



## show u ~ show z

---

- [show uauth](#) (3 ページ)
- [show url-block](#) (6 ページ)
- [show url-cache statistics](#) (8 ページ)
- [show url-server](#) (10 ページ)
- [show user-alert](#) (13 ページ)
- [show user-identity ad-agent](#) (14 ページ)
- [show user-identity ad-group-members](#) (17 ページ)
- [show user-identity ad-groups](#) (19 ページ)
- [show user-identity ad-users](#) (21 ページ)
- [show user-identity group](#) (23 ページ)
- [show user-identity ip-of-user](#) (25 ページ)
- [show user-identity memory](#) (27 ページ)
- [show user-identity statistics](#) (29 ページ)
- [show user-identity statistics top user](#) (31 ページ)
- [show user-identity user active](#) (33 ページ)
- [show user-identity user all](#) (37 ページ)
- [show user-identity user inactive](#) (39 ページ)
- [show user-identity user-not-found](#) (41 ページ)
- [show user-identity user-of-group](#) (43 ページ)
- [show user-identity user-of-ip](#) (45 ページ)
- [show version](#) (47 ページ)
- [show vlan](#) (51 ページ)
- [show vm](#) (53 ページ)
- [show vni vlan-mapping](#) (55 ページ)
- [show vpdn](#) (57 ページ)
- [show vpn cluster stats internal](#) (59 ページ)
- [show vpn load-balancing](#) (60 ページ)
- [show vpn-sessiondb](#) (63 ページ)
- [show vpn-sessiondb ratio](#) (78 ページ)

- [show vpn-sessiondb summary](#) (81 ページ)
- [show wccp](#) (86 ページ)
- [show webvpn anyconnect](#) (88 ページ)
- [show webvpn anyconnect external-browser-pkg](#) (90 ページ)
- [show webvpn csd \(廃止\)](#) (92 ページ)
- [show webvpn debug-condition](#) (95 ページ)
- [show webvpn group-alias](#) (96 ページ)
- [show webvpn group-url](#) (98 ページ)
- [show webvpn hostscan](#) (100 ページ)
- [show webvpn hsts](#) (102 ページ)
- [show webvpn kcd](#) (103 ページ)
- [show webvpn mus](#) (105 ページ)
- [show webvpn saml](#) (106 ページ)
- [show webvpn sso-server \(廃止\)](#) (107 ページ)
- [show webvpn statistics](#) (110 ページ)
- [show xlate](#) (112 ページ)
- [show zone](#) (115 ページ)

## show uauth

現在認証済みの1名またはすべてのユーザー、ユーザーがバインドされているホストIP、およびキャッシュされたIPとポートの認可情報を表示するには、特権 EXEC モードで **show uauth** コマンドを使用します。

**show uauth** [ *username* ]

### 構文の説明

*username* (任意) 表示するユーザー認証情報とユーザー認可情報をユーザー名で指定します。

### コマンドデフォルト

ユーザー名を省略すると、すべてのユーザーの認可情報が表示されます。

### 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。

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

### コマンド履歴

リリース 変更内容

7.0(1) このコマンドが追加されました。

7.2(1) アイドル時間が出力に追加されました。

7.2(2) アイドル時間が出力から削除されました。

### 使用上のガイドライン

**show uauth** コマンドは、1名またはすべてのユーザーのAAA認可キャッシュおよび認証キャッシュを表示します。

このコマンドは、**timeout** コマンドとともに使用します。

各ユーザーホストのIPアドレスには、認可キャッシュが付加されます。このキャッシュでは、ユーザーホストごとに16個までのアドレスとサービスのペアが許可されます。正しいホストからキャッシュされているサービスにユーザーがアクセスしようとした場合、ASAではそのアクセスが事前に許可されていると見なし、その接続を即座に代理します。あるWebサイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、イメージごとに認可サーバーと通信しません（イメージが同じIPアドレスからであると想定されます）。この処理により、パフォーマンスが大幅に向上され、認可サーバーの負荷が削減されます。

**show uauth** コマンドの出力には、認証と認可のために認可サーバーに渡されたユーザー名、そのユーザー名がバインドされている IP アドレス、およびこのユーザーが認証されたのみであるか、または、キャッシュされたサービスがあるかが表示されます。



- (注) Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル (**show uauth** コマンドで表示できます) に追加されます。ただし、ネットワーク拡張モードで Easy VPN Remote 機能とともに Xauth を使用すると、ネットワーク間に IPsec トンネルが作成されるため、ファイアウォールの向こう側にいるユーザーを 1 つの IP アドレスに関連付けることができません。したがって、Xauth の完了時に uauth エントリが作成されません。AAA 認可またはアカウントサービスが必要となる場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの向こう側にいるユーザーを認証します。AAA 認証プロキシの詳細については、**aaa** コマンドを参照してください。

ユーザーの接続がアイドルになった後にキャッシュを保持する期間を指定するには、**timeout uauth** コマンドを使用します。すべてのユーザーのすべての認可キャッシュを削除するには、**clear uauth** コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

## 例

次に、いずれのユーザーも認証されておらず、かつ、1 つのユーザー認証が進行している場合の **show uauth** コマンドの出力例を示します。

```
ciscoasa(config)# show uauth

Authenticated Users      Current      Most Seen
Authen In Progress       0            1
user 'v039294' at 136.131.178.4, authenticated (idle for 0:00:00)
  access-list #ACSACL#-IP-v039294-521b0b8b (*)
  absolute timeout: 0:00:00
  inactivity timeout: 0:05:00
```

次に、3 人のユーザーが認証されており、かつ、ASA を介してサービスを使用することが認可されている場合の **show uauth** コマンドの出力例を示します。

```
ciscoasa(config)# show uauth
user 'pat' from 209.165.201.2 authenticated
user 'robin' from 209.165.201.4 authorized to:
  port 192.168.67.34/telnet                               192.168.67.11/http
  192.168.67.33/tcp/8001                                  192.168.67.56/tcp/25
  192.168.67.42/ftp
user 'terry' from 209.165.201.7 authorized to:
  port 192.168.1.50/http
209.165.201.8/http
```

## 関連コマンド

コマンド	説明
<b>clear uauth</b>	現在のユーザーの認証情報と認可情報を削除します。

コマンド	説明
<b>timeout</b>	アイドル時間の最大継続期間を設定します。

# show url-block

url-blockバッファに保持されているパケット数と、バッファ上限を超えたか再送信のためにドロップされたパケット数（ある場合）を表示するには、特権 EXEC モードで **show url-block** コマンドを使用します。

## show url-block [ block statistics ]

### 構文の説明

**blockstatistics** (任意) ブロックバッファの使用状況に関する統計情報を表示します。

### コマンド デフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリース 変更内容  
ス

7.0(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 url-block block statistics** コマンドは、URL ブロックバッファに保持されているパケット数と、バッファ上限を超えたか再送信のためにドロップされたパケット数（ある場合）を表示します。

### 例

次に、**show url-block** コマンドの出力例を示します。

```
ciscoasa# show url-block
| url-block url-mempool 128 | url-block url-size 4 | url-block block 128
```

URL ブロック バッファのコンフィギュレーションが表示されています。

次に、**show url-block block statistics** コマンドの出力例を示します。

```
ciscoasa# show url-block block statistics
URL Pending Packet Buffer Stats with max block 128 |
Cumulative number of packets held: | 896
Maximum number of packets held (per URL): | 3
Current number of packets held (global): | 38
```

```
Packets dropped due to
| exceeding url-block buffer limit: | 7546
| HTTP server retransmission: | 10
Number of packets released back to client: | 0
```

## 関連コマンド

コマンド	説明
<b>clear url-block block statistics</b>	ブロック バッファの使用状況カウンタをクリアします。
<b>filter url</b>	トラフィックを URL フィルタリング サーバーに送ります。
<b>url-block</b>	Web サーバーの応答に使用される URL バッファを管理します。
<b>url-cache</b>	N2H2 サーバーまたは Websense サーバーからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
<b>url-server</b>	filter コマンドで使用する N2H2 サーバーまたは Websense サーバーを指定します。

## show url-cache statistics

N2H2 または Websense のフィルタリングサーバーから受信した URL 応答に使用される URL キャッシュの情報を表示するには、特権 EXEC モードで **show url-cache statistics** コマンドを使用します。

### show url-cache statistics

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンド デフォルト

デフォルトの動作や値はありません。

#### 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。

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

#### コマンド履歴

リリース 変更内容  
7.0(1) このコマンドが追加されました。

7.0(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 url-cache statistics** コマンドには、次のエントリが表示されます。

- Size : キャッシュサイズ (KB 単位)。**url-cache size** オプションを使用して設定します。
- Entries : キャッシュ サイズに基づくキャッシュ エントリの最大数。
- In Use : キャッシュに含まれる現在のエントリ数。
- Lookups : ASA がキャッシュエントリを検索した回数。
- Hits : ASA がキャッシュ内でエントリを検出した回数。

**show perfmon** コマンドを使用すると、N2H2 Sentian または Websense のフィルタリング アクティビティに関する追加情報を表示できます。

#### 例

次に、**show url-cache statistics** コマンドの出力例を示します。

```
ciscoasa# show url-cache statistics
URL Filter Cache Stats
-----
|
```



```

Size :                               1KB
Entries :                               36
      In Use :                               30
Lookups :                               300
|
Hits :                               290

```

---

 関連コマンド

コマンド	説明
<b>clear url-cache statistics</b>	コンフィギュレーションから <b>url-cache</b> コマンド ステートメントを削除します。
<b>filter url</b>	トラフィックを URL フィルタリング サーバーに送ります。
<b>url-block</b>	Web サーバーの応答に使用される URL バッファを管理します。
<b>url-cache</b>	N2H2 サーバーまたは Websense サーバーから受信した応答の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
<b>url-server</b>	<b>filter</b> コマンドで使用する N2H2 サーバーまたは Websense サーバーを指定します。

# show url-server

URLフィルタリングサーバーに関する情報を表示するには、特権EXECモードで**show url-server** コマンドを使用します。

## show url-server statistics

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンド デフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリー 変更内容  
ス

7.0(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 url-server statistics** コマンドは、URL サーバーのベンダーおよびステータスを表示します。また、URL、HTTPS 接続、および TCP 接続について、合計数、許可された数、拒否された数を表示します。

**show url-server** コマンドには、次の情報が表示されます。

- N2H2 の場合：**url-server (if\_name)vendor n2h2host local\_ip port number timeout seconds protocol [{TCP | UDP} {version 1 | 4}]**
- Websense の場合：**url-server (if\_name)vendor websense host local\_ip timeout seconds protocol [{TCP | UDP}]**

