher	Display information about the cipher negotiation between the HTTP server and the client.						
	device	Displays information about the SSL device including session initiation and ongoing status.						
	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.							
Defaults	The default value for	for <i>level</i> is 1.						
Command Modes	The following table	e shows the m	odes in whic	h you can enter	the comma	nd:		
			Firewall M	ode	Security C	Context		
						Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	
	Privileged EXEC		•	—	•	—	—	
Command History	Release Modification							
	Preexisting This command was preexisting.							
Usage Guidelines	unusable. For this r troubleshooting ses during periods of lo	ng output is assigned high priority in the CPU process, it can render the system s reason, use <b>debug</b> commands only to troubleshoot specific problems or during essions with Cisco technical support staff. Moreover, it is best to use <b>debug</b> comman lower network traffic and fewer users. Debugging during these periods decreases the creased <b>debug</b> command processing overhead will affect system use.						
Examples	debug command re hostname# debug s debug ssl cipher hostname# show de	enabled at level 1						
# Related Commands Command Description show debug Displays current debug configuration.

### debug sunrpc

To show debug messages for RPC application inspection, use the **debug sunrpc** command in privileged EXEC mode. To stop showing debug messages for RPC application inspection, use the **no** form of this command.

debug sunrpc [level]

**no debug sunrpc** [*level*]

Syntax Description	level	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.						
Defaults	The default value for	level is 1.						
Command Modes	The following table s	shows the modes in whic	ch you can enter	the comma	und:			
		Firewall N	Node	Security (	Context			
					Multiple	·		
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
Command History	Release Modification							
	Preexisting This command was preexisting.							
Usage Guidelines		bug command settings, e ommand. To stop all deb						
<u>Note</u>	Enabling the <b>debug</b>	sunrpc command may s	low down traffic	c on busy n	etworks.			
Examples	The following examp hostname# <b>debug su</b>	ble enables debug messa nrpc	ges at the defaul	t level (1) f	for RPC applic	ation inspectio		
Related Commands								

Command	Description				
class-map	Defines the traffic class to which to apply security actions.				
inspect sunrpc	Enables Sun RPC application inspection.				
policy-map	Associates a class map with specific security actions.				
show conn	Displays the connection state for different connection types, including RPC.				
timeout	Sets the maximum idle time duration for different protocols and session types.				

## debug tacacs

To display TACACS+ debug information, use the **debug tacacs** command in privileged EXEC mode. To disable the display of TACACS+ debug information, use the **no** form of this command.

debug tacacs [session | user username]

no debug tacacs [session | user username]

Syntax Description	session Displays session-related TACACS+ debug messages.							
	<b>user</b> Displays user-specific TACACS+ debug messages. You can display TACACS+ debug messages for only one user at a time.							
	TACACS+ debug messages for only one user at a time.         username       Specifies the user whose TACACS+ debug messages you want to view.							
	username	Specifies the user v	vnose IACACS-	+ debug me	essages you wa	int to view.		
Defaults	No default behavior or	values.						
Command Modes	The following table sh	ows the modes in whic	h you can enter	the comma	ind:			
		Firewall N	lode	Security (	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	•		
Command History	Release Modification							
	7.0(1)     This command was introduced.							
Usage Guidelines	Because debugging ou unusable. For this reas troubleshooting session	on, use <b>debug</b> commar	nds only to troub	leshoot sp	ecific problem	•		
	during periods of lowe likelihood that increase		ewer users. Debu	igging duri	ng these perio	ebug commands		
Examples	e i	ed <b>debug</b> command pro e enables TACACS+ de ages are enabled.	ewer users. Debu ocessing overhea	igging duri ad will affe	ng these perio ct system use.	ebug commands ds decreases the		

Related Commands	Command	Description
	show debug	Displays current debug configuration.

### debug tcp-map

To show debug messages for TCP application inspection maps, use the **debug tcp-map** command in privileged EXEC mode. To stop showing debug messages for TCP application inspection, use the **no** form of this command.

debug tcp-map

no debug tcp-map

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History	Release	Modification
	7.0(1)	This command was introduced.

