CHAPTER 25

show asp drop ～ show curpriv コマンド

show asp drop

コントロール プレーン パスでパケットまたは接続が破棄された原因をデバッグするには、特権 EXEC モードで **show asp drop** コマンドを使用します。このコマンドは、コントロール プレーン パスを通過するトラフィックについて、破棄されたパケットとフローのみを表示します。これには、大半のインスペクション トラフィック、FWSM を直接の宛先とするトラフィック、およびすべての IPv6 トラフィックが含まれます。FWSM 内で処理または破棄されたパケットやフローは、このコマンドの出力に含まれません。

show asp drop [**flow** *drop_reason* | **frame** *drop_reason*]

シンタックスの説明

flow	（任意）廃棄されたフロー（接続）数を表示します。
frame	（任意）廃棄されたパケット数を表示します。
drop_reason	（任意）特定のプロセスによって廃棄されたフローまたはパケットを表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

show asp drop コマンドは、コントロール プレーンで発生した問題のトラブルシューティングに使用します。この情報はデバッグ専用です。出力される情報は変更されることがあります。このコマンドを使用してシステムをデバッグする方法については、シスコの TAC にお問い合わせください。

例

次に、**show asp drop** コマンドの出力例を示します。

```
hostname# show asp drop

Frame drop:
No route to host                                        600
TCP packet SEQ past window                               13
TCP invalid ACK                                        2051
TCP packet buffer full                                   15
TCP DUP and has been ACKed                             4206
TCP packet failed PAWS test                              32
No inspect found                                        151
Invalid connection address in delete indication        1465

Flow drop:
```

関連コマンド

コマンド	説明
clear asp drop	高速セキュリティ パスの廃棄に関する統計情報を消去します。
show conn	接続に関する情報を表示します。

show asp table arp

高速セキュリティ パスの ARP テーブルをデバッグするには、特権 EXEC モードで **show asp table arp** コマンドを使用します。

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

シンタックスの説明

address *ip_address*	（任意）表示する ARP テーブル エントリに対応した IP アドレスを識別します。
interface *interface_name*	（任意）表示する ARP テーブルに対応した特定のインターフェイスを識別します。
netmask *mask*	（任意）IP アドレスのサブネット マスクを設定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

show arp コマンドはコントロール プレーンの内容を表示し、**show asp table arp** コマンドは高速セキュリティ パスの内容を表示します。これらの情報は、問題のトラブルシューティングに役立ちます。高速セキュリティ パスの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。これらの情報はデバッグ専用です。出力される情報は変更されることがあります。このコマンドを使用してシステムをデバッグする方法については、シスコの TAC にお問い合わせください。

例

次に、**show asp table arp** コマンドの出力例を示します。

```
hostname# show asp table arp

Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0

Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

関連コマンド

コマンド	説明
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。

show asp table classify

高速セキュリティ パスの分類子テーブルをデバッグするには、特権 EXEC モードで **show asp table classify** コマンドを使用します。分類子は着信パケットのプロパティ（プロトコル、送信元や宛先アドレスなど）を調べ、各パケットと対応する分類ルールを照合します。各ルールには、パケット廃棄やパケット通過許可など、実行するアクション タイプを判別する分類ドメインがラベルとして付加されています。

show asp table classify [**crypto** | **domain** *domain_name* | **interface** *interface_name*]

シンタックスの説明

domain *domain_name*	（任意）特定の分類子ドメインのエントリを表示します。ドメイン リストについては、「使用上のガイドライン」を参照してください。
interface *interface_name*	（任意）表示する分類子テーブルに対応した特定のインターフェイスを識別します。
crypto	（任意）暗号、暗号解除、および IPSec トンネル フロー ドメインのみを表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

show asp table classifier コマンドは、高速セキュリティ パスの分類子の内容を表示します。この情報は、問題のトラブルシューティングに役立ちます。高速セキュリティ パスの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。これらの情報はデバッグ専用です。出力される情報は変更されることがあります。このコマンドを使用してシステムをデバッグする方法については、シスコの TAC にお問い合わせください。

分類子ドメインは次のとおりです。

```
aaa-acct
aaa-auth
aaa-user
accounting
arp
capture
capture
conn-nailed
conn-set
ctcp
decrypt
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
host
inspect
inspect-ctiqbe
inspect-dns
inspect-dns-ids
inspect-ftp
inspect-ftp-data
inspect-gtp
inspect-h323
inspect-http
inspect-icmp
inspect-icmp-error
inspect-ils
inspect-mgcp
inspect-netbios
inspect-pptp
inspect-rsh
inspect-rtsp
inspect-sip
inspect-skinny
inspect-smtp
inspect-snmp
inspect-sqlnet
inspect-sqlnet-plus
inspect-sunrpc
inspect-tftp
inspect-xdmcp
ipsec-natt
ipsec-tunnel-flow
ipsec-user
limits
lu
mac-permit
mgmt-lockdown
mgmt-tcp-intercept
multicast
nat
nat-exempt
nat-exempt-reverse
nat-reverse
null
permit
permit-ip-option
permit-log
pim
ppp
punt
punt-l2
punt-root
```

```
shun
tcp-intercept
```

例

次に、**show asp table classify** コマンドの出力例を示します。

```
hostname# show asp table classify

Interface test:
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=10.86.194.60, mask=255.255.255.255, port=0
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
...
```

関連コマンド

コマンド	説明
show asp drop	廃棄されたパケット数を示す高速セキュリティ パスのカウンタを表示します。

show asp table interfaces

高速セキュリティ パスのインターフェイス テーブルをデバッグするには、特権 EXEC モードで **show asp table interfaces** コマンドを使用します。

show asp table interfaces

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

show asp table interfaces コマンドは、高速セキュリティ パスのインターフェイス テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立ちます。高速セキュリティ パスの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。これらの情報はデバッグ専用です。出力される情報は変更されることがあります。このコマンドを使用してシステムをデバッグする方法については、シスコの TAC にお問い合わせください。

例

次に、**show asp table interfaces** コマンドの出力例を示します。

```
hostname# show asp table interfaces

** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20

Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan 301, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan 302, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 303, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスのランタイム ステータスおよび統計情報を表示します。

show asp table mac-address-table

高速セキュリティ パスの MAC（メディア アクセス制御）テーブルをデバッグするには、特権 EXEC モードで **show asp table mac-address-table** コマンドを使用します。

show asp table mac-address-table [**interface** *interface_name*]

シンタックスの説明

interface *interface_name*	（任意）特定のインターフェイスの MAC アドレス テーブルを表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	•

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

show asp table mac-address-table コマンドは、高速セキュリティ パスの MAC アドレス テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立ちます。高速セキュリティ パスの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。これらの情報はデバッグ専用です。出力される情報は変更されることがあります。このコマンドを使用してシステムをデバッグする方法については、シスコの TAC にお問い合わせください。

例

次に、**show asp table mac-address-table** コマンドの出力例を示します。

```
hostname# show asp table mac-address-table

interface                  mac  address       flags
----------------------------------------------------------
    inside1                     0009.b74d.3800     None
    inside1                     0007.e903.ad6e     None
    inside1                     0007.e950.2067     None
    inside1                     0050.0499.3749     None
    inside1                     0012.d96f.e200     None
    inside1                     0001.02a7.f4ec     None
    inside1                     0001.032c.6477     None
    inside1                     0004.5a2d.a1c8     None
    inside1                     0003.4773.c87b     None
    inside1                     000d.88ef.5d1c     None
    inside1                     00c0.b766.adce     None
    inside1                     0050.5640.450d     None
    inside1                     0001.03cf.0431     None
...
```

関連コマンド

コマンド	説明
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含めて、MAC アドレス テーブルを表示します。

show asp table routing

高速セキュリティ パスのルーティング テーブルをデバッグするには、特権 EXEC モードで **show asp table routing** コマンドを使用します。このコマンドは IPv4 および IPv6 アドレスをサポートします。

show asp table routing [**input** | **output**] [**address** *ip_address* [***netmask*** *mask*] |
interface *interface_name*]