### 例

次に、**show url-server statistics** コマンドの出力例を示します。

```
ciscoasa## show url-server statistics
Global Statistics:
-----
URLs total/allowed/denied          994387/155648/838739
URLs allowed by cache/server       70483/85165
URLs denied by cache/server        801920/36819
HTTPSs total/allowed/denied       994387/155648/838739
HTTPs allowed by cache/server      70483/85165
```

```

HTTPs denied by cache/server      801920/36819
FTP's total/allowed/denied        994387/155648/838739
FTP's allowed by cache/server     70483/85165
FTP's denied by cache/server      801920/36819
Requests dropped                   28715
Server timeouts/retries           567/1350
Processed rate average 60s/300s   1524/1344 requests/second
Denied rate average 60s/300s     35648/33022 requests/second
Dropped rate average 60s/300s    156/189 requests/second
URL Server Statistics:
-----
192.168.0.1                        UP
Vendor                             websense
Port                               17035
Requests total/allowed/denied     366519/255495/110457
Server timeouts/retries           567/1350
Responses received                 365952
Response time average 60s/300s    2/1 seconds/request
192.168.0.2                        DOWN
Vendor                             websense
Port                               17035
Requests total/allowed/denied     0/0/0
Server timeouts/retries           0/0
Responses received                 0
Response time average 60s/300s    0/0 seconds/request
. . .
URL Packets Sent and Received Stats:
-----
Message                            Sent    Received
STATUS_REQUEST                     411     0
LOOKUP_REQUEST                     366519 365952
LOG_REQUEST                         0       NA
Errors:
-----
RFC noncompliant GET method        0
URL buffer update failure          0
Semantics:
This command allows the operator to display url-server statistics organized on a global
and per-server basis. The output is reformatted to provide: more-detailed information
and per-server organization.
Supported Modes:
privileged
router || transparent
single || multi/context
Privilege:
ATTR_ES_CHECK_CONTEXT
Debug support:
N/A
Migration Strategy (if any):
N/A

```

## 関連コマンド

コマンド	説明
<b>clear url-server</b>	URL フィルタリング サーバーの統計情報をクリアします。
<b>filter url</b>	トラフィックを URL フィルタリング サーバーに送ります。
<b>url-block</b>	Web サーバーの応答に使用される URL バッファを管理します。

コマンド	説明
<b>url-cache</b>	N2H2 サーバーまたは Websense サーバーからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
<b>url-server</b>	filter コマンドで使用する N2H2 サーバーまたは Websense サーバーを指定します。

## show user-alert

すべてのアクティブなクライアントレス WebVPN セッションに対して表示できる、現在設定されているユーザーアラートを表示するには、特権 EXEC モードで show user-alert コマンドを使用します。

### show user-alert

**コマンドデフォルト** デフォルトの動作や値はありません。

**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。

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

**コマンド履歴** リリース 変更内容

8.4(2) コマンドが追加されました。

**関連コマンド**

コマンド	説明
<b>user-alert</b>	現在のアクティブセッションのすべてのクライアントレス SSL VPN ユーザーに対する緊急メッセージのブロードキャストをイネーブルにします。

# show user-identity ad-agent

アイデンティティファイアウォールのADエージェントに関する情報を表示するには、特権 EXEC モードで **show user-identity ad-agent** コマンドを使用します。

**show user-identity ad-agent [ statistics ]**

## 構文の説明

**statistics** (オプション) ADエージェントに関する統計情報を表示します。

## コマンドデフォルト

デフォルトの動作や値はありません。

## 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。

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

## コマンド履歴

リリー 変更内容  
ス

8.4(2) コマンドが追加されました。

## 使用上のガイドライン

アイデンティティファイアウォールのADエージェントコンポーネントをモニターできます。

AD エージェントのトラブルシューティング情報を取得するには、**show user-identity ad-agent** コマンドを使用します。このコマンドは、プライマリ AD エージェントおよびセカンダリ AD エージェントに関する次の情報を表示します。

- AD エージェントのステータス
- ドメインのステータス
- AD エージェントの統計情報

表 1: コマンド出力の説明

タイプ	値	説明
[モード (Mode) ]	コンフィギュレーションモード	フルダウンロードまたはオンデマンドダウンロードを指定します。

タイプ	値	説明
AD Agent IP Address	IP address	アクティブな AD エージェントの IP アドレスを表示します。
バックアップ	IP address	バックアップの AD エージェントの IP アドレスを表示します。
AD Agent Status	<ul style="list-style-type: none"> <li>• ディセーブル</li> <li>• Down</li> <li>• Up (registered)</li> <li>• Probing</li> </ul>	<ul style="list-style-type: none"> <li>• アイデンティティ ファイアウォールはディセーブルです。</li> <li>• AD エージェントはダウンしています。</li> <li>• AD エージェントは稼働しています。</li> <li>• ASA は登録され、AD エージェントが稼働しています。</li> <li>• ASA は AD エージェントに接続しようとしています。</li> </ul>
Authentication Port	udp/1645	AD エージェントの認証ポートを表示します。
Accounting Port	udp/1646	AD エージェントのアカウントング ポートを表示します。
ASA Listening Port	udp/3799	ASA リスニング ポートを表示します。
インターフェイス	インターフェイス	AD エージェントと通信するために ASA が使用するインターフェイスを表示します。
IP Address	IP address	AD エージェントと通信するために ASA が使用する IP アドレスを表示します。
Uptime	時刻	AD エージェントのアップタイムを表示します。
Average RTT	ミリ秒	AD エージェントと通信するために ASA を使用する平均ラウンドトリップ時間を表示します。
ドメイン (Domain)	ドメイン ニックネーム Status: up Status: down	AD エージェントの Microsoft Active Directory ドメインを表示します。

## 例

次に、アイデンティティ ファイアウォールの AD エージェントの情報を表示する例を示します。

```
ciscoasa# show user-identity ad-agent
```

## show user-identity ad-agent

```

Primary AD Agent:
  Status                up (registered)
  Mode                  full-download
  IP address:          172.23.62.125
  Authentication port:  udp/1645
  Accounting port:     udp/1646
  ASA Listening port:   udp/3799
  Interface:           mgmt
  Up time:              15 mins 41 secs
  Average RTT:         57 msec
Secondary AD Agent:
  Status                up
  Mode                  full-download
  IP address:          172.23.62.136
  Authentication port:  udp/1645
  Accounting port:     udp/1646
  ASA Listening port:   udp/3799
  Interface:           mgmt
  Up time:              7 mins 56 secs
  Avg RTT:             15 msec

```

## 関連コマンド

コマンド	説明
<b>clear user-identity ad-agent statistics</b>	アイデンティティ ファイアウォールの ASA によって保持されている AD エージェントの統計データをクリアします。
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。
<b>show user-identity ad-group-members</b>	アイデンティティファイアウォールの AD エージェントのドメインにあるグループ メンバーを表示します。



## show user-identity ad-group-members

アイデンティティファイアウォールの AD エージェント のドメインにあるグループメンバーを表示するには、特権 EXEC モードで **show user-identity ad-group-members** コマンドを使用します。

**show user-identity ad-group-members** [ *domain\_nickname* \ ] *user\_group\_name* [ **timeout seconds** *seconds* ]

### 構文の説明

*domain\_nickname* (オプション) アイデンティティファイアウォールのドメイン名を指定します。

**timeout seconds** 秒 (オプション) グループメンバーの統計情報を取得するタイマーを設定して、タイマーの期間を指定します。

*user\_group\_name* (オプション) 統計情報を取得するグループ名を指定します。

### コマンドデフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリー 変更内容  
ス

8.4(2) コマンドが追加されました。

### 使用上のガイドライン

**show user-identity ad-group-members** コマンドは、指定したユーザーグループの直近メンバー (ユーザーとグループ) を表示します。



- (注) このコマンドでは、**object-group user** コマンドを使用して設定された、ASA 上のローカルに定義されたグループの情報は表示されません。

ASA は、Active Directory サーバーで設定された Active Directory グループに対する LDAP クエリーを送信します。このコマンドを実行することは、指定したユーザーグループのメンバーをチェックできる LDAP ブラウザ コマンドを実行することと同等です。ASA は、1 つのレベル

のLDAPクエリを発行して、`distinguishedName`形式で指定したグループの直近メンバーを取得します。このコマンドを実行しても、インポートされたユーザーグループのASA内部キャッシュは更新されません。

`domain_nickname`を指定しない場合、ASAはデフォルトドメインに`user_group_name`があるグループの情報を表示します。`domain_nickname`引数には、実際のドメインニックネームまたはLOCALを指定できます。

グループ名は、CN名ではなくADグループの一意のsAMAccountNameになります。特定グループのsAMAccountNameの情報を表示するには、**show user-identity ad-groups filter** `filter_string` コマンドを使用して、グループのsAMAccountNameを取得します。

## 例

次に、アイデンティティファイアウォールのグループ `sample1` のメンバーを表示する例を示します。

```
ciscoasa# show user-identity ad-group-member group.sample1
Domain:CSCO          AAA Server Group:  CISCO_AD_SERVER
Group Member List Retrieved Successfully
Number of Members in AD Group group.schiang: 12
dn: CN=user1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
dn: CN=user2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
...
```

## 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。
<b>show user-identity ad-groups</b>	アイデンティティファイアウォールのADエージェントに関する情報を表示します。

## show user-identity ad-groups

アイデンティティファイアウォールの特定グループに関する情報を表示するには、特権 EXEC モードで **show user-identity ad-groups** コマンドを使用します。

```
show user-identity ad-groups domain_nickname { filter filter_string | import-user-group [ count ] }
```

### 構文の説明

**count** (オプション) アクティブ化されたグループの数を表示します。

**domain\_nickname** アイデンティティファイアウォールのドメイン名を指定します。

**filter filter\_string** Microsoft Active Directory のドメインコントローラの CN 属性に、指定したフィルタ文字列が含まれるグループを表示するように指定します。

**import-user-group** アイデンティティファイアウォールのアクティブ化されたグループのみを表示します。

### コマンドデフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリース 変更内容  
ス

8.4(2) コマンドが追加されました。

### 使用上のガイドライン

**show user-identity ad-groups** コマンドを実行する場合、ASA は Microsoft Active Directory に LDAP クエリーを送信し、指定したドメインニックネームに含まれるすべてのユーザーグループを取得します。*domain\_nickname* 引数には、実際のドメインニックネームまたは LOCAL を指定できます。ASA は、グループオブジェクトクラス属性を持つグループのみを取得します。ASA は、取得したグループを *distinguishedName* 形式で表示します。