Usage GuidelinesBecause debugging output is assigned high priority in the CPU process, it can render the system<br/>unusable. For this reason, use debug commands only to troubleshoot specific problems or during<br/>troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands<br/>during periods of lower network traffic and fewer users. Debugging during these periods decreases the<br/>likelihood that increased debug command processing overhead will affect system use.

Examples

The following example enables debug messages for TCP application inspection maps. The **show debug** command reveals that debug messages for TCP application inspection maps are enabled.

hostname# debug tcp-map
debug tcp-map enabled at level 1.
hostname# show debug
debug tcp-map enabled at level 1.
hostname#

### **Related Commands**

Command	Description
show debug	Displays current debug configuration.

## debug timestamps

To add timestamp information to the beginning of all debug messages, use the **debug timestamps** command in privileged EXEC mode. To disable the use of debug timestamps, use the **no** form of this command.

debug timestamps [level]

no debug timestamps

Syntax Description	level (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level is a higher number.							
Defaults	The defaults are as fo	ollows:						
	• Debug timestam	p information is disabled	1.					
	• The default value	e for <i>level</i> is 1.						
Command Modes	The following table s	shows the modes in whic	h you can enter	the comma	ind:			
		Firewall N	lode	Security C	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	•		
Command History	Release Modification							
	7.0(1)	This command was	s introduced.					
Usage Guidelines	unusable. For this rea	output is assigned high p ason, use <b>debug</b> comman ons with Cisco technical	nds only to troub	leshoot spo	ecific problems	s or during		
	during periods of low	ver network traffic and for ased <b>debug</b> command pro-	ewer users. Debu		• •			

#### hostname# **show debug**

1982769.770000000: parser cache: try to match 'show debug' in exec mode 1982769.770000000: parser cache: hit at index 8 hostname#

**Related Commands** 

ands	Command	Description
	show debug	Displays current debug configuration.

## debug vpn-sessiondb

To display VPN-session database debug information, use the **debug vpn-sessiondb** command in privileged EXEC mode. To disable the display of VPN-session database debug information, use the **no** form of this command.

debug vpn-sessiondb [level]

no debug vpn-sessiondb

Syntax Description	<i>level</i> (Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.						
Defaults	The default value for <i>level</i>	<i>l</i> is 1.					
Command Modes	The following table shows	s the modes in whic	h you can enter	the comma	nd:		
		Firewall N	lode	Security (	Context		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	
		This command was					
Usage Guidelines	Because debugging output unusable. For this reason, troubleshooting sessions w during periods of lower ne likelihood that increased d	use <b>debug</b> commany with Cisco technical etwork traffic and for	nds only to troub support staff. M ewer users. Debu	oleshoot sp oreover, it ugging duri	ecific problems is best to use <b>d</b> ng these period	s or during ebug command	
Examples	The following example enables VPN-session database debug messages. The <b>show debug</b> command reveals that VPN-session database debug messages are enabled.						
	hostname# <b>debug vpn-ses</b> debug vpn-sessiondb en hostname# <b>show debug</b> debug vpn-sessiondb en hostname#	nabled at level 1					

### **Related Commands**

Command	Description
show debug	Displays current debug configuration.

### debug webvpn

To log WebVPN debug messages, use the **debug webvpn** command in privileged EXEC mode. To disable the logging of WebVPN debug messages, use the **no** form of this command.

debug webvpn [chunk | cifs | citrix | failover | html | javascript | request | response | svc | transformation | url | util | xml] [*level*]

no debug webvpn [chunk | cifs | citrix | failover | html | javascript | request | response | svc | transformation | url | util | xml] [*level*]

Syntax Description	chunk	Displays debug messages about memory blocks used to support WebVPN connections.
	cifs	Displays debug messages about connections between Common Internet File System (CIFS) servers and WebVPN users.
	citrix	Displays debug messages about connections between Citrix Metaframe Servers and Citrix ICA clients over WebVPN.
	failover	Displays debug messages about equipment failovers affecting WebVPN connections.
	html	Displays debug messages about HTML pages sent over WebVPN connections.
	javascript	Displays debug messages about JavaScript sent over WebVPN connections.
	request	Displays debug messages about requests issued over WebVPN connections.
	response	Displays debug messages about responses issued over WebVPN connections.
	svc	Displays debug messages about connections to SSL VPN clients over WebVPN.
	transformation	Displays debug messages about WebVPN content transformation.
	url	Displays debug messages about website requests issued over WebVPN connections.
	util	Displays debug messages about CPU utilization dedicated to support connections to WebVPN remote users.
	xml	Displays debug messages about JavaScript sent over WebVPN connections.
	level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