シンタックスの説明

address *ip_address*	表示するルーティング エントリに対応した IP アドレスを設定します。IPv6 アドレスの場合は、スラッシュ（/）のあとにプレフィクス（0 ～ 128）を付加して、サブネット マスクを追加できます。たとえば、次のように入力します。 `fe80::2e0:b6ff:fe01:3b7a/128`
input	入力ルート テーブルのエントリを表示します。
interface *interface_name*	（任意）表示するルーティング テーブルに対応した特定のインターフェイスを識別します。
netmask *mask*	IPv4 アドレスの場合は、サブネット マスクを指定します。
output	出力ルート テーブルのエントリを表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

show asp table routing コマンドは、高速セキュリティ パスのルーティング テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立ちます。高速セキュリティ パスの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。これらの情報はデバッグ専用です。出力される情報は変更されることがあります。このコマンドを使用してシステムをデバッグする方法については、シスコの TAC にお問い合わせください。

例

次に、**show asp table routing** コマンドの出力例を示します。

```
hostname# show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

関連コマンド

コマンド	説明
show route	コントロール プレーンのルーティング テーブルを表示します。

show asp table vpn-context

高速セキュリティ パスの VPN（バーチャル プライベート ネットワーク）コンテキスト テーブルをデバッグするには、特権 EXEC モードで **show asp table vpn-context** コマンドを使用します。

show asp table vpn-context [**detail**]

シンタックスの説明

detail	（任意）VPN コンテキスト テーブルの詳細を表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

show asp table vpn-context コマンドは、高速セキュリティ パスの VPN コンテキストの内容を表示します。この情報は、問題のトラブルシューティングに役立ちます。高速セキュリティ パスの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。これらの情報はデバッグ専用です。出力される情報は変更されることがあります。このコマンドを使用してシステムをデバッグする方法については、シスコの TAC にお問い合わせください。

例

次に、**show asp table vpn-context** コマンドの出力例を示します。

```
hostname# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

次に、**show asp table vpn-context detail** コマンドの出力例を示します。

```
hostname# show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

関連コマンド

コマンド	説明
show asp drop	廃棄されたパケット数を示す高速セキュリティ パスのカウンタを表示します。

show asr

ASR グループのメンバーを表示するには、特権 EXEC モードで **show asr** コマンドを使用します。

show asr {*group_id* | ***all***}

シンタックスの説明

group_id	指定した ASR グループに属する VLAN（仮想 LAN）を表示します。有効値は 1 ～ 32 です。
all	32 のすべての ASR グループのメンバーシップを表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

ASR グループにはメンバーを 8 つまで含めることができます。出力に [0]（ゼロ）が表示されている場合は、スロットが空です。

show asr コマンドの出力は、**show np asr** コマンドの出力と同じです。

例

次に、**show asr** コマンドの出力例を示します。ASR グループ 1 に属する VLAN に限定して表示します。

```
hostname# sh asr 1

ASR Group |    Vlan Entries in ASR Group (0 denotes empty slot)
----------|-----------------------------------------------------
        1 |    10   20   0    0    0    0    0    0
```

次に、**show asr** コマンドの出力例を示します。有効なすべての ASR グループの VLAN メンバーシップを表示します。この例では、ASR グループ 1 にのみメンバー VLAN が含まれています。

```
hostname# sh asr all
ASR Group |    Vlan Entries in ASR Group (0 denotes empty slot)
----------|-------------------------------------------------
        1 |    10   20   0    0    0    0    0    0
        2 |    0    0    0    0    0    0    0    0
        3 |    0    0    0    0    0    0    0    0
        4 |    0    0    0    0    0    0    0    0
        5 |    0    0    0    0    0    0    0    0
        6 |    0    0    0    0    0    0    0    0
        7 |    0    0    0    0    0    0    0    0
        8 |    0    0    0    0    0    0    0    0
        9 |    0    0    0    0    0    0    0    0
       10 |    0    0    0    0    0    0    0    0
       11 |    0    0    0    0    0    0    0    0
       12 |    0    0    0    0    0    0    0    0
       13 |    0    0    0    0    0    0    0    0
       14 |    0    0    0    0    0    0    0    0
       15 |    0    0    0    0    0    0    0    0
       16 |    0    0    0    0    0    0    0    0
       17 |    0    0    0    0    0    0    0    0
       18 |    0    0    0    0    0    0    0    0
       19 |    0    0    0    0    0    0    0    0
       20 |    0    0    0    0    0    0    0    0
       21 |    0    0    0    0    0    0    0    0
       22 |    0    0    0    0    0    0    0    0
       23 |    0    0    0    0    0    0    0    0
       24 |    0    0    0    0    0    0    0    0
       25 |    0    0    0    0    0    0    0    0
       26 |    0    0    0    0    0    0    0    0
       27 |    0    0    0    0    0    0    0    0
       28 |    0    0    0    0    0    0    0    0
       29 |    0    0    0    0    0    0    0    0
       30 |    0    0    0    0    0    0    0    0
       31 |    0    0    0    0    0    0    0    0
       32 |    0    0    0    0    0    0    0    0
```

関連コマンド

コマンド	説明
asr-group	ASR グループのメンバーとしてインターフェイスを指定します。

show auto-update

Auto Update Server の設定を表示するには、特権 EXEC モードで **show auto-update** コマンドを使用します。

show auto-update

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、**show auto-update** コマンドの出力例を示します。

```
hostname# show arp-inspection
Poll period: 1 minutes, retry count: 1, retry period: 5 minutes
Timeout: none
Device ID: host name [farscape]
```

関連コマンド

コマンド	説明
auto-update device-id	Auto Update Server で使用する FWSM のデバイス ID を設定します。
auto-update poll-period	FWSM が Auto Update Server からの更新をチェックする頻度を設定します。
auto-update server	Auto Update Server を識別します。
auto-update timeout	タイムアウト期間内に Auto Update Server と通信しなかった場合、FWSM 内のトラフィック通過を停止します。
clear configure auto-update	Auto Update Server の設定を消去します。

show blocks

パケット バッファ利用率を表示するには、特権 EXEC モードで **show blocks** コマンドを使用します。

show blocks [{***address*** *hex* | ***all*** | ***assigned*** | ***free*** | ***old*** | ***pool*** *size* [***summary***]} [**diagnostics** | ***dump*** | ***header*** | ***packet***] | ***queue history*** [***detail***]]

シンタックスの説明

address *hex*	（任意）このアドレスに対応するブロックを 16 進数で表示します。
all	（任意）すべてのブロックを表示します。
assigned	（任意）割り当てられてアプリケーションで使用中のブロックを表示します。
detail	（任意）一意のキュー タイプごとに、先頭ブロックの一部（128 バイト）を表示します。
dump	（任意）ヘッダーやパケット情報を含めて、ブロックの内容全体を表示します。**packet** との違いは、**dump** にはヘッダーとパケット間の追加情報が含まれる点です。
diagnostics	（任意）ブロック診断情報を表示します。
free	（任意）使用可能なブロック数を表示します。
header	（任意）ブロックのヘッダーを表示します。
old	（任意）1 分よりも前に割り当てられたブロック数を表示します。
packet	（任意）ブロックのヘッダーおよびパケットの内容を表示します。
pool *size*	（任意）特定のサイズのブロックを表示します。
queue history	（任意）FWSM でブロックが不足した場合に、ブロックが割り当てられる場所を表示します。プール内のブロックが割り当てられることはありますが、ブロックがキューに割り当てられることはありません。この場合は、ブロックを割り当てたコードのアドレスが割り当て場所になります。
summary	（任意）詳細なブロック使用情報を表示します。この情報は、このクラスにブロックを割り当てたアプリケーションのプログラム アドレス、このクラス内のブロックを解放したアプリケーションのプログラム アドレス、およびこのクラス内の有効ブロックが属するキューを基準として並べ替えられます。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
3.1(1)	**pool summary** オプションが追加されました。

使用上のガイドライン

show blocks コマンドは、FWSM が過負荷かどうかを判別する場合に役立ちます。このコマンドは、事前に割り当てられたシステム バッファの利用率を表示します。メモリが一杯になっていても、FWSM によってトラフィックが送受信されている場合は問題ありません。**show conn** コマンドを使用すると、トラフィックが送受信されているかどうかを確認できます。トラフィックが送受信されず、メモリが一杯の場合は、問題が発生することがあります。

SNMP（簡易ネットワーク管理プロトコル）を使用してこの情報を表示することもできます。

セキュリティ コンテキストで表示される情報には、システム全体の情報、使用中のブロックに関するコンテキスト固有の情報、およびブロック使用率の上限値が含まれます。

出力の説明については、「例」を参照してください。

例

次に、シングル モードにおける **show blocks** コマンドの出力例を示します。