**filter filter\_string** キーワードおよび引数を指定する場合、ASA は指定したフィルタ文字列をドメインコントローラの CN 属性に含むグループを表示します。**access-list** および **object-group** コマンドは sAMAccountName のみを取得するため、**show user-identity ad-users filter filter\_string**

コマンドを実行してグループの sAMAccountName を取得できます。filter filter\_string を指定しない場合、ASA はすべての Active Directory グループを表示します。

**import-user-group count** キーワードを指定している場合、ASA はアクティブ化され（アクセスグループ、インポートユーザーグループ、またはサービス ポリシー コンフィギュレーションの一部であるため）、ローカルデータベースに保存されているすべての Active Directory グループを表示します。ASA は、グループの sAMAccountName のみを表示します。

## 例

次に、アイデンティティファイアウォールに指定したドメインニックネームに含まれるユーザー グループを表示する例を示します。

```
ciscoasa# show user-identity ad-groups CSCO filter sampleuser1
Domain: CSCO      AAA Server Group:      CISCO_AD_SERVER
Group list retrieved successfully
Number of Active Directory Groups      6
dn: CN=group.reg.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.reg.sampleuser1
dn: CN=group.temp.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.temp.sampleuser1
...
ciscoasa# show user-identity ad-groups CSCO import-user-group count
Total AD groups in domain CSCO stored in local: 2
ciscoasa# show user-identity ad-groups CSCO import-user-group

Domain: CSCO
Groups:
    group.SampleGroup1
    group.SampleGroup2
...
```

次に、コマンドを実行して、access-list コマンドおよび object-group コマンドから結果にフィルタ文字列を適用する例を示します。show user-identity ad-users CSCO filter SampleGroup1 コマンドを実行すると、指定した文字列の sAMAccountName が取得されます。

```
ciscoasa# show user-identity ad-users CSCO filter SampleGroup1

Domain:CSCO      AAA Server Group:      CISCO_AD_SERVER
User list retrieved successfully
Number of Active Directory Users: 2
dn: CN=SampleUser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: SampleUser2
dn: CN=SAMPLEUSER2-WXP05,OU=Workstations,OU=Cisco Computers,DC=cisco,DC=com
sAMAccountName: SAMPLEUSER2-WXP05$
```

## 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。

## show user-identity ad-users

アイデンティティ ファイアウォールの Microsoft Active Directory ユーザーを表示するには、特権 EXEC モードで **show user-identity ad-users** コマンドを使用します。

**show user-identity ad-users** *domain\_nickname* [ **filter** *filter\_string* ]

### 構文の説明

*domain\_nickname* アイデンティティ ファイアウォールのドメイン名を指定します。

**filter** (オプション) Microsoft Active Directory のドメイン コントローラの CN 属性に、指定したフィルタ文字列が含まれるユーザーを表示するように指定します。  
*filter\_string*

### コマンドデフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリー 変更内容  
ス

8.4(2) コマンドが追加されました。

### 使用上のガイドライン

**show user-identity ad-users** コマンドを実行すると、ASA は Microsoft Active Directory に LDAP クエリーを送信し、指定したドメインニックネームに含まれるすべてのユーザーを取得します。*domain\_nickname* 引数には、実際のドメインニックネームまたは LOCAL を指定できます。

**filter** *filter\_string* キーワードおよび引数を指定すると、ASA は指定したフィルタ文字列をドメインコントローラの CN 属性に含むユーザーを表示します。ASA は、Active Directory サーバーで設定された Active Directory グループに対する LDAP クエリーを送信します。

ASA は、ユーザー オブジェクトクラス属性と `samAccountType` 属性 805306368 を持つユーザーのみを取得します。マシン オブジェクトなどの他のオブジェクトは、ユーザー オブジェクトクラスに含まれることがありますが、`samAccountType` 805306368 は非ユーザー オブジェクトを除外します。フィルタ文字列を指定しない場合、ASA はすべての Active Directory ユーザーを表示します。

ASA は、取得したユーザーを `distinguishedName` 形式で表示します。

## 例

次に、アイデンティティファイアウォールの Active Directory ユーザーに関する情報を表示する例を示します。

```
ciscoasa# show user-identity ad-users CSCO filter user
Domain: CSCO          AAA Server Group:  CISCO_AD_SERVER
User list retrieved successfully
Number of Active Directory Users: 10
dn: CN=sampleuser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser1
dn: CN=sampleuser2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser2
dn: CN=user3,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: user3
...
```

## 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。

# show user-identity group

アイデンティティファイアウォール用に設定されたユーザーグループを表示するには、特権 EXEC モードで **show user-identity group** コマンドを使用します。

## show user-identity group

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンドデフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリース 変更内容

8.4(2) コマンドが追加されました。

### 使用上のガイドライン

アイデンティティファイアウォール用に設定されたユーザーグループのトラブルシューティング情報を取得するには、**show user-identity group** コマンドを使用します。ASA は、Active Directory サーバーで設定された Active Directory グループに対する LDAP クエリーを送信します。このコマンドは、アクティブ化されたユーザーグループのリストを次の形式で表示します。

*domain \group\_name*

ASA は、セキュリティポリシーに適用される上位グループのみを表示します。アクティブ化された上位グループの最大数は 256 です。グループは、アクセスグループ、インポートユーザーグループ、またはサービスポリシーコンフィギュレーションの一部である場合にアクティブ化されます。

### 例

次に、アイデンティティファイアウォールのアクティブ化されたグループを表示する例を示します。

```
ciscoasa# show user-identity group
Group ID      Activated Group Name (Domain\Group)
-----
1             LOCAL\ogl
2             LOCAL\marketing
```

## show user-identity group

```
3      CISCO\group.sampleuser1
4      IDFW\grp1
...
```

## 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。



## show user-identity ip-of-user

アイデンティティファイアウォールに指定したユーザーの IP アドレスを表示するには、特権 EXEC モードで **show user-identity ip-of-user** コマンドを使用します。

**show user-identity ip-of-user** [ *domain\_nickname* \ ] *user-name* [ **detail** ]

### 構文の説明

**detail** (オプション) ユーザーおよび IP アドレスに関する詳細な出力を表示します。

*domain\_nickname* (オプション) アイデンティティファイアウォールのドメイン名を指定します。

*user-name* IP アドレスを取得するユーザーを指定します。

### コマンドデフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリース 変更内容  
8.4(2) コマンドが追加されました。

### 使用上のガイドライン

このコマンドは、指定したユーザーのユーザー情報と IP アドレスを表示します。1 ユーザーに複数の IP アドレスが関連付けられている場合があります。

*domain\_nickname* 引数を指定しない場合、ASA はデフォルトドメインに *user\_name* があるユーザーの情報を表示します。*domain\_nickname* 引数には、実際のドメインニックネームまたは LOCAL を指定できます。

**detail** キーワードを指定する場合、ASA は、指定したユーザー IP アドレスのすべてで、アクティブな接続の合計数、ユーザー統計情報の期間およびドロップ、期間中の入力パケットおよび出力パケットを表示します。**detail** オプションを指定しない場合、ASA は各 IP アドレスのドメインニックネームとステータスのみを表示します。



- (注) ASAは、アイデンティファイアウォールのユーザー統計情報スキャンまたはアカウントリングをイネーブルにした場合にのみ、指定した期間の受信パケット、送信パケット、およびドロップなどの詳細なユーザー統計情報を表示します。アイデンティファイアウォールの設定の詳細については、CLI コンフィギュレーションガイドを参照してください。

## 例

次に、アイデンティファイアウォールの指定したユーザーのIPアドレスを表示する例を示します。

```
ciscoasa# show user-identity ip-of-user sampleuser1
CSCO\172.1.1.1 (Login)
CSCO\172.100.3.23 (Login)
CSCO\10.23.51.3 (Inactive)
ciscoasa# show user-identity ip-of-user sampleuser1 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins; Idle time: 10 mins; 2 active conns
CSCO\172.100.3.23 (Login) Login time: 20 mins; Idle time: 10 mins; 10 active conns
CSCO\10.23.51.3 (Inactive) Login time: 3000 mins; Idle time: 2040 mins; 8 active conns
Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560
ciscoasa# show user-identity ip-of-user sampleuser2
ERROR: no such user
ciscoasa# show user-identity ip-of-user sampleuser3
ERROR: no IP address, user not login now
```

## IPv6 サポート

```
ciscoasa# show user-identity ip-of-user sampleuser4
CSCO\172.1.1.1 (Login)
CSCO\8080:1:3::56 (Login)
CSCO\8080:2:3::34 (Inactive)
ciscoasa# show user-identity ip-of-user sampleuser4 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins; Idle time: 10 mins; 8 active conns
CSCO\8080:1:3::56 (Login) Login time: 20 mins; Idle time: 10 mins; 12 active conns
CSCO\8080:2:3::34 (Inactive) Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560
```

## 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。
<b>show user-identity user-of-ip</b>	指定した IP アドレスに関連付けられたユーザー情報を表示します

## show user-identity memory

アイデンティティ ファイアウォールの各種モジュールのメモリを表示するには、特権 EXEC モードで **show user-identity memory** コマンドを使用します。

### show user-identity memory

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンドデフォルト

デフォルトの動作や値はありません。

#### 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。

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

#### コマンド履歴

リリース 変更内容  
8.4(2) コマンドが追加されました。

#### 使用上のガイドライン

アイデンティティ ファイアウォールが ASA 上で消費するメモリ使用率をモニターできます。**show user-identity memory** コマンドを実行すると、ユーザーレコード、グループレコード、ホストレコード、およびそれらに関連するハッシュテーブルのメモリが表示されます。ASA は、ID ベースの tmatch テーブルで使用されるメモリも表示します。

このコマンドは、アイデンティティファイアウォールの各種モジュールのメモリ使用率をバイト単位で表示します。

- ユーザー
- グループ
- User Statistics
- LDAP

ASA は、Active Directory サーバーで設定された Active Directory グループに対する LDAP クエリーを送信します。Active Directory サーバーは、ユーザーを認証し、ユーザー ログオンセキュリティ ログを生成します。

- AD エージェント

- その他
- メモリ使用率合計

Identity Firewall で設定した AD エージェントからユーザー情報を取得する方法によって、この機能が使用するメモリの量が変わります。ASA がオンデマンド取得とフルダウンロード取得のどちらを使用するかを指定します。オンデマンドを選択すると、受信パケットのユーザーだけが取得および保存されるためにメモリの使用量が少なくなるというメリットがあります。これらのオプションの説明については、CLI コンフィギュレーションガイドの「アイデンティティオプションの設定」を参照してください。