show debug

		Firewall	Firewall Mode		Security Context		
		Routed	Transparent	Single	Multiple		
	Command Mode				Context	System	
	Privileged EXEC	•	•	•		•	
Command History	Release Modification						
-	7.0(1)	This command wa	as introduced.				
Jsage Guidelines	The high priority assig <b>debug</b> commands only technical support staff traffic and fewer users command processing of	to troubleshoot speci Moreover, it is best to Debugging during the	fic problems or d to use <b>debug</b> com tese periods decre	uring troub mands duri	leshooting sessing periods of	sions with Cis lower networ	
	<b>debug</b> commands only technical support staff traffic and fewer users command processing of	y to troubleshoot speci . Moreover, it is best t . Debugging during the poverhead will affect sy	fic problems or d to use <b>debug</b> com lese periods decre ystem use.	uring troub mands duri eases the lik	leshooting sess ing periods of celihood that in	sions with Cis lower networ hcreased <b>deb</b> i	
Jsage Guidelines Examples	<b>debug</b> commands only technical support staff traffic and fewer users	y to troubleshoot speci . Moreover, it is best t . Debugging during the poverhead will affect sy e enables WebVPN de	fic problems or d to use <b>debug</b> com lese periods decre ystem use.	uring troub mands duri eases the lik	leshooting sess ing periods of celihood that in	sions with Cis lower networ hcreased <b>deb</b> i	
	debug commands only technical support staff traffic and fewer users command processing of The following example command reveals that hostname# debug webv INF0: debug webvpn of hostname# show debug	y to troubleshoot speci . Moreover, it is best to . Debugging during the poverhead will affect sy e enables WebVPN de CIFS debug messages vpn cifs cifs enabled at level g	fic problems or d to use <b>debug</b> com lese periods decre ystem use.	uring troub mands duri eases the lik	leshooting sess ing periods of celihood that in	sions with Cis lower networ hcreased <b>deb</b> i	
	debug commands only technical support staff traffic and fewer users command processing of The following example command reveals that hostname# debug webv INF0: debug webvpn of	y to troubleshoot speci . Moreover, it is best to . Debugging during the poverhead will affect sy e enables WebVPN de CIFS debug messages vpn cifs cifs enabled at level g	fic problems or d to use <b>debug</b> com lese periods decre ystem use.	uring troub mands duri eases the lik	leshooting sess ing periods of celihood that in	sions with Cis lower networ hcreased <b>deb</b> i	

Displays current debug configuration.

The following table shows the modes in which you can enter the command:

## debug xdmcp

To show debug messages for XDMCP application inspection, use the **debug xdmcp** command in privileged EXEC mode. To stop showing debug messages for XDMCP application inspection, use the **no** form of this command.

debug xdmcp [level]

no debug xdmcp [level]

Syntax Description	level	(Optional) Sets the default is 1. To dis a higher number.	0 0		<b>T A</b> .			
Defaults	The default value for <i>lev</i>	<i>vel</i> is 1.						
Command Modes	The following table shows the modes in which you can enter the command:							
		Firewall N	Firewall Mode		Security Context			
	Command Mode		Transparent		Multiple			
		Routed		Single	Context	System		
	Privileged EXEC	•	•	•	•			
Command History	Release Modification							
	Preexisting This command was preexisting.							
Usage Guidelines	To see the current debug enter the <b>no debug</b> comp command.							
Note	Enabling the <b>debug xdn</b>	<b>ncp</b> command may s	low down traffic	on busy no	etworks.			
Note	Enabling the <b>debug xdn</b> The following example of inspection:					plication		

### Related Commands

ıds	Command	Description	
	class-map	Defines the traffic class to which to apply security actions.	
	inspect xdmcp	Enables XDMCP application inspection.	
	policy-map	Associates a class map with specific security actions.	
	service-policy	Applies a policy map to one or more interfaces.	