```
hostname# show blocks
SIZE     MAX    LOW    CNT
     4    1600   1598   1599
    80     400    398    399
   256    3600   3540   3542
  1550    4716   3177   3184
 16384      10     10     10
  2048    1000   1000   1000
```

表 25-1 に各フィールドの説明を示します。

表 25-1　show blocks のフィールド

フィールド	説明
SIZE	ブロック プールのサイズ（バイト）。各サイズは特定のタイプを表します。次に例を示します。
4	DNS、ISAKMP、URL フィルタリング、uauth、TFTP（簡易ファイル転送プロトコル）、および TCP モジュールなどのアプリケーションで、既存のブロックを複製します。
80	確認応答パケットを生成するため、およびフェールオーバー hello メッセージ用に、TCP 代行受信で使用されます。
256	ステートフル フェールオーバー更新、Syslog 作成、およびその他の TCP 機能に使用されます。 これらのブロックは、主にステートフル フェールオーバー メッセージに使用されます。アクティブ FWSM はパケットを生成し、スタンバイ FWSM に送信して、変換および接続テーブルを更新します。バースト トラフィックが発生し、大量の接続が作成または切断された場合は、使用可能なブロック数が 0 になることがあります。この状況は、スタンバイ FWSM に対して更新されなかった接続が 1 つまたは複数あったことを示します。ステートフル フェールオーバー プロトコルは次回に、失われた変換または接続を捕捉します。256 バイト ブロックに関する CNT カラム値が 0 付近に長時間留まっている場合は、FWSM が 1 秒間に処理する接続数がネックとなって、FWSM は変換および接続テーブルの同期を保つことができません。 FWSM から送信される Syslog メッセージにも 256 バイト ブロックが使用されますが、通常は、256 バイト ブロック プールを枯渇させるほど、これらのメッセージが大量にリリースされることはありません。CNT カラムに表示された 256 バイト ブロック数が 0 付近の値である場合は、Syslog サーバに Debugging（レベル 7）でロギングしていないかを確認してください。ロギング レベルは、FWSM コンフィギュレーション内のロギング トラップ行で示されます。デバッグのための追加情報が必要な場合を除き、ロギング レベルを Notification（レベル 5）以下に設定することを推奨します。

表 25-1　show blocks のフィールド（続き）

フィールド	説明
1550	FWSM を介して処理するイーサネット パケットの保存に使用します。 FWSM のインターフェイスに着信したパケットは、入力インターフェイス キューに格納され、OS（オペレーティング システム）に送信されて、ブロックに格納されます。FWSM は、セキュリティ ポリシーに基づいてパケットが許可されるか、または拒否されるかを判別し、発信インターフェイスの出力キューにパケットを送信します。FWSM がトラフィック負荷に対応できない場合は、使用可能なブロック数が 0 に近い値になります（コマンド出力の CNT カラムに表示）。CNT カラムが 0 の場合、FWSM はより多くのブロック（最大 8192）を割り当てようとします。使用可能なブロックがない場合、FWSM はパケットを廃棄します。
16384	64 ビットの 66 MHz ギガビット イーサネット カード（i82543）専用です。 イーサネット パケットの詳細については、1550 の説明を参照してください。
2048	制御更新に使用されるコントロールまたはガイド付きフレーム
MAX	指定されたバイト数のブロック プールで使用可能な最大ブロック数。起動時に、最大限のブロック数がメモリから切り分けられます。通常、最大ブロック数は変化しません。256 および 1550 バイト ブロックの場合は例外的に、FWSM は必要に応じて最大で 8192 のブロックを動的に作成できます。
LOW	下限値を示します。この値は、FWSM に電源を投入したあと、または（**clear blocks** コマンドを使用して）前回ブロックを削除したあとに、使用可能な該当サイズの最小ブロック数を示します。LOW カラムが 0 の場合は、直前のイベントでメモリが一杯になったことを示します。
CNT	特定のサイズのブロック プールで現在使用可能なブロック数。CNT カラムが 0 の場合は、現在メモリが一杯であることを示します。

次に、**show blocks all** コマンドの出力例を示します。

```
hostname# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc
not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc
not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc
not_specified

...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

表 25-2 に各フィールドの説明を示します。

表 25-2　show blocks all のフィールド

フィールド	説明
Block	ブロックのアドレス
allocd_by	最後にブロックを使用したアプリケーションのプログラム アドレス（ブロックを使用しなかった場合は 0）
freed_by	最後にブロックを解放したアプリケーションのプログラム アドレス
data size	ブロック内のアプリケーション バッファ / パケット データのサイズ

表 25-2　show blocks all のフィールド

フィールド	説明
alloccnt	ブロック存続後の該当ブロックの使用回数
dup_cnt	該当ブロックが使用されている場合は、このブロックの現在の参照数。0 は参照数が 1、1 は参照数が 2 です。
oper	ブロックに最後に実行された処理（alloc、get、put、free の 4 つのうちのいずれか）。
location	ブロックを使用しているアプリケーション、または最後にブロックを割り当てたアプリケーションのプログラム アドレス（allocd_by フィールドと同じ）

次に、コンテキスト内の **show blocks** コマンドの出力例を示します。

```
hostname/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

次に、**show blocks queue history** コマンドの出力例を示します。

```
hostname# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb

Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
...
```

次に、**show blocks queue history detail** コマンドの出力例を示します。

```
hostname# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

次に、**show blocks pool summary** コマンドの出力例を示します。

```
hostname# show blocks pool 1550 summary
Class 3, size 1550

================================================
         total_count=1531    miss_count=0
Alloc_pc        valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
         total_count=9716    miss_count=0
Freed_pc        valid_cnt       invalid_cnt
0x9a81f3        00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326        00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2        00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
         total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

表 25-3 に各フィールドの説明を示します。

表 25-3　show blocks pool summary のフィールド

フィールド	説明
total_count	指定されたクラスのブロック数
miss_count	技術的な理由により、指定されたカテゴリ内で報告されなかったブロック数
Freed_pc	このクラス内のブロックを解放したアプリケーションのプログラム アドレス
Alloc_pc	このクラス内のブロックを割り当てたアプリケーションのプログラム アドレス
Queue	このクラス内の有効ブロックが属するキュー
valid_cnt	現在割り当てられているブロック数
invalid_cnt	現在割り当てられていないブロック数
Invalid Bad qtype	このキューが解放されて内容が無効であるか、またはこのキューが初期化されていません。
Valid tcp_usr_conn_inp	キューが有効です。

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てるメモリを増加させます。
clear blocks	システム バッファ統計情報を消去します。
show conn	アクティブな接続を表示します。

show capture

オプションを指定しない場合のキャプチャ設定を表示するには、**show capture** コマンドを使用します。

show capture [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**detail**] [**dump**] [**packet-number** *number*]

シンタックスの説明

capture_name	（任意）パケット キャプチャの名前
access-list *access_list_name*	（任意）特定のアクセス リスト ID の IP フィールドまたはその上位フィールドに基づいてパケット情報を表示します。
count *number*	（任意）指定されたデータのパケット数を表示します。
detail	（任意）各パケットの追加プロトコル情報を表示します。
dump	（任意）データ リンク トランスポートを介して転送されるパケットの 16 進ダンプを表示します。
packet-number *number*	指定されたパケット番号から表示を開始します。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

セキュリティ コンテキスト モード:シングル コンテキスト モードおよびマルチ コンテキスト モード

アクセス場所：システムおよびコンテキスト コマンドライン

コマンド モード：特権モード

ファイアウォール モード：ルーテッド ファイアウォール モードおよびトランスペアレント ファイアウォール モード

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

capture_name を指定した場合は、該当するキャプチャのキャプチャ バッファの内容が表示されます。

dump キーワードを指定した場合、16 進ダンプ内の MAC（メディア アクセス制御）情報は表示されません。

パケットのデコード出力は、パケットのプロトコルによって異なります。表 25-4 のカッコで囲まれた出力は、**detail** キーワードを指定した場合に表示されます。

表 25-4　パケット キャプチャの出力形式

パケット タイプ	キャプチャ出力形式
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp:*icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*:[checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*:*tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/ その他	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*:*ip-protocol ip-length*
その他	*HH:MM:SS.ms ether-hdr* : *hex-dump*

例

次に、**show capture** コマンドの出力例を示します。このコマンドは、FWSM 上に設定されているキャプチャを表示します。