## 例

次に、アイデンティティファイアウォールのモジュールのメモリステータスを表示する例を示します。

```
ciscoasa# show user-identity memory
Users:          22416048 bytes
Groups:         320 bytes
User stats:    0 bytes
LDAP:          300 bytes
AD agent:      500 bytes
Misc:          32428 bytes
Total:         22449596 bytes
Users:         22416048 bytes
```

## 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。

## show user-identity statistics

アイデンティティファイアウォールのユーザーまたはユーザーグループの統計情報を表示するには、特権 EXEC モードで **show user-identity statistics** コマンドを使用します。

**show user-identity statistics** [ **user** [ *domain\_nickname* \ ] *user\_name* | **user-group** [ *domain\_nickname* \ ] *user\_group\_name* ]

構文の説明	<i>domain_nickname</i>	(オプション) アイデンティティファイアウォールのドメイン名を指定します。
	<b>user</b> <i>user_name</i>	(オプション) 統計情報を取得するユーザー名を指定します。
	<b>user-group</b> <i>domain_nickname</i> \ <i>user_group_name</i>	(オプション) 統計情報を取得するグループ名を指定します。

コマンドデフォルト デフォルトの動作や値はありません。

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。

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

コマンド履歴 リリース 変更内容

8.4(2) コマンドが追加されました。

使用上のガイドライン ユーザーまたはユーザーグループの統計情報を表示するには、**user-identity statistics** コマンドを実行します。

*domain\_nickname* 引数を **user** キーワードとともに指定しない場合、ASA はデフォルトドメインに *user\_name* があるユーザーの情報を表示します。

*domain\_nickname* を **user-group** キーワードとともに指定しない場合、ASA はデフォルトドメインに *user\_group\_name* があるグループに関する情報を表示します。*domain\_nickname* 引数には、実際のドメインニックネームまたは LOCAL を指定できます。

## 例

次に、アイデンティティファイアウォールのユーザーに関する統計情報を表示する例を示します。

```
ciscoasa# show user-identity statistics user

Current monitored users:11 Total not monitored users:0
                Average (eps)    Current (eps) Trigger    Total events
User: CSCO\user1 tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0

    20-min Recv attack:                4                10    14                4861
    1-hour Recv pkts:                  1                10     0                4901
User: CSCO\user2 tot-ses:2456 act-ses:607 fw-drop:0 insp-drop:0 null-ses:2431 bad-acc:0
    20-min Sent attack:                4                10     4                4862
    1-hour Sent pkts:                  0                5     0                2451
...
ciscoasa# show user-identity statistics user user1

Current                Average (eps)    Current (eps) Trigger    Total events
User: -(user1-) tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0
    20-min Recv attack:                4                10    14                4861
    1-hour Recv pkts:                  1                10     0                4901
```

## 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。

## show user-identity statistics top user

アイデンティティファイアウォールの上位10ユーザーの統計情報を表示するには、特権EXECモードで **show user-identity statistics top user** コマンドを使用します。

### show user-identity statistics top user

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンドデフォルト

デフォルトの動作や値はありません。

#### 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。

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

#### コマンド履歴

リリース 変更内容  
8.4(2) コマンドが追加されました。

#### 使用上のガイドライン

**show user-identity statistics top user** コマンドは、上位10ユーザーの受信したEPSパケット、送信したEPSパケット、および送信された攻撃に関する統計情報を表示します。*(domain \user\_name* として表示される) 各ユーザーに関して、ASAは、そのユーザーの平均EPSパケット、現在のEPSパケット、トリガー、および合計イベント数を表示します。

#### 例

次に、アイデンティティファイアウォールの上位10ユーザーに関する情報を表示する例を示します。

```
ciscoasa# show user-identity statistics top user
Top      Name      Id      Average (eps)      Current (eps)      Trigger      Total events
1-hour Recv pkts:
01      APAC\sampleuser1
                                0                0                0                391
1-hour Sent pkts:
01      APAC\sampleuser2
                                0                0                0                196
02      CSCO\sampleuser3
                                0                0                0                195
10-min Sent attack:
01      CSCO\sampleuser4
                                0                0                0                352
```

## show user-identity statistics top user

```
02    CSCO\sampleuser3          0          0          0          350
```

## 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。



## show user-identity user active

アイデンティティファイアウォールのアクティブユーザーを表示するには、特権 EXEC モードで **show user-identity user active** コマンドを使用します。

```
show user-identity user active [ domain domain_nickname | user-group [ domain_nickname \]
user_group_name | user [ domain_nickname \] user_name ] [ list [ detail ] ]
```

構文の説明	<b>detail</b>	(オプション) アクティブユーザーセッションの詳細な出力を表示します。
	<b>domain</b> <i>domain_nickname</i>	指定したドメインのアクティブユーザーの統計情報を表示します。
	<b>list</b>	(オプション) アクティブユーザーの統計情報を要約したリストを表示します。
	<b>user</b> <i>domain_nickname</i> \ <i>user_name</i>	(オプション) 指定したユーザーの統計情報を表示します。
	<b>user-group</b> <i>domain_nickname</i> \ <i>user_group_name</i>	(オプション) 指定したユーザーグループの統計情報を表示します。

コマンドデフォルト デフォルトの動作や値はありません。

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。

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

コマンド履歴 リリース 変更内容  
ス

8.4(2) コマンドが追加されました。

使用上のガイドライン アイデンティティファイアウォールで使用される IP/ユーザーマッピングデータベースに含まれるすべてのユーザーに関する情報を表示できます。

**show user-identity user active** コマンドは、ユーザーに関する次の情報を表示します。

- *domain* \ *user\_name*
- Active Connections

- アイドル時間 (分数)

デフォルトのドメイン名は、実際のドメイン名、特別な予約語、LOCAL のいずれかです。アイデンティティファイアウォールは、ローカルに定義されたすべてのユーザーグループまたはユーザー (VPN または Web ポータルを使用してログインおよび認証を行うユーザー) に対して LOCAL ドメイン名を使用します。デフォルトドメインを指定しない場合、LOCAL がデフォルトドメインとなります。

ユーザー名には、アイドル時間の数値が付加されます。ログイン時間およびアイドル時間は、ユーザーの IP アドレスごとではなくユーザーごとに保存されます。

**user-group** キーワードを指定した場合、アクティブ化されたユーザーグループのみが表示されます。グループは、アクセスグループ、インポートユーザーグループ、またはサービスポリシー コンフィギュレーションの一部である場合にアクティブ化されます。

*domain\_nickname* を **user-group** キーワードとともに指定しない場合、ASA はデフォルトドメインに *user\_group\_name* があるグループに関する情報を表示します。



- (注) **user-identity action domain-controller-down** を **disable-user-identity-rule** キーワードとともに設定し、指定したドメインがダウンしているか、または **user-identity action ad-agent-down** コマンドを **disable-user-identity-rule** キーワードとともに設定し、AD エージェントがダウンしている場合は、ユーザー統計情報に、ログインしているすべてのユーザーがディセーブルになっていると表示されます。



- (注) ASA は、アイデンティティファイアウォールのユーザー統計情報スキャンまたはアカウントリングをイネーブルにした場合にのみ、指定した期間の受信パケット、送信パケット、およびドロップなどの詳細なユーザー統計情報を表示します。アイデンティティファイアウォールの設定の詳細については、CLI コンフィギュレーションガイドを参照してください。

## 例

次に、アイデンティティファイアウォールのアクティブユーザーに関する情報を表示する例を示します。

```
ciscoasa# show user-identity user active

Total active users: 30 Total IP addresses: 35
LOCAL: 0 users, 0 IP addresses
cisco.com: 0 users, 0 IP addresses
dl: 0 users, 0 IP addresses
IDFW: 0 users, 0 IP addresses
idfw.com: 0 users, 0 IP addresses
IDFWTEST: 30 users, 35 IP addresses
ciscoasa# show user-identity user active domain CSCO

Total active users: 48020 Total IP addresses:10000
CSCO: 48020 users, 10000 IP addresses
ciscoasa# show user-identity user active domain CSCO list
```

```

Total active users: 48020 Total IP addresses: 10000
  CSCO: 48020 users, 10000 IP addresses
    CSCO\sampleuser1: 20 active conns; idle 0 mins
    CSCO\member-1: 20 active conns; idle 5 mins
    CSCO\member-2: 20 active conns; idle 20 mins
    CSCO\member-3: 3 active conns; idle 101 mins
    ...
ciscoasa# show user-identity user active list

Total active users: 48032 Total IP addresses: 10000
  CSCO\sampleuser1: 20 active conns; idle 0 mins
  CSCO\member-1: 20 active conns; idle 6 mins
  APAC\sampleuser2: 20 active conns; idle 0 mins
  CSCO\member-2: 20 active conns; idle 1 mins
  CSCO\member-3: 20 active conns; idle 0 mins
  APAC\member-2: 20 active conns; idle 22 mins
  CSCO\member-4: 3 active conns; idle 101 mins
  ...
ciscoasa# show user-identity user active list detail

Total active users: 48032 Total IP addresses: 10010
  CSCO: 48020 users, 10000 IP addresses
  APAC: 12 users, 10 IP addresses
    CSCO\sampleuser1: 20 active conns; idle 0 mins
      172.1.1.1: login 360 mins, idle 0 mins, 15 active conns
      172.100.3.23: login 200 min, idle 15 mins , 5 active conns
      10.23.51.3: inactive
      1-hour rcv packets: 12560
      1-hour sent packets: 32560
      20-min drops: 560
    CSCO\member-1: 4 active connections; idle 350 mins
    ...
  APAC\sampleuser12: 3 active conns; idle 101 mins
      172.1.1.1: login 360 mins, idle 101 mins, 1 active conns
      172.100.3.23: login 200 min, idle 150 mins, 2 active conns
      10.23.51.3: inactive
      1-hour rcv packets: 12560
      1-hour sent packets: 32560
      20-min drops: 560
ciscoasa# show user-identity user active list detail
Total users: 25 Total IP addresses: 5
  LOCAL\idfw: 0 active conns
    6.1.1.1: inactive
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns
    20.0.0.3: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser4: 0 active conns; idle 0 mins
    20.0.0.2: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser5: 0 active conns
  ...
ciscoasa# show user-identity user active user sampleuser1 list detail

CSCO\sampleuser1: 20 active conns; idle 3 mins
  172.1.1.1: login 360 mins, idle 20 mins, 15 active conns
  172.100.3.23: login 200 mins, idle 3 mins, 5 active conns
  10.23.51.3: inactive
  1-hour rcv packets: 12560
  1-hour sent packets: 32560
  20-min drops: 560
ciscoasa# show user-identity user active user APAC\sampleuser2

APAC\sampleuser2: 20 active conns; idle 2 mins
ciscoasa# show user-identity user active user-group APAC\marketing list