```
hostname(config)# sh capture

capture cap_out type raw-data access-list capture interface outside[Capturing - 504
bytes]
capture cap_in type raw-data access-list capture interface inside[Capturing - 504
bytes]
```

次に、特定のキャプチャに対する **show capture** コマンドの出力例を示します。

```
hostname(config)# sh capture cap_in

6 packets seen, 6 packets captured
   1: 22:46:15.235410840 802.1Q vlan#3 P0 10.2.1.1 > 10.1.1.1: icmp: echo request
   2: 22:46:15.235410840 802.1Q vlan#3 P0 10.1.1.1 > 10.2.1.1: icmp: echo reply
   3: 22:46:16.235411840 802.1Q vlan#3 P0 10.2.1.1 > 10.1.1.1: icmp: echo request
   4: 22:46:16.235411840 802.1Q vlan#3 P0 10.1.1.1 > 10.2.1.1: icmp: echo reply
   5: 22:46:17.235412840 802.1Q vlan#3 P0 10.2.1.1 > 10.1.1.1: icmp: echo request
   6: 22:46:17.235412850 802.1Q vlan#3 P0 10.1.1.1 > 10.2.1.1: icmp: echo reply
6 packets shown
```

次に、**show capture** コマンドに ***detail*** キーワードを指定した場合の出力例を示します。

```
hostname(config)# sh capture cap_out detail

6 packets seen, 6 packets captured
   1: 22:46:15.235410840 0016.c873.9300 0001.0310.f4c5 0x8100 102: 802.1Q vlan#2 P0
10.2.1.1 > 10.1.1.1: icmp: echo request (DF) (ttl 64, id 0)
   2: 22:46:15.235410840 0001.0310.f4c5 0016.c873.9300 0x8100 102: 802.1Q vlan#2 P0
10.1.1.1 > 10.2.1.1: icmp: echo reply (ttl 64, id 26957)
   3: 22:46:16.235411840 0016.c873.9300 0001.0310.f4c5 0x8100 102: 802.1Q vlan#2 P0
10.2.1.1 > 10.1.1.1: icmp: echo request (DF) (ttl 64, id 0)
   4: 22:46:16.235411840 0001.0310.f4c5 0016.c873.9300 0x8100 102: 802.1Q vlan#2 P0
10.1.1.1 > 10.2.1.1: icmp: echo reply (ttl 64, id 26958)
   5: 22:46:17.235412840 0016.c873.9300 0001.0310.f4c5 0x8100 102: 802.1Q vlan#2 P0
10.2.1.1 > 10.1.1.1: icmp: echo request (DF) (ttl 64, id 0)
   6: 22:46:17.235412850 0001.0310.f4c5 0016.c873.9300 0x8100 102: 802.1Q vlan#2 P0
10.1.1.1 > 10.2.1.1: icmp: echo reply (ttl 64, id 26959)
6 packets shown
hostname(config)#
```

関連コマンド

コマンド	説明
capture	パケット キャプチャ機能をイネーブルにして、パケット スニフィングおよびネットワーク障害検出を有効にします。
clear capture	キャプチャ バッファを消去します。
copy capture	キャプチャ ファイルをサーバにコピーします。

show checkheaps

チェックヒープ統計情報を表示するには、特権 EXEC モードで **show checkheaps** コマンドを使用します。チェックヒープは、ヒープ メモリ バッファの妥当性（動的メモリはシステム ヒープ メモリ領域から割り当てられます）、およびコード領域の整合性を検証する定期的なプロセスです。

show checkheaps

シンタックスの説明　このコマンドには、引数またはキーワードはありません。

デフォルト　このコマンドには、デフォルトの動作または値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

例　次に、**show checkheaps** コマンドの出力例を示します。

```
hostname# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

関連コマンド

コマンド	説明
checkheaps	チェックヒープの検証間隔を設定します。

show checksum

設定のチェックサムを表示するには、特権 EXEC モードで **show checksum** コマンドを使用します。

show checksum

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

show checksum コマンドを使用すると、設定内容のデジタル サマリーとして機能する、4 つの 16 進数のグループを表示できます。このチェックサムが計算されるのは、設定がフラッシュ メモリに保存されている場合のみです。

show config または **show checksum** コマンド出力のチェックサムの前にドット（[.]）が表示されている場合、この出力は通常のコンフィギュレーション読み込みまたは書き込みモードのインジゲータを示しています（FWSM フラッシュ パーティションからのロード、またはそこへの書き込みを行っている場合）。[.] は、FWSM が他の処理を実行中ではあるが、「ハングアップ」していないことを示しています。このメッセージは、[system processing, please wait] というメッセージと同じです。

例

次に、設定のチェックサムを表示する例を示します。

```
hostname(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

チャンク統計情報を表示するには、特権 EXEC モードで **show chunkstat** コマンドを使用します。

show chunkstat

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

例

次に、チャンク統計情報を表示する例を示します。

```
hostname# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24,
end @ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
show cpu	CPU 利用率情報を表示します。

show class

クラスに割り当てられたコンテキストを表示するには、特権 EXEC モードで **show class** コマンドを使用します。

show class *name*

シンタックスの説明

name	名前を最大 20 文字の文字列で指定します。デフォルト クラスを表示するには、名前として **default** を入力します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	該当なし	該当なし	—	—	•

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

例

次に、**show class default** コマンドの出力例を示します。

```
hostname# show class default

Class Name           Members    ID   Flags
default                All       1    0001
```

関連コマンド

コマンド	説明
class	リソース クラスを設定します。
clear configure class	クラス設定を消去します。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスのリソース制限を設定します。
member	リソース クラスにコンテキストを割り当てます。

show conn

指定された接続タイプの接続状態を表示するには、特権 EXEC モードで **show conn** コマンドを使用します。このコマンドは IPv4 および IPv6 アドレスをサポートします。

show conn [**all** | **count**] [**state** *state_type*] | [{{**foreign** | **local**} *ip* [*-ip2*] **netmask** *mask*}] | [**long** | ***detail***] | [{{**lport** | **fport**} *port1*} [*-port2*]] | [**protocol** {**tcp** | **udp**}]

シンタックスの説明

all	トラフィックが通過する接続およびデバイスとの接続を表示します。
count	（任意）アクティブな接続数を表示します。
detail	変換タイプやインターフェイス情報など、接続の詳細を表示します。
foreign	指定された外部 IP アドレスを持つ接続を表示します。
fport	指定された外部ポートを持つ接続を表示します。
ip	ドット付き 10 進表記の IP アドレス、または IP アドレス範囲の先頭アドレス
-ip2	（任意）IP アドレス範囲の終了 IP アドレス
local	指定されたローカル IP アドレスを持つ接続を表示します。
long	（任意）接続をロング形式で表示します。
lport	指定されたローカル ポートを持つ接続を表示します。
netmask	指定された IP アドレスで使用するサブネット マスクを指定します。
mask	ドット付き 10 進表記のサブネット マスク
port1	ポート番号、またはポート番号範囲の先頭ポート番号
-port2	（任意）ポート番号範囲の終了ポート番号
protocol	（任意）接続プロトコルを指定します。
state	（任意）指定された接続の状態を表示します。
state_type	接続状態のタイプを指定します。接続状態のタイプに使用できるキーワードについては、表 25-5 を参照してください。
tcp	TCP プロトコル接続を表示します。
udp	UDP プロトコル接続を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

show conn コマンドはアクティブな TCP 接続数、および各タイプの接続情報を表示します。接続情報全体を表示するには、**show conn all** コマンドを使用します。

（注）　FWSM によってピンホールが作成され、セカンダリ接続を確立できる場合、**show conn** コマンドの出力には不完全接続として表示されます。この不完全接続を消去するには、**clear local** コマンドを使用します。

show conn state コマンドを使用して指定できる接続タイプは、表 25-5 で定義されています。複数の接続タイプを指定する場合は、キーワードをカンマで区切ります。スペースは挿入しません。

表 25-5　接続状態のタイプ

キーワード	表示される接続タイプ
up	アップ状態の接続
conn_inbound	着信接続
ctiqbe	Computer Telephony Interface Quick Buffer Encoding（CTIQBE）接続
data_in	着信データ接続
data_out	発信データ接続
finin	FIN 着信接続
finout	FIN 発信接続
h225	H.225 接続
h323	H.323 接続
http_get	HTTP get 接続
mgcp	Media Gateway Control Protocol（MGCP）接続
nojava	Java アプレットへのアクセスを拒否する接続
rpc	RPC 接続
sip	SIP 接続
skinny	Skinny Client Control Protocol（SCCP）接続
smtp_data	SMTP メール データ接続
sqlnet_fixup_data	SQL*Net データ インスペクション エンジン接続

detail オプションを使用すると、表 25-6 で定義された接続フラグを使用して、変換タイプおよびインターフェイス情報が表示されます。

表 25-6　接続フラグ

フラグ	説明
a	SYN に対する待機中の外部 ACK（確認応答）
A	SYN に対する待機中の内部 ACK
B	外部からの初期 SYN
C	CTIQBE メディア接続
d	ダンプ
D	DNS
E	外部バック接続
f	内部 FIN
F	外部 FIN
g	MGCP 接続

表 25-6　接続フラグ（続き）

フラグ	説明
G	グループに属する接続[1]
h	H.225
H	H.323
i	不完全な TCP または UDP 接続
I	着信データ
k	SCCP メディア接続
m	SIP メディア接続
M	SMTP データ
O	発信データ
p	複製済み（未使用）
P	内部バック接続
q	SQL*Net データ
r	内部確認応答済み FIN
R	外部確認応答済み FIN（TCP 接続用）
R	UDP RPC[2]
s	待機中の外部 SYN
S	待機中の内部 SYN
t	SIP の過渡的接続[3]
T	SIP 接続[4]
U	アップ

1. G フラグは、接続がグループの一部であることを示します。制御接続および関連するすべてのセカンダリ接続を指定するために、GRE および FTP Strict フィックスアップによって設定されます。制御接続が終了すると、関連するすべてのセカンダリ接続も終了します。
2. **show conn** コマンド出力の各行は 1 つの接続（TCP または UDP）を表すため、各行に表示される R フラグは 1 つのみです。
3. UDP 接続の場合、値 t は 1 分後に接続がタイムアウトすることを示します。
4. UDP 接続の場合、値 T は **timeout sip** コマンドで指定された値に従って接続がタイムアウトすることを示します。

（注） DNS サーバを使用する接続の場合、接続の送信元ポートは **show conn** コマンド出力の *IP address of DNS server* で置き換えることができます。

複数の DNS セッションが同じ 2 つのホスト間にあり、これらのセッションの 5 つのタプル（送信元 / 宛先 IP アドレス、送信元 / 宛先ポート、およびプロトコル）が同じである場合、これらのセッションに対応する接続が 1 つ作成されます。DNS の ID は *app_id* によって追跡され、各 app_id のアイドル タイマーはそれぞれ独立して作動します。

app_id は別々に期限切れになるため、正規の DNS 応答が FWSM を通過できるのは特定の期間に限定され、リソースは構築されません。ただし、**show conn** コマンドを入力すると、新しい DNS セッションによってリセットされた DNS 接続のアイドル タイマーが表示されます。これは、共有された DNS 接続の性質によるものであり、設計上の仕様です。

（注）　**conn timeout** コマンドで定義された非アクティビティ期間（デフォルトでは 1:00:00）中に TCP トラフィックが発生しなかった場合、接続は終了し、対応する接続フラグ エントリは表示されなくなります。

例

複数の接続タイプを指定する場合は、キーワードをカンマで区切ります。スペースは挿入しません。次に、アップ状態の RPC、H.323、および SIP 接続情報を含む **show conn** コマンドの出力例を示します。

```
hostname# show conn state up,rpc,h323,sip
```

次に、内部ホスト 10.1.1.15 から外部 Telnet サーバ 192.168.49.10 への TCP セッション接続の出力例を示します。B フラグがないので、この接続は内部から開始されています。[U]、[I]、および [O] フラグは、この接続がアクティブであり、着信および発信データを受信したことを示します。

```
hostname# show conn
2 in use, 2 most used
TCP out 192.168.49.10:23 in 10.1.1.15:1026 idle 0:00:22
Bytes 1774 flags UIO
UDP out 192.168.49.10:31649 in 10.1.1.15:1028 idle 0:00:14
flags D-
```

次に、外部ホスト 192.168.49.10 から内部ホスト 10.1.1.15 への UDP 接続の出力例を示します。D フラグは、これが DNS 接続であることを示します。値 1028 は、接続上の DNS ID です。

```
hostname(config)# show conn detail
2 in use, 2 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIBQE media, D - DNS, d - dump,
       E - outside back connection, f - inside FIN, F - outside FIN,
       G - group, g - MGCP, H - H.323, h - H.255.0, I - inbound data, i - incomplete,
       k - Skinny media, M - SMTP data, m - SIP media
       O - outbound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
TCP outside:192.168.49.10/23 inside:10.1.1.15/1026 flags UIO
UDP outside:192.168.49.10/31649 inside:10.1.1.15/1028 flags dD
```

次に、ホスト 172.16.2.1 からホスト 172.16.112.2 への GRE セッション接続（PROT:47）の出力例を示します。この接続は TCP 接続でないため、単一方向であり、フラグは設定されていません。

```
hostname# show conn
2 in use, 2 most used
Network Processor 1 connections
PROT:47 out 172.16.112.2 in 172.16.2.1 idle 0:00:08
Bytes 18
```

次に、**show conn all** コマンドの出力例を示します。

```
hostname# show conn all
6 in use, 6 most used
  TCP out 209.165.201.1:80 in 10.3.3.4:1404 idle 0:00:00 Bytes 11391
  TCP out 209.165.201.1:80 in 10.3.3.4:1405 idle 0:00:00 Bytes 3709
  TCP out 209.165.201.1:80 in 10.3.3.4:1406 idle 0:00:01 Bytes 2685
  TCP out 209.165.201.1:80 in 10.3.3.4:1407 idle 0:00:01 Bytes 2683
  TCP out 209.165.201.1:80 in 10.3.3.4:1403 idle 0:00:00 Bytes 15199
  TCP out 209.165.201.1:80 in 10.3.3.4:1408 idle 0:00:00 Bytes 2688
  UDP out 209.165.201.7:24 in 10.3.3.4:1402 idle 0:01:30
  UDP out 209.165.201.7:23 in 10.3.3.4:1397 idle 0:01:30
  UDP out 209.165.201.7:22 in 10.3.3.4:1395 idle 0:01:30
```

この例では、内部のホスト 10.3.3.4 は、Web サイト 209.165.201.1 にアクセスしました。外部インターフェイスのグローバル アドレスは 209.165.201.7 です。