```

```

APAC\sampleuser1: 20 active conns; idle 2 mins
APAC\member-1: 20 active conns; idle 0 mins
APAC\member-2: 20 active conns; idle 0 mins
APAC\member-3: 20 active conns; idle 6 mins
...
ciscoasa# show user-identity user active user-group APAC\inactive list
ERROR: group is not activated

```

## 関連コマンド

コマンド	説明
<b>clear user-identity active-user-database</b>	アイデンティティファイアウォールの、指定したユーザー、指定したユーザー グループに属するすべてのユーザー、またはログアウトするすべてのユーザーのステータスを設定します。
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。

## show user-identity user all

アイデンティティファイアウォールのユーザーに関する統計情報を表示するには、特権 EXEC モードで **show user-identity user all** コマンドを使用します。

**show user-identity user all** [ list ] [ detail ]

### 構文の説明

**detail** (オプション) アイデンティティファイアウォールのすべてのユーザーに関する詳細な出力を表示します。

**list** (オプション) アイデンティティファイアウォールのすべてのユーザーの統計情報を要約したリストを表示します。

### コマンドデフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリー 変更内容  
ス

8.4(2) コマンドが追加されました。

### 使用上のガイドライン

アイデンティティファイアウォールで使用される IP ユーザー マッピング データベースに含まれるすべてのユーザーの情報を表示するには、**show user-identity all** コマンドを使用します。

このコマンドとともに **detail** キーワードを指定し、コマンド出力に IP アドレスが非アクティブであると表示される場合、IP アドレスはユーザーに関連付けられていません。その IP アドレスに関連付けられているユーザーを検索するとエラーが返されます。



- (注) **user-identity action domain-controller-down** を **disable-user-identity-rule** キーワードとともに設定し、指定したドメインがダウンしているか、または **user-identity action ad-agent-down** コマンドを **disable-user-identity-rule** キーワードとともに設定し、AD エージェントがダウンしている場合は、ユーザー統計情報に、ログインしているすべてのユーザーがディセーブルになっていると表示されます。



- (注) ASAは、アイデンティティファイアウォールのユーザー統計情報スキャンまたはアカウントリングをイネーブルにした場合にのみ、指定した期間の受信パケット、送信パケット、およびドロップなどの詳細なユーザー統計情報を表示します。アイデンティティファイアウォールの設定の詳細については、CLI コンフィギュレーションガイドを参照してください。

## 例

次に、アイデンティティファイアウォールのすべてのユーザーに関する統計情報を表示する例を示します。

```
ciscoasa# show user-identity user all list
Total inactive users: 1201 Total IP addresses: 100
ciscoasa# show user-identity user all list
Total users: 7
LOCAL\idfw: 0 active conns
cisco.com\sampleuser1: 0 active conns
cisco.com\sampleuser2: 0 active conns
cisco.com\sampleuser3: 0 active conns
cisco.com\sampleuser4: 0 active conns; idle 300 mins
cisco.com\sampleuser5: 0 active conns
cisco.com\sampleuser6: 0 active conns
cisco.com\sampleuser7: 0 active conns
ciscoasa# show user-identity user all list detail
Total users: 7 Total IP addresses: 3
LOCAL\idfw: 0 active conns
10.1.1.1: inactive
cisco.com\sampleuser1: 0 active conns
cisco.com\sampleuser2: 0 active conns
cisco.com\sampleuser3: 0 active conns; idle 300 mins
171.69.42.8: inactive
10.0.0.2: login 300 mins, idle 300 mins, 5 active conns
cisco.com\sampleuser4: 0 active conns
cisco.com\sampleuser5: 0 active conns
cisco.com\sampleuser6: 0 active conns
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560
```

## 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。

## show user-identity user inactive

アイデンティティファイアウォールの非アクティブユーザーに関する情報を表示するには、特権 EXEC モードで **show user-identity user inactive** コマンドを使用します。

**show user-identity user inactive** [ **domain** *domain\_nickname* | **user-group** [ *domain\_nickname* \ ] *user\_group\_name* ]

### 構文の説明

**domain** *domain\_nickname* (オプション) アイデンティティファイアウォールの指定したドメイン名にある非アクティブユーザーの統計情報を表示します。

**user-group** *domain\_nickname*\*user\_group\_name* (オプション) 指定したユーザーグループの非アクティブユーザーの統計情報を表示します。

### コマンドデフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリー 変更内容  
ス

8.4(2) コマンドが追加されました。

### 使用上のガイドライン

**user-identity inactive-user-timer** コマンドを使用して設定した値よりも長い期間、アクティブトラフィックがないユーザーに関する情報を表示するには、**show user-identity user inactive** コマンドを使用します。

**user-group** キーワードを指定した場合、アクティブ化されたユーザーグループのみが表示されます。グループは、アクセスグループ、インポートユーザーグループ、またはサービスポリシーコンフィギュレーションの一部である場合にアクティブ化されます。

*domain\_nickname* を **user-group** キーワードとともに指定しない場合、ASA はデフォルトドメインに *user\_group\_name* があるグループに関する情報を表示します。*domain\_nickname* 引数には、実際のドメインニックネームまたは LOCAL を指定できます。

## 例

次に、アイデンティティファイアウォールの非アクティブユーザーのステータスを表示する例を示します。

```
ciscoasa# show user-identity user inactive
Total inactive users: 1201
  APAC\sampleuser1
  CSCO\sampleuser2
172.1.1.1: inactive  ...
...
ciscoasa# show user-identity user inactive domain CSCO
Total inactive users: 1101
  CSCO: 1101
  CSCO\sampleuser1
  CSCO\sampleuser2
  CSCO\sampleuser3
...
ciscoasa# show user-identity user inactive user-group CSCO\marketing
Total inactive users: 21
  CSCO\sampleuser1
  CSCO\sampleuser2
...
```

## 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。
<b>user-identity inactive-user-timer</b>	ユーザーを Cisco アイデンティティファイアウォールインスタンスのアイドル状態と見なすまでの時間を指定します。



## show user-identity user-not-found

アイデンティティ ファイアウォールの見つからない Active Directory ユーザーの IP アドレスを表示するには、特権 EXEC モードで **show user-identity user-not-found** コマンドを使用します。

### show user-identity user-not-found

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンドデフォルト

デフォルトの動作や値はありません。

#### 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。

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

#### コマンド履歴

リリース 変更内容

8.4(2) コマンドが追加されました。

#### 使用上のガイドライン

Microsoft Active Directory で見つからないユーザーの IP アドレスを表示するには、**show user-identity user-not-found** コマンドを使用します。

ASA は、これらの IP アドレスのローカルの user-not-found データベースを保持します。ASA は、データベースのリスト全体ではなく、user-not-found リストの最後の 1024 パケットのみを保持します（同じ送信元 IP アドレスからの連続するパケットは 1 つのパケットとして扱われます）。

#### 例

次に、アイデンティティ ファイアウォールの not-found ユーザーに関する情報を表示する例を示します。

```
ciscoasa# show user-identity user-not-found
172.13.1.2
171.1.45.5
169.1.1.2
172.13.12
...
```

## 関連コマンド

コマンド	説明
<b>clear user-identity user-not-found</b>	アイデンティティファイアウォールの ASA のローカル user-not-found データベースをクリアします。
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。
<b>user-identity user-not-found</b>	アイデンティティファイアウォールの user-not-found トラッキングをイネーブルにします。

## show user-identity user-of-group

アイデンティティファイアウォールの指定したユーザーグループのユーザーを表示するには、特権 EXEC モードで **show user-identity user-of-group** コマンドを使用します。

**show user-identity user-of-group** [ *domain\_nickname* \ ] *user\_group\_name*

### 構文の説明

*domain\_nickname* アイデンティティファイアウォールのドメイン名を指定します。

*user\_group\_name* 統計情報を表示するユーザー グループを指定します。

### コマンドデフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリー 変更内容  
ス

8.4(2) コマンドが追加されました。

### 使用上のガイドライン

グループ ID が指定したユーザーグループに一致するユーザーを表示するには、**show user-identity user-of-group** コマンドを使用します (ASA は、LDAP クエリーを Active Directory に送信するのではなく、この情報の IP ユーザーハッシュリストをスキャンします。AD エージェントは、ユーザー ID および IP アドレス マッピングのキャッシュを保持し、ASA に変更を通知します)。

名前を指定するユーザーグループはアクティブ化されている必要があります。グループはインポートユーザーグループ (アクセスリストまたはサービスポリシー コンフィギュレーションのユーザーグループとして定義) またはローカルユーザーグループ (オブジェクトグループ ユーザーとして定義) です。

グループは、複数のユーザー メンバーを持つことができます。ユーザーグループのメンバーは、すべて、指定したグループの直近メンバー (ユーザーとグループを含む) です。

*domain\_nickname* を *user\_group\_name* 引数とともに指定しない場合、ASA はデフォルトドメインに *user\_group\_name* があるグループに関する情報を表示します。*domain\_nickname* 引数には、実際のドメイン ニックネームまたは LOCAL を指定できます。

コマンド出力にユーザーステータスが非アクティブであると表示される場合、ユーザーはログアウトしているか、一度もログインしていません。

### 例

次に、アイデンティティファイアウォールの指定したユーザーグループのユーザーを表示する例を示します。

```
ciscoasa# show user-identity user-of-group group.samplegroup1
Group: CSCO\group.user1 Total users: 13
CSCO\user2 10.0.0.10(Login) 20.0.0.10(Inactive) ...
CSCO\user3 10.0.0.11(Inactive)
CSCO\user4 10.0.0.12 (Login)
CSCO\user5 10.0.0.13 (Login)
CSCO\user6 10.0.0.14 (Inactive)
....
ciscoasa# show user-identity user-of-group group.local1
Group: LOCAL\group.local1 Total users: 2
CSCO\user1 10.0.4.12 (Login)
LOCAL\user2 10.0.3.13 (Login)
```

### 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。

## show user-identity user-of-ip

アイデンティティファイアウォールの特定 IP アドレスを使用するユーザーに関する情報を表示するには、特権 EXEC モードで **show user-identity user-of-ip** コマンドを使用します。