関連コマンド

コマンド	説明
inspect ctiqbe	CTIQBE アプリケーション検査をイネーブルにします。
inspect h323	H.323 アプリケーション検査をイネーブルにします。
inspect mgcp	MGCP アプリケーション検査をイネーブルにします。
inspect sip	HTTP トラフィックから Java アプレットを削除します。
inspect skinny	SCCP アプリケーション検査をイネーブルにします。

show console-output

現在キャプチャされているコンソール出力を表示するには、特権 EXEC モードで **show console-output** コマンドを使用します。FWSM は内部コンソール ポート宛の出力を自動的にキャプチャします。シスコ TAC からの指示がないかぎり、内部コンソール ポートは使用しないでください。このコマンドを使用すると、Telnet または SSH セッションに関するコンソール出力を表示できます。

show console-output

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

コンソール ポートにのみ表示される情報は、**perfmon** コマンドの出力、起動メッセージ、および一部のデバッグ メッセージなどです。コンソール バッファのサイズは最大で 1 K です。ユーザは設定できません。

例

次に、コンソール出力がない場合に表示されるメッセージの例を示します。

```
hostname# show console-output
Sorry, there are no messages to display
```

関連コマンド

コマンド	説明
clear configure console	コンソール接続の設定をデフォルトに戻します。

show context

割り当てられたインターフェイスやコンフィギュレーション ファイルの URL などのコンテキスト情報や、設定されたコンテキスト数を表示したり、システム実行スペースからすべてのコンテキストのリストを表示するには、特権 EXEC モードで **show context** コマンドを使用します。

show context [*name* | ***detail*** | ***count***]

シンタックスの説明

count	（任意）設定されたコンテキスト数を表示します。
detail	（任意）実行状態や内部使用情報など、コンテキストに関する詳細情報を表示します。
name	（任意）コンテキスト名を設定します。名前を指定しない場合は、すべてのコンテキストが表示されます。コンテキスト内で入力できるのは、現在のコンテキスト名のみです。

デフォルト

システム実行スペースの場合は、名前を指定しないと、すべてのコンテキストが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

出力の説明については、例を参照してください。

例

次に、**show context** コマンドの出力例を示します。3 つのコンテキストを表示しています。

```
Context Name      Class       Interfaces          Mode          URL
*admin            default     Vlan100,101         Routed        disk:/admin.cfg
contexta          Gold        Vlan200,201         Transparent   disk:/contexta.cfg
contextb          Silver      Vlan300,301         Routed        disk:/contextb.cfg
Total active Security Contexts: 3
```

表 25-7 に各フィールドの説明を示します。

表 25-7　show context のフィールド

フィールド	内容
Context Name	すべてのコンテキストの名前を表示します。アスタリスク（*）が付いたコンテキスト名は管理コンテキストです。
Class	コンテキストが属するリソース クラスを表示します。
Interfaces	コンテキストに割り当てられたインターフェイスを表示します。

表 25-7　show context のフィールド

フィールド	内容
Mode	各コンテキストのファイアウォール モード（ルーテッドまたはトランスペアレント）を表示します。
URL	FWSM がコンテキスト設定をロードする場合のロード元 URL を表示します。

次に、**show context detail** コマンドの出力例を示します。

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk:/admin.cfg
  Real Interfaces: Vlan100
  Mapped Interfaces: Vlan100
  Class: default, Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: disk:/ctx.cfg
  Real Interfaces: Vlan10,20,30
  Mapped Interfaces: int1, int2, int3
  Class: default, Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Vlan100,10,20,30
  Class: default, Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Class: default, Flags: 0x00000009, ID: 258
```

表 25-8 に各フィールドの説明を示します。

表 25-8　コンテキストの状態

フィールド	説明
Context	コンテキストの名前。ヌル コンテキスト情報は内部専用です。システム コンテキストはシステム実行スペースを表します。
State Message:	コンテキストの状態。以下の有効なメッセージを参照してください。
Has been created, but initial ACL rules not complete	FWSM は設定を解析しましたが、デフォルト セキュリティ ポリシーを確立するためのデフォルト ACL（アクセス コントロール リスト）をダウンロードしていません。デフォルト セキュリティ ポリシーは、すべてのコンテキストに最初に適用されます。このポリシーは、下位セキュリティ レベルから上位セキュリティ レベルへのトラフィック送信を禁止したり、アプリケーション検査やその他のパラメータをイネーブルにします。このセキュリティ ポリシーにより、設定が解析されてから、設定 ACL がコンパイルされるまで、トラフィックは FWSM を通過できなくなります。通常、設定 ACL は短時間でコンパイルされるため、この状態は表示されません。
Has been created, but not initialized	**context** *name* コマンドを入力しましたが、**config-url** コマンドを入力していません。

表 25-8　コンテキストの状態（続き）

フィールド	説明
Has been created, but the config hasn't been parsed	デフォルト ACL をダウンロードしましたが、FWSM が設定を解析していません。この状態は、ネットワーク接続問題が原因で設定のダウンロードに失敗したか、**config-url** コマンドをまだ入力していないことなどが考えられます。設定をリロードするには、コンテキスト内から **copy startup-config running-config** と入力します。システムから、**config-url** コマンドを再入力します。ブランクの実行コンフィギュレーションを設定することもできます。
Is a system resource	この状態が適用されるのは、システム実行スペースおよびヌル コンテキストのみです。ヌル コンテキストはシステムで使用され、情報は内部専用です。
Is a zombie	**no context** または **clear context** コマンドを使用してコンテキストを削除しましたが、FWSM がこのコンテキスト ID を新しいコンテキストに再使用するか、またはユーザが再起動するまで、メモリ内にコンテキスト情報が存続します。
Is active	このコンテキストは現在実行中であり、コンテキスト設定セキュリティ ポリシーに従ってトラフィックを送信できます。
Is ADMIN and active	このコンテキストは管理コンテキストであり、現在実行中です。
Was a former ADMIN, but is now a zombie	**clear configure context** コマンドを使用して管理コンテキストを削除しましたが、FWSM がこのコンテキスト ID を新しいコンテキストに再使用するか、またはユーザが再起動するまで、メモリ内にコンテキスト情報が存続します。
Real Interfaces	コンテキストに割り当てられたインターフェイス。 **allocate-interface** コマンドでインターフェイス ID をマッピングした場合は、インターフェイスの実際の名前が表示されます。システム実行スペースにはすべてのインターフェイスが含まれます。
Mapped Interfaces	**allocate-interface** コマンドでインターフェイス ID をマッピングした場合は、マッピング名が表示されます。インターフェイスをマッピングしなかった場合は、実際の名前が再表示されます。
Class	コンテキストが属するリソース クラス
フラグ	内部専用です。
ID	このコンテキストの内部 ID

次に、**show context count** コマンドの出力例を示します。

```
hostname# show context count
Total active contexts: 2
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキストとシステム実行スペースを切り替えます。
config-url	コンテキスト設定の場所を指定します。
context	システム コンフィギュレーション内にセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。

show counters

プロトコル スタック カウンタを表示するには、特権 EXEC モードで **show counters** コマンドを使用します。

show counters [all | **context** *context-name* | **summary** | **top** *n*] [**detail**]
[**protocol** *protocol_name*[**:***counter_name*]] [**threshold** *n*]

シンタックスの説明

all	（マルチ モードのみ）すべてのコンテキストのカウンタを表示します。
context *context-name*	（マルチ モードのみ）カウンタを表示するコンテキスト名を指定します。
:*counter_name*	カウンタを名前で指定します。
detail	カウンタの詳細情報を表示します。
protocol *protocol_name*	指定されたプロトコルのカウンタを表示します。
summary	（マルチ モードのみ）すべてのコンテキスト カウンタをまとめて表示します。
threshold *n*	指定されたしきい値以上のカウンタのみを表示します。指定できる範囲は 1 ～ 4294967295 です。
top *n*	（マルチ モードのみ）指定されたカウンタの上位 *n* 名のユーザのコンテキストを表示します。このオプションでは、カウンタ名を指定する必要があります。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

マルチ コンテキスト モードの場合、デフォルト コンテキストは、各コンテキストのカウンタがまとめて表示される **summary** です。シングル モードの場合、コンテキスト名は無視され、出力の [context] には [single_vf] と表示されます。

デフォルトのカウンタしきい値は **1** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

例

次に、すべてのカウンタを表示する例を示します。

```
hostname# show counters all
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               2   admin
IOS_IPC       OUT_PKTS              2   admin
IOS_IPC       IN_PKTS              15   customera
IOS_IPC       OUT_PKTS              6   customera
```

次に、複数のカウンタのサマリーを表示する例を示します。

```
hostname# show counters
Protocol     Counter           Value   Context
NPCP         IN_PKTS            7195   Summary
NPCP         OUT_PKTS           7603   Summary
IOS_IPC      IN_PKTS             869   Summary
IOS_IPC      OUT_PKTS            865   Summary
IP           IN_PKTS             380   Summary
IP           OUT_PKTS            411   Summary
IP           TO_ARP              105   Summary
IP           TO_UDP                9   Summary
UDP          IN_PKTS               9   Summary
UDP          DROP_NO_APP           9   Summary
FIXUP        IN_PKTS             202   Summary
```

次に、特定のコンテキストのカウンタを表示する例を示します。

```
hostname# show counters context admin
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               4   admin
IOS_IPC      OUT_PKTS              4   admin
```

関連コマンド

コマンド	説明
clear counters	プロトコル スタック カウンタをクリアします。
show counters description	プロトコル カウンタのリストを表示します。

show counters description

プロトコル スタック カウンタの説明を表示するには、特権 EXEC モードで **show counters description** コマンドを使用します。

show counters description

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

例

次に、**show counters description** コマンドの出力例を示します。

```
hostname# show counters description
Protocol     Counter              Description
NPCP         IN_PKTS              Packets from network processors
NPCP         OUT_PKTS             Packets to network processors
NPCP         DROP_LIMIT1          Gigamac packets dropped due to IP protocol que
ue limiter
NPCP         DROP_LIMIT2          Gigamac packets dropped due to ARP protocol qu
eue limiter
NPCP         DROP_LIMIT3          Gigamac packets dropped due to Fixup queue lim
iter
...
```

関連コマンド

コマンド	説明
clear counters	プロトコル スタック カウンタをクリアします。
show counters	プロトコル スタック カウンタを表示します。

show cpu

CPU の使用状況に関する情報を表示するには、特権 EXEC モードで **show cpu usage** コマンドを使用します。

show cpu [**usage**]

マルチ コンテキスト モードで、システム コンフィギュレーションから次のように入力します。

show cpu [**usage**] [**context** {**all** | *context_name*}]

シンタックスの説明

all	すべてのコンテキストを表示するように指定します。
context	特定のコンテキストを表示するように指定します。
context_name	表示するコンテキスト名を指定します。
usage	（任意）CPU 使用率を表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

CPU 使用率は 5 秒ごとの負荷の近似値を使用し、さらに、以降の 2 つの移動平均にこの近似値を適用して計算されます。

show cpu コマンドを使用すると、プロセスに関連する負荷を検出できます（シングルモードで、およびシステム コンフィギュレーションからマルチ コンテキスト モードで、***show process*** コマンドを実行した場合に表示される項目の代わりに、アクティビティが表示されます）。

さらに、マルチ コンテキスト モードの場合は、プロセス関連負荷を分散するよう、設定されたすべてのコンテキストで消費される CPU に要求できます。そのためには、各コンテキストに切り替えて ***show cpu*** コマンドを入力するか、このコマンドの ***show cpu context*** 形式を入力します。

プロセス関連負荷は最も近い整数に丸められますが、コンテキスト関連負荷には精度を表す 10 進数が 1 つ追加されます。たとえば、システム コンテキストから ***show cpu*** を入力すると、***show cpu context system*** コマンドを入力した場合と異なる値が生成されます。***show cpu*** は ***show cpu context all*** のサマリーとほぼ同じですが、***show cpu context system*** はこのサマリーの一部にすぎません。

例

次に、CPU 使用率を表示する例を示します。

```
hostname# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

次に、マルチ モードでシステム コンテキストの CPU 使用率を表示する例を示します。

```
hostname# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

次に、すべてのコンテキストの CPU 使用率を表示する例を示します。

```
hostname# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

次に、コンテキスト [one] の CPU 使用率を表示する例を示します。

```
hostname/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。

show crashinfo

フラッシュ メモリに格納されたクラッシュ ファイルの内容を表示するには、特権 EXEC モードで ***show crashinfo*** コマンドを入力します。

show crashinfo [**save**]

シンタックスの説明

save	(任意) フラッシュ メモリにクラッシュ情報を保存するように FWSM が設定されているかどうかを表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
3.1	このコマンドが追加されました。

使用上のガイドライン

クラッシュ ファイルがテスト クラッシュ（**crashinfo test** コマンド）によって生成された場合、クラッシュ ファイルの最初の文字列は [`: Saved_Test_Crash`]、最後の文字列は [`: End_Test_Crash`] です。クラッシュ ファイルが実際のクラッシュによって生成された場合、クラッシュ ファイルの最初の文字列は [`: Saved_Crash`]、最後の文字列は [`: End_Crash`] です（このファイルには、**crashinfo force page-fault** または **crashinfo force watchdog** コマンドを使用した場合のクラッシュも含まれます）。

フラッシュ内にクラッシュ データが保存されていない場合、または **clear crashinfo** コマンドを入力してクラッシュ データを消去した場合は、**show crashinfo** コマンドを実行すると、エラー メッセージが表示されます。

例

次に、現在のクラッシュ情報設定を表示する例を示します。

```
hostname# show crashinfo save
crashinfo save enable
```

次に、クラッシュ ファイル test の出力例を示します（ただし、このテストでは FWSM を実際にクラッシュしません。シミュレートされたサンプル ファイルが作成されます）。

```
hostname(config)# crashinfo test
hostname(config)# exit
hostname# show crashinfo
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)

Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
```

```
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
```

```
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
```

```
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008

Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X

Compiled on Fri 15-Nov-04 14:35 by root

hostname up 10 days 0 hours

Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2004

------------------ show memory ------------------

Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used
```

```
------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3792/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 PIX Garbage Collecr
```

```
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0       4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48        120 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc         10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
```

```
Xlates                0/s           0/s
Connections           0/s           0/s
TCP Conns             0/s           0/s
UDP Conns             0/s           0/s
URL Access            0/s           0/s
URL Server Req        0/s           0/s
TCP Fixup             0/s           0/s
TCPIntercept          0/s           0/s
HTTP Fixup            0/s           0/s
FTP Fixup             0/s           0/s
AAA Authen            0/s           0/s
AAA Author            0/s           0/s
AAA Account           0/s           0/s
: End_Test_Crash
```

関連コマンド

コマンド	説明
clear crashinfo	クラッシュ ファイルの内容を削除します。
crashinfo force	FWSM を強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリへのクラッシュ情報の書き込みを禁止します。
crashinfo test	フラッシュ メモリ内のファイルにクラッシュ情報を保存する FWSM の機能をテストします。

show crypto accelerator statistics

ハードウェアの暗号アクセラレータ MIB（管理情報ベース）から、グローバル統計情報およびアクセラレータ固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto accelerator statistics** コマンドを使用します。

show crypto accelerator statistics

シンタックスの説明

このコマンドには、キーワードまたは変数はありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、暗号アクセラレータのグローバル統計情報を表示する例を示します。

```
hostname # show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
```

```
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                            Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                            SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                            IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
      Keys generated: 97
      Secret keys derived: 1
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
```

```
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 1
      Random number request failures: 0
hostname #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB のグローバル統計情報およびアクセラレータ固有の統計情報を消去します。
clear crypto protocol statistics	暗号アクセラレータ MIB のプロトコル固有の統計情報を消去します。
show crypto protocol statistics	暗号アクセラレータ MIB のプロトコル固有の統計情報を表示します。

show crypto ca certificates

特定のトラストポイントに対応付けられた証明書、またはシステムに導入されたすべての証明書を表示するには、特権 EXEC モードで **show crypto ca certificates** コマンドを使用します。

show crypto ca certificates [*trustpointname*]

シンタックスの説明

trustpointname	（任意）トラストポイントの名前を指定します。名前を指定しない場合は、システムに導入されたすべての証明書が表示されます。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、トラストポイント tp1 の CA 証明書を表示する例を示します。