**show user-identity user-of-ip** *ip\_address* [ **detail** ]

### 構文の説明

**detail** (オプション) 指定した IP アドレスを使用するユーザーに関する詳細な出力を表示します。

*ip\_address* 情報を表示するユーザーの IP アドレスを示します。

### コマンドデフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリース 変更内容  
ス

8.4(2) コマンドが追加されました。

### 使用上のガイドライン

指定した IP アドレスに関連付けられたユーザー情報を表示するには、**show user-identity user-of-ip** コマンドを使用します。

**detail** キーワードを指定する場合、ASA は、ユーザーログイン時間、アイドル時間、アクティブな接続数、ユーザー統計情報の期間とドロップ、および期間中の入力パケットと出力パケットを表示します。**detail** キーワードを指定しない場合、ASA はドメインニックネーム、ユーザー名、およびステータスのみを表示します。

ユーザーステータスが非アクティブな場合、ユーザーはログアウトしているか、一度もログインしていません。

このコマンドとともに **detail** キーワードを指定し、IP アドレスのコマンド出力にエラーが表示される場合、IP アドレスは非アクティブです。つまり、IP アドレスがユーザーに関連付けられていません。



- (注) ASAは、アイデンティファイアウォールのユーザー統計情報スキャンまたはアカウントリングをイネーブルにした場合にのみ、指定した期間の受信パケット、送信パケット、およびドロップなどの詳細なユーザー統計情報を表示します。アイデンティファイアウォールの設定の詳細については、CLI コンフィギュレーションガイドを参照してください。

## 例

次に、アイデンティファイアウォールのアクティブユーザーのステータスを表示する例を示します。

```
ciscoasa# show user-identity user-of-ip 172.1.1.1
CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 172.1.1.1 detail
CSCO\sampleuser1 (Login) Login time: 240 mins; Idle time: 10 mins
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 172.1.2.2 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 172.1.7.7
ERROR: no user with this IP address
```

## IPv6 のサポート

```
ciscoasa# show user-identity user-of-ip 8080:1:1::4

CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 8080:1:1::4 detail
CSCO\sampleuser1 (Login) Login time: 240 mins; Idle time: 10 mins
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 8080:1:1::6 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 8080:1:1::100
ERROR: no user with this IP address
```

## 関連コマンド

コマンド	説明
<b>user-identity enable</b>	Cisco Identity Firewall インスタンスを作成します。

## show version

ソフトウェアバージョン、ハードウェア構成、ライセンスキー、および関連する動作期間データを表示するには、ユーザー EXEC モードで **show version** コマンドを使用します。

### show version

**コマンドデフォルト** デフォルトの動作や値はありません。

**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。

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

### コマンド履歴

#### リリース 変更内容

- 7.2(1) ステートフル フェールオーバー モードでは、クラスタの動作期間を示す追加の行が表示されます。
- 8.3(1) 出力に、機能で使用されるのが永続キーまたは時間ベース キーのいずれであるか、および使用中の時間ベース キーの期間が含まれるようになりました。
- 8.4(1) ペイロード暗号化機能のないモデル (NPE) のサポートが追加されました。
- 9.3(2) REST API エージェントがイネーブルの場合、バージョン番号が表示されます。
- 9.17(1) システムの起動 (ブート) にかかった時間に関する情報が出力に追加されました。

### 使用上のガイドライン

**show version** コマンドを使用すると、ソフトウェアバージョン、最後にリブートされてからの動作時間、プロセッサタイプ、フラッシュパーティションタイプ、インターフェイスボード、シリアル番号 (BIOSID)、アクティベーションキー値、ライセンスタイプ、およびコンフィギュレーションが最後に変更されたときのタイムスタンプを表示できます。

REST API エージェントがインストールされ、イネーブルになっている場合、バージョン番号も表示されます。

**show version** コマンドで表示されるシリアル番号は、フラッシュパーティション BIOS の番号です。この番号は、シャーシのシリアル番号とは異なります。ソフトウェアアップグレードを入手する場合は、シャーシ番号ではなく、**show version** コマンドで表示されるシリアル番号が必要です。

フェールオーバー クラスタの動作期間の値は、フェールオーバー セットが動作している期間の長さを示しています。1 台のユニットが動作を停止しても、アクティブなユニットが動作を継続する限り、動作期間の値は増加し続けます。このため、フェールオーバー クラスタの動作期間を個別のユニットの動作期間よりも長くすることができます。フェールオーバーを一時的にディセーブルにしてから再びイネーブルにすると、フェールオーバーがディセーブルになる前のユニットの稼働時間と、フェールオーバーがディセーブルである間のユニットの稼働時間が加算されて、フェールオーバー クラスタの動作期間がレポートされます。

ペイロード暗号化機能のないモデルでライセンスを表示すると、VPN およびユニファイド コミュニケーション ライセンスはリストに示されません。

ASA 5505 の合計 VPN ピアの場合、すべてのタイプの VPN セッションの合計数はライセンスによって異なります。AnyConnect Essentials をイネーブルにしている場合、合計はモデルの最大数の 25 です。AnyConnect Premium をイネーブルにしている場合、合計は AnyConnect Premium 値にその他の VPN 値を加えた、25 セッションを超えないものとなります。その他の VPN 値がすべての VPN セッションのモデル制限と等しい他のモデルとは異なり、ASA 5505 のその他の VPN 値はモデル制限よりも低いため、合計値は AnyConnect Premium ライセンスによって変わることがあります。

## 例

次に、**show version** コマンドの出力例を示します。この例では、ソフトウェアバージョン、ハードウェア コンフィギュレーション、ライセンスキー、および関連する稼働時間データを表示する方法を示しています。ステートフルフェールオーバーが設定されている環境では、フェールオーバー クラスタの動作期間を示す追加の行が表示されません。フェールオーバーが設定されていない場合、この行は表示されません。この表示は、最小メモリ要件に関する警告メッセージを示します。

```
*****
**                                     **
**   *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING ***   **
**                                     **
**           ----> Minimum Memory Requirements NOT Met! <----           **
**                                     **
** Installed RAM:   512 MB                                     **
** Required  RAM:  2048 MB                                    **
** Upgrade part#:  ASA5520-MEM-2GB=                           **
**                                     **
** This ASA does not meet the minimum memory requirements needed to **
** run this image. Please install additional memory (part number **
** listed above) or downgrade to ASA version 8.2 or earlier.     **
** Continuing to run without a memory upgrade is unsupported, and **
** critical system features will not function properly.          **
**                                     **
*****
Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)
Compiled on Thu 20-Jan-12 04:05 by builders
System image file is "disk0:/cdisk.bin"
Config file at boot was "disk0:/tomm_backup.cfg"

asa3 up 3 days 3 hours
Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 64MB
Slot 1: ATA Compact Flash, 128MB
BIOS Flash AT49LW080 @ 0xffff00000, 1024KB
```



```

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                          Boot microcode   : CN1000-MC-BOOT-2.00
                          SSL/IKE microcode: CNLite-MC-SSLM-PLUS-2.03
                          IPsec microcode  : CNLite-MC-IPSECM-MAIN-2.06
0: Ext: GigabitEthernet0/0 : address is 0013.c480.82ce, irq 9
1: Ext: GigabitEthernet0/1 : address is 0013.c480.82cf, irq 9
2: Ext: GigabitEthernet0/2 : address is 0013.c480.82d0, irq 9
3: Ext: GigabitEthernet0/3 : address is 0013.c480.82d1, irq 9
4: Ext: Management0/0     : address is 0013.c480.82cd, irq 11
5: Int: Not used          : irq 11
6: Int: Not used          : irq 5
Licensed features for this platform:
Maximum Physical Interfaces : Unlimited    perpetual
Maximum VLANs               : 150          perpetual
Inside Hosts                 : Unlimited   perpetual
Failover                     : Active/Active perpetual
VPN-DES                      : Enabled     perpetual
VPN-3DES-AES                 : Enabled     perpetual
Security Contexts           : 10          perpetual
GTP/GPRS                    : Enabled     perpetual
AnyConnect Premium Peers    : 2           perpetual
AnyConnect Essentials       : Disabled    perpetual
Other VPN Peers              : 750         perpetual
Total VPN Peers              : 750         perpetual
Shared License               : Enabled     perpetual
  Shared AnyConnect Premium Peers : 12000      perpetual
AnyConnect for Mobile        : Disabled    perpetual
AnyConnect for Cisco VPN Phone : Disabled    perpetual
Advanced Endpoint Assessment : Disabled    perpetual
UC Phone Proxy Sessions     : 12          62 days
Total UC Proxy Sessions     : 12          62 days
Botnet Traffic Filter        : Enabled     646 days
Intercompany Media Engine    : Disabled    perpetual
This platform has a Base license.
The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled     646 days
Oxyadayad2 Oxyadayad2 Oxyadayad2 Oxyadayad2 Oxyadayad2
Total UC Proxy Sessions     : 10          62 days
Serial Number: JMX0938K0C0
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Configuration register is 0x1
Configuration last modified by docs at 15:23:22.339 EDT Fri Oct 30 2012

```

**show version** コマンドを実行した後、デバイスが物理的に取り外されていない状態で **eject** コマンドを入力すると、次のメッセージが表示されます。

```

Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.

```

バージョン9.17(1)以降では、システムの起動にかかった時間を確認できます。この情報は、システムの稼働時間のステータスの後に表示されます。

```

FP2130-2# show version
Cisco Adaptive Security Appliance Software Version 99.17(1)144
SSP Operating System Version 82.11(1.288i)
Device Manager Version 88.31(0)45

```

```

Compiled on Tue 06-Apr-21 05:41 GMT by builders
System image file is
"disk0:/mnt/boot/installables/switch/fxos-k8-fp2k-npu.82.11.1.288i.SSB"
Config file at boot was "startup-config"

FP2130-2 up 1 day 23 hours
Start-up time 2 mins 40 secs

Hardware:   FPR-2130, 13703 MB RAM, CPU MIPS 1200 MHz, 1 CPU (12 cores)

1: Int: Internal-Data0/1   : address is 000f.b748.4800, irq 0
3: Int: Not licensed      : irq 0
4: Ext: Management1/1     : address is 2cf8.9b36.0759, irq 0
5: Int: Internal-Data1/1  : address is 0000.0100.0001, irq 0

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces      : Unlimited
Maximum VLANs                   : 1024
Inside Hosts                    : Unlimited
Failover                        : Active/Active
Encryption-DES                  : Enabled
Encryption-3DES-AES             : Disabled
Security Contexts               : 2
Carrier                          : Disabled
AnyConnect Premium Peers        : 7500
AnyConnect Essentials           : Disabled
Other VPN Peers                 : 7500
Total VPN Peers                 : 7500
AnyConnect for Mobile           : Enabled
AnyConnect for Cisco VPN Phone  : Enabled
Advanced Endpoint Assessment    : Enabled
Shared License                  : Disabled
Total TLS Proxy Sessions        : 8000
Cluster                         : Disabled

Serial Number: JAD232913UX
Configuration register is 0x1
Configuration has not been modified since last system restart.