```
hostname# show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = a@b.com
    CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
    Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
    Associated Trustpoints: tp2 tp1
hostname#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定したトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定したトラストポイントの設定パラメータに基づいて CRL を要求します。
crypto ca enroll	CA による登録プロセスを開始します。
crypto ca import	指定したトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定したトランスポートでトラストポイント モードを開始します。

show crypto ca crls

キャッシュ内のすべての CRL を表示するか、または指定したトラストポイントに対応するキャッシュ内のすべての CRL を表示するには、特権 EXEC モードで **show crypto ca crls** コマンドを使用します。

show crypto ca crls [*trustpointname*]

シンタックスの説明

trustpointname	（任意）トラストポイントの名前を指定します。名前を指定しない場合は、システムのキャッシュ内にあるすべての CRL が表示されます。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、トラストポイント tp1 の CRL を表示する例を示します。

```
hostname# show crypto ca crls tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@cisco.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定したトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定したトラストポイントの設定パラメータに基づいて CRL を要求します。
crypto ca enroll	CA による登録プロセスを開始します。
crypto ca import	指定したトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定したトランスポートでトラストポイント モードを開始します。

show crypto ipsec df-bit

指定したインターフェイスの IPSec パケットに対する IPSec DF ビット ポリシーを表示するには、グローバル コンフィギュレーション モードおよび特権 EXEC モードで **show crypto ipsec df-bit** コマンドを使用します。

show crypto ipsec df-bit *interface*

シンタックスの説明

interface	インターフェイス名を指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。
3.1(1)	このコマンドは **show crypto ipsec** から変更されました。

例

次に、インターフェイス inside の IPSec DF ビット ポリシーを表示する例を示します。

```
hostname(config)# show crypto ipsec df-bit inside
df-bit inside copy
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPSec パケットの IPSec DF ビット ポリシーを設定します。
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを表示します。

show crypto ipsec fragmentation

IPSec パケットのフラグメンテーション ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec fragmentation** コマンドを使用します。

show crypto ipsec fragmentation *interface*

シンタックスの説明

interface	インターフェイス名を指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。
3.1(1)	このコマンドは **show crypto ipsec** から変更されました。

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、インターフェイス inside の IPSec フラグメンテーション ポリシーを表示する例を示します。

```
hostname(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
crypto ipsec df-bit	IPSec パケットの DF ビット ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show crypto key mypubkey

指定したタイプの鍵ペアを表示するには、特権 EXEC モードで **show crypto key mypubkey** コマンドを使用します。

show crypto key mypubkey {***rsa*** | ***dsa***}

シンタックスの説明

dsa	DSA 鍵ペアを表示します。
rsa	RSA 鍵ペアを表示します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、RSA 鍵ペアを表示する例を示します。

```
hostname(config)# show crypto key mypubkey rsa
...
```

関連コマンド

コマンド	説明
crypto key generate dsa	DSA 鍵ペアを生成します。
crypto key generate rsa	RSA 鍵ペアを生成します。
crypto key zeroize	指定したタイプの鍵ペアをすべて削除します。

show crypto protocol statistics

暗号アクセラレータ MIB（管理情報ベース）にあるプロトコル固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto protocol statistics** コマンドを使用します。

show crypto protocol statistics *protocol*

シンタックスの説明

protocol	統計情報を表示するプロトコルの名前を指定します。選択できるプロトコルは、次のとおりです。 ***ikev1* —** Internet Key Exchange バージョン 1 ***ipsec* —** IP Security Phase-2 プロトコル ***ssl* —** Secure Socket Layer ***other* —** 新しいプロトコル用 ***all* —** 現在サポートされているすべてのプロトコル

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、指定したプロトコルの暗号アクセラレータ統計情報を表示する例を示します。

```
hostname # show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
   SA rekey requests: 3
    SA deletion requests: 2
   Next phase key allocation requests: 2
   Random number generation requests: 0
    Failed requests: 0
```

```
hostname # show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics ssl
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0

hostname # show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
    SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
    Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
```

```
   Encapsulate packet requests: 700
    Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
    HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
hostname #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB のグローバル統計情報およびアクセラレータ固有の統計情報を消去します。
clear crypto protocol statistics	暗号アクセラレータ MIB のプロトコル固有の統計情報を消去します。
show crypto accelerator statistics	暗号アクセラレータ MIB のグローバル統計情報およびアクセラレータ固有の統計情報を表示します。

show ctiqbe

FWSM に確立された CTIQBE セッションに関する情報を表示するには、特権 EXEC モードで **show ctiqbe** コマンドを使用します。

show ctiqbe

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

show ctiqbe コマンドは、FWSM に確立された CTIQBE セッションの情報を表示します。CTIQBE インスペクション エンジンに関する問題のトラブルシューティングを行う場合は、このコマンドと **debug ctiqbe** および **show local-host** コマンドを組み合わせて使用します。

（注） **pager** コマンドを設定してから、**show ctiqbe** コマンドを使用することを推奨します。多数の CTIQBE セッションが存在する場合に **pager** コマンドが設定されていないと、**show ctiqbe** コマンド出力が終了するまでに時間がかかることがあります。

例

次に、以下の条件における **show ctiqbe** コマンドの出力例を示します。FWSM にアクティブな CTIQBE セッションが 1 つだけ設定されています。このセッションは、ローカル アドレスが 10.0.0.99 の内部 CTI デバイス（Cisco IP SoftPhone など）とアドレスが 172.29.1.77 の外部 Cisco CallManager との間に確立されています。TCP ポート 2748 は Cisco CallManager です。セッションのハートビート インターバルは 120 秒です。

```
hostname# show ctiqbe

Total: 1
LOCAL           FOREIGN          STATE HEARTBEAT
-------------------------------------------------------------
1 10.0.0.99/1117 172.29.1.77/2748 1     120
  RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 1029)
  MEDIA: Device ID 27   Call ID 0
  Foreign 172.29.1.99   (1028 1029)
  Local   172.29.1.88   (26822 26823)
  ------------------------------------------------
```

CallManager には CTI デバイスがすでに登録されています。デバイス内部アドレスおよび RTP 待ち受けポートは 172.29.1.99 の UDP ポート 1028 に PAT（ポート アドレス変換）されます。RTCP 待ち受けポートは UDP 1029 に PAT されます。

RTP/RTCP:PAT xlates: で開始する行が表示されるのは、外部 CallManager に内部 CTI デバイスが登録されていて、CTI デバイスのアドレスおよびポートがこの外部インターフェイスに PAT される場合のみです。CallManager が内部インターフェイス上にある場合、または内部 CTI デバイスのアドレスおよびポートが CallManager で使用されるのと同じ外部インターフェイスに NAT（ネットワーク アドレス変換）される場合は、この行が表示されません。

出力は、この CTI デバイスと 172.29.1.88 にある別の Phone との間にコールが確立されたことを示します。その他の Phone の RTP および RTCP 待ち受けポートは UDP 26822 および 26823 です。FWSM には別の Phone や CallManager に関連した CTIQBE セッション レコードが保持されないため、その他の Phone は CallManager と同じインターフェイスに接続されます。CTI デバイス側のアクティブなコール レッグは、Device ID 27 および Call ID 0 で識別できます。

次に、これらの CTIQBE 接続の xlate 情報を示します。

```
hostname# show xlate debug
3 in use, 3 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect ctiqbe	CTIQBE アプリケーション検査をイネーブルにします。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。
show conn	各接続タイプの接続状態を表示します。
timeout	各プロトコルおよびセッション タイプの最大アイドル時間を設定します。

show curpriv

現在のユーザ権限を表示するには、**show curpriv** コマンドを使用します。

show curpriv

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•
特権 EXEC	•	•	—	—	•
ユーザ	•	•	—	—	•

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

show curpriv コマンドは、現在の特権レベルを表示します。特権レベルは値が小さいほど、レベルが低くなります。

例

次に、enable_15 という名のユーザに複数の特権レベルが設定されている場合の **show curpriv** コマンドの出力例を示します。ユーザ名はユーザがログインするときに入力した名前、P_PRIV はユーザが **enable** コマンドを入力したこと、P_CONF はユーザが **config terminal** コマンドを入力したことを示します。

```
hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド ステートメントを削除します。
show running-config privilege	コマンドの特権レベルを表示します。