```

## 関連コマンド

コマンド	説明
<b>eject</b>	ASA から物理的に取り外す前に外部コンパクトフラッシュデバイスをシャットダウンできるようにします。
<b>show hardware</b>	ハードウェアの詳細情報を表示します。
<b>show serial</b>	ハードウェアのシリアル情報を表示します。
<b>show uptime</b>	ASA の稼働時間を表示します。

# show vlan

ASA に設定されているすべての VLAN を表示するには、特権 EXEC モードで show vlan コマンドを使用します。

**show vlan** [ **mapping** [ *primary\_id* ] ]

## 構文の説明

**mapping** (オプション) プライマリ VLAN にマッピングされたセカンダリ VLAN を表示します。

*primary\_id* (オプション) 特定のプライマリ VLAN のセカンダリ VLAN を表示します。

## コマンドデフォルト

デフォルトの動作や値はありません。

## 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。

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

## コマンド履歴

リリース 変更内容  
ス

7.2(1) このコマンドが追加されました。

9.5(2) **mapping** キーワードが追加されました。

## 例

次に、設定されている VLAN を表示する例を示します。

```
ciscoasa# show vlan
10-11,30,40,300
```

次に、各プライマリ VLAN にマッピングされたセカンダリ VLAN を表示する例を示します。

```
ciscoasa# show vlan mapping
Interface ID                Secondary VLAN ID          Mapped VLAN
-----
0/1.100                      200                        300
0/1.100                      201                        300
0/2.500                      400                        200
```

## 関連コマンド

コマンド	説明
clear interface	<b>show interface</b> コマンドのカウンタをクリアします。
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実行時ステータスと統計情報を表示します。

## show vm

ASA 仮想 の仮想プラットフォーム情報を表示するには、特権 EXEC モードで show vm コマンドを使用します。

### show vm

#### 構文の説明

このコマンドにはキーワードまたは引数はありません。

#### コマンドデフォルト

デフォルトの動作や値はありません。

#### 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。

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

#### コマンド履歴

リリース 変更内容  
ス

9.2(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

ASA 仮想 に関して、次のライセンス ガイドラインに注意してください。

- 許可される vCPU の数は、インストールされている vCPU プラットフォーム ライセンスによって決定されます。
  - ライセンス vCPU の数が、プロビジョニングされた vCPU の数と一致する場合、状態は Compliant になります。
  - ライセンス vCPU の数が、プロビジョニングされた vCPU の数を下回る場合、状態は Noncompliant: Over-provisioned になります。
  - ライセンス vCPU の数が、プロビジョニングされた vCPU の数を超える場合、状態は Compliant: Under-provisioned になります。
- メモリ制限は、プロビジョニングされた vCPU の数によって決定されます。
  - プロビジョニングされたメモリが上限にある場合、状態は Compliant になります。
  - プロビジョニングされたメモリが上限を超える場合、状態は Noncompliant: Over-provisioned になります。

- プロビジョニングされたメモリが上限を下回る場合、状態は **Compliant: Under-provisioned** になります。
- 周波数予約制限は、プロビジョニングされた vCPU の数によって決定されます。
- 周波数予約メモリが必要最低限 (1000 MHz) 以上である場合、状態は **Compliant** になります。
- 周波数予約メモリが必要最低限 (1000 MHz) 未満である場合、状態は **Compliant: Under-provisioned** になります。

## 例

次に、ライセンスなしの ASAv10 に関する仮想プラットフォーム情報を表示する例を示します。

```
ciscoasa# show vm
Virtual Platform Resource Limits
-----
Number of vCPUs           :      0
Processor Memory         :    0 MB
Virtual Platform Resource Status
-----
Number of vCPUs           :      1      (Noncompliant: Over-provisioned)
Processor Memory         :    2048 MB (Noncompliant: Over-provisioned)
Hypervisor                :    VMware
Model Id                  :    ASAv10
```

次に、ライセンス付き ASAv10 に関する仮想プラットフォーム情報を表示する例を示します。

```
ciscoasa# show vm
Virtual Platform Resource Limits
-----
Number of vCPUs           :      1
Processor Memory         :    2048 MB
Virtual Platform Resource Status
-----
Number of vCPUs           :      1      (Compliant)
Processor Memory         :    2048 MB (Compliant)
Hypervisor                :    VMware
Model Id                  :    ASAv10
```

## 関連コマンド

コマンド	説明
show cpu detail	vCPU ごとに vCPU 情報を表示します。

## show vni vlan-mapping

VNI セグメント ID と VLAN インターフェイスまたは物理インターフェイスとの間のマッピングを表示するには、特権 EXEC モードで **show vni vlan-mapping** コマンドを使用します。

### show vni vlan-mapping

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンドデフォルト

デフォルトの動作や値はありません。

#### 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。

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

#### コマンド履歴

リリース 変更内容  
ス

9.4(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

このコマンドは、ルーテッドモードでは、VXLAN と VLAN 間のマッピングに表示する値を大量に含めることができるため、トランスペアレント ファイアウォールモードでのみ有効です。

#### 例

**show vni vlan-mapping** コマンドについては、次の出力を参照してください。

```
ciscoasa# show vni vlan-mapping
vni1: segment-id: 6000, interface: 'g0110', vlan 10, interface: 'g0111', vlan 11
vni2: segment_id: 5000, interface: 'g01100', vlan 1, interface: 'g111', vlan 3, interface:
'g112', vlan 4
```

#### 関連コマンド

コマンド	説明
<b>debug vxlan</b>	VXLAN トラフィックをデバッグします。
<b>default-mcast-group</b>	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャストグループを指定します。

コマンド	説明
<b>encapsulation vxlan</b>	NVE インスタンスを VXLAN カプセル化に設定します。
<b>inspect vxlan</b>	標準 VXLAN ヘッダー形式に強制的に準拠させます。
<b>interface vni</b>	VXLAN タギング用の VNI インターフェイスを作成します。
<b>mcast-group</b>	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
<b>nve</b>	ネットワーク仮想化エンドポイント インスタンスを指定します。
<b>nve-only</b>	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
<b>peer ip</b>	ピア VTEP の IP アドレスを手動で指定します。
<b>segment-id</b>	VNI インターフェイスの VXLAN セグメント ID を指定します。
<b>show arp vtep-mapping</b>	リモートセグメントドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
<b>show interface vni</b>	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
<b>show mac-address-table vtep-mapping</b>	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル（MAC アドレステーブル）を表示します。
<b>show nve</b>	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
<b>show vni vlan-mapping</b>	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレントモードの物理インターフェイス間のマッピングを表示します。
<b>source-interface</b>	VTEP 送信元インターフェイスを指定します。
<b>vtep-nve</b>	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
<b>vxlan port</b>	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。



## show vpdn

PPPoE または L2TP のような仮想プライベートダイヤルアップネットワーク (VPDN) 接続のステータスを表示するには、特権 EXEC モードで **show vpdn** コマンドを使用します。

```
show vpdn { group name | pppinterface [ id number ] | session [ [ l2tp | pppoe ] [ id number ] {
packets | state | window } | tunnel [ l2tp | pppoe ] [ id number ] { packets | state | summary |
transport } | username name }
```

### 構文の説明

<b>group name</b>	VPDN グループのコンフィギュレーションを表示します。
<b>id number</b>	(オプション) 指定された ID を持つ VPDN セッションに関する情報を表示します。
<b>l2tp</b>	(オプション) L2TP に関するセッションまたはトンネルの情報を表示します。
<b>packets</b>	セッションまたはトンネル パケットの情報を表示します。
<b>pppinterface</b>	PPP インターフェイス情報を表示します。
<b>pppoe</b>	(オプション) PPPoE に関するセッションまたはトンネルの情報を表示します。
<b>session</b>	セッション情報を表示します。
<b>state</b>	セッションまたはトンネルの状態の情報を表示します。
<b>summary</b>	トンネルの概要を表示します。
<b>transport</b>	トンネルのトランスポート情報を表示します。
<b>tunnel</b>	トンネル情報を表示します。
<b>username name</b>	ユーザー情報を表示します。
<b>window</b>	セッション ウィンドウ情報を表示します。

### コマンドデフォルト

デフォルトの動作や値はありません。

### 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。

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

## コマンド履歴

リリース 変更内容  
ス

7.2(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

VPDN PPPoE 接続または L2TP 接続をトラブルシューティングするには、このコマンドを使用します。

## 例

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

```
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
```

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

```
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
  time since change 65901 secs
  Remote Internet Address 10.0.0.1
  Local Internet Address 199.99.99.3
  6 packets sent, 6 received, 84 bytes sent, 0 received
```

## 関連コマンド

コマンド	説明
<b>vpdn group</b>	VPDN クライアント設定を行います。

# show vpn cluster stats internal

VPN クラスタリングの内部カウンタを表示するには、グローバル設定または特権 EXEC モードでこのコマンドを使用します。

## show vpn cluster stats internal

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンドデフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリー 変更内容  
ス

9.9(1) コマンドが追加されました。

### 関連コマンド

コマンド	説明
clear vpn cluster stats internal	すべての VPN クラスタ カウンタをクリアします。

## show vpn load-balancing

VPN ロードバランシングの仮想クラスター コンフィギュレーションに関する実行時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、特権 EXEC モード、または VPN ロードバランシングモードで **show vpn-load-balancing** コマンドを使用します。

### show vpn load-balancing

#### 構文の説明

このコマンドには、変数も引数もありません。

#### コマンド デフォルト

デフォルトの動作や値はありません。

#### 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—
VPN ロードバランシング	• 対応	—	• 対応	—	—

#### コマンド履歴

リリース 変更内容  
ス

7.0(1) このコマンドが追加されました。

7.1(1) 出力例の Load (%) 表示および Session 表示に、個別の IPsec 列および SSL 列が追加されました。

8.4(2) 表示される出力に新しい情報が追加されました。

9.0(1) マルチ コンテキスト モー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 vpn load-balancing** コマンドは、仮想 VPN ロードバランシングクラスターに関する統計情報を表示します。ローカルデバイスが VPN ロードバランシングクラスターに参加していない場合、このコマンドはデバイスに VPN ロードバランシングが設定されていないことを通知します。

出力にあるアスタリスク (\*) は、接続先の ASA の IP アドレスを示します。

## 例

次に、ローカルデバイスがVPNロードバランシングクラスタに参加している場合の **show vpn load-balancing** コマンドの出力例を示します。

```
ciscoasa# sh vpn load-balancing
-----
      Status      Role  Failover  Encryption      Cluster IP  Peers
-----
  Enabled  Master      n/a    Disabled  192.0.2.255    0
Peers:
-----
      Public IP      Role  Pri      Model  Load-Balancing Version
-----
  192.0.2.255      Master  5      ASA-5520      3
Total License Load:
-----
      Public IP      AnyConnect Premium/Essentials      Other VPN
                          Limit  Used  Load      Limit  Used  Load
-----
  192.0.2.255      750   0   0%      750   1   0%
Licenses Used By Inactive Sessions :
-----
      Public IP      AnyConnect Premium/Essentials      Inactive Load
-----
  192.0.2.255      0      0%
```

プライマリ デバイスでは、[Total License Load] 出力にプライマリおよびバックアップ デバイスに関する情報が示されます。ただし、バックアップデバイスは、プライマリ デバイスではなく自身に関する情報のみを表示します。したがって、プライマリ デバイスはすべてのライセンスメンバーを認識しますが、ライセンスメンバーは自身のライセンスのみを認識します。

出力には、[License Used by Inactive Session] セクションも含まれます。セキュアクライアントセッションが非アクティブになる場合、セッションが正常な手段で終了していない間、ASAはそのセッションを保持します。そのため、セキュアクライアントセッションは同じ WebVPN Cookie を使用して再接続できます。再認証する必要はありません。非アクティブなセッションは、セキュアクライアントがセッションを再開するか、アイドルタイムアウトが発生するまで、非アクティブのままになります。セッションのライセンスは、これらの非アクティブなセッションのために保持され、この [License Used by Inactive Session] セクションに示されます。

ローカルデバイスが VPN ロードバランシングクラスタに参加していない場合、**show vpn load-balancing** コマンドには次のような異なる結果が表示されます。

```
ciscoasa(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

## 関連コマンド

コマンド	説明
<b>clear configure vpn load-balancing</b>	すべての <b>vpn load-balancing</b> コマンドステートメントをコンフィギュレーションから削除します。

コマンド	説明
<b>show running-config vpn load-balancing</b>	現在のVPNロードバランシング仮想クラスタのコンフィギュレーションを表示します。
<b>vpn load-balancing</b>	VPNロードバランシングモードを開始します。

## show vpn-sessiondb

VPN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 vpn-sessiondb** コマンドを使用します。このコマンドには、すべての情報または詳細な情報を表示するためのオプションがあり、表示するセッションのタイプを指定できます。また、情報をフィルタリングおよびソートするためのオプションも用意されています。構文の表と使用上の注意で、使用可能なオプションについてそれぞれ説明しています。

```
show vpn-sessiondb [ all ] [ backup { index | l2l } ] [ detail ] [ ospfv3 ] [ failover ] [ full ] [
summary ] [ ratio { encryption | protocol } ] [ license-summary ] { anyconnect | email-proxy |
index indexnumber / l2l | ra-ikev1-ipsec | ra-ikev2-ipsec | vpn-lb | webvpn } [ filter { name username
| ipaddress IPaddr | a-ipaddress IPaddr | p-ipaddress IPaddr | tunnel-group groupname | protocol
protocol-name | encryption encryption-algo | inactive } ] [ sort { name | ipaddress | a-ipaddress |
p-ip address | tunnel-group | protocol | encryption | inactivity } ]
```

### 構文の説明

all	アクティブとバックアップのすべてのクラスタセッションを表示します。
anyconnect	<b>Displays AnyConnect VPN client sessions, including OSPFv3 session information.</b>
backup {index   l2l}	バックアップセッションのみを表示します。
detail	(任意) セッションに関する詳細情報を表示します。たとえば、IPsecセッションに対して detail オプションを使用すると、IKE ハッシュ アルゴリズム、認証モード、キー再生成間隔などの詳細情報が表示されます。  detail および full オプションを指定すると、ASA ではマシンで読み取り可能な形式で詳細な出力を表示します。
email-proxy	(廃止予定) 電子メールプロキシセッションを表示します。
encryption	セッション合計数の比率として暗号化タイプの比率を表示します。
failover	フェールオーバー IPsec トンネルのセッション情報を表示します。
filter filter_criteria	(任意) 1つまたは複数のフィルタ オプションを使用して、指定する情報だけを表示するように出力をフィルタリングします。filter_criteria オプションのリストについては、「使用上のガイドライン」を参照してください。
full	(任意) 連続した、短縮されていない出力を表示します。出力のレコード間には   文字と    スtringが表示されます。
index indexnumber	インデックス番号を指定して、単一のセッションを表示します。セッションのインデックス番号を指定します。範囲は 1 ~ 750 です。
l2l	VPN の LAN-to-LAN セッション情報を表示します。  detail を選択しているときには、クラスタの情報も提供されます。

license-summary	VPN ライセンス サマリー情報を表示します。
ospfv3	OSPFv3 セッション情報を表示します。
protocol	セッション合計数の比率としてプロトコルタイプの比率を表示します。
ra-ikev1-ipsec	IPsec IKEv1 セッションを表示します。
ra-ikev2-ipsec	IKEv2 リモートアクセスクライアント接続の詳細を表示します。
sort <i>sort_criteria</i>	(任意) 指定するソート オプションに従って出力をソートします。 <i>sort_criteria</i> オプションのリストについては、「使用上のガイドライン」を参照してください。
summary	VPN セッション サマリー情報を表示します。
vpn-lb	VPN ロード バランシングの管理セッションを表示します。
webvpn	OSPFv3 セッション情報を含むクライアントレス SSL VPN セッションを表示します。

コマンド デフォルト      デフォルトの動作や値はありません。

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。

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

コマンド履歴

リリー      変更内容  
ス

7.2(1)      このコマンドが追加されました。

8.0(2)      VLAN フィールドの説明が追加されました。

8.0(5)      **inactive** が **filter** オプションとして、**inactivity** が **sort** オプションとして追加されました。

8.2(1)      ライセンス情報が出力に追加されました。

8.4(1)      svc キーワードが anyconnect に変更されました。remote キーワードが ra-ikev1-ipsec に変更されました。、 **ratio keyword was added.**



リリース	変更内容
9.0(1)	<p><b>ospfv3</b> キーワードが追加され、OSPFv3 セッション情報が VPN セッションのサマリーに含まれるようになりました。</p> <p><b>filter a-ipversion</b> オプションおよび <b>filter p-ipversion</b> オプションが追加され、IPv4 または IPv6 アドレスが割り当てられたすべてのセキュアクライアント、LAN-to-LAN、およびクライアントレス SSL VPN のセッションでフィルタリングできるようになりました。</p> <p>マルチ コンテキスト モードのサポートが追加されました。</p>
9.1(2)	<p>フェールオーバー IPsec トンネルをサポートするフェールオーバー トンネルタイプと <b>failover</b> キーワードが追加されました。 <b>failover ipsec pre-shared-key</b> コマンドを参照してください。</p>
9.1(4)	<p>割り当てられた IPv6 アドレスを反映し、IKEv2 デュアルトラフィックの実行時に GRE トランスポートモードのセキュリティ アソシエーションを示すように、<b>detail anyconnect</b> オプションおよび <code>show crypto ipsec sa</code> を使用する場合は出力が更新されました。</p>
9.3(2)	<p>IKEv2 リモートアクセスクライアント接続の詳細を表示する <b>ra-ikev2-ipsec</b> キーワードが追加されました。IKEv2 リモートアクセスクライアント接続および IKEv2 および IPsec トンネルカウントを含めるように、VPN セッションのサマリー出力が更新されました。IKEv2 リモートアクセスクライアント接続を追加するように、VPN ライセンスの使用状況のサマリー出力が更新されました。</p>
9.4(1)	<p>このコマンドの出力に、Cert Auth Int と Cert Auth Left が追加されました。</p>
9.8(1)	<p><b>email-proxy</b> オプションが廃止されました。</p>
9.9(1)	<p><b>all</b> および <b>backup</b> オプションが追加されました。</p>
9.19(1)	<p><b>ra-ikev2-ipsec</b> キーワードは、IKEv2 リモートアクセスクライアント VPN セッションに割り当てられた IPv4 アドレスと IPv6 アドレスの両方を表示します。</p>

### 使用上のガイドライン

次のオプションを使用して、セッションに関する表示内容をフィルタリングおよびソートできます。

フィルタ/ソートオプション	説明
<b>filter a-ipaddress</b> <i>IPAddr</i>	出力をフィルタリングして、指定した割り当て済み IP アドレス（複数可）に関する情報だけを表示します。
<b>sort a-ipaddress</b>	割り当て済み IP アドレスで表示内容をソートします。

フィルタ/ソート オプション	説明
<b>filter a-ipversion</b> {v4 v6}	出力をフィルタ処理して、IPv4 または IPv6 アドレスを割り当てられたすべてのセキュアクライアントセッションに関する情報を表示します。
<b>filter encryption</b> <i>encryption-algo</i>	出力をフィルタリングして、指定した暗号化アルゴリズム（複数可）を使用しているセッションに関する情報だけを表示します。
<b>sort encryption</b>	暗号化アルゴリズムで表示内容をソートします。暗号化アルゴリズムには、aes128、aes192、aes256、des、3des、rc4 が含まれます。
<b>filter inactive</b>	アイドル状態であり、（ハイバネーション、モバイルデバイス切断などによって）接続が切断された可能性がある非アクティブなセッションをフィルタリングします。非アクティブなセッションの数は、TCP キープアライブがセキュアクライアントからの応答なしで ASA から送信されると増加します。各セッションには、SSL トンネルがドロップした時間でタイムスタンプが付けられます。セッションが SSL トンネルを介してアクティブにトラフィックを渡している場合、00:00m:00s が表示されます。  (注) ASA は、バッテリー寿命を節約するために一部のデバイス（iPhone、iPad、iPod など）に TCP キープアライブを送信しないため、障害検出は切断とスリープを区別できません。そのため、非アクティブなカウンタは設計によって 00:00:00 のままになります。
<b>sort inactivity</b>	非アクティブなセッションをソートします。
<b>filter ipaddress</b> <i>IPAddr</i>	出力をフィルタリングして、指定した内部 IP アドレス（複数可）に関する情報だけを表示します。
<b>sort ipaddress</b>	内部 IP アドレスで表示内容をソートします。
<b>filter name</b> <i>username</i> <b>sort name</b>	出力をフィルタリングして、指定したユーザー名（複数可）のセッションを表示します。  ユーザー名のアルファベット順に表示内容をソートします。
<b>filter p-address</b> <i>IPAddr</i>	出力をフィルタリングして、指定した外部 IP アドレスに関する情報だけを表示します。
<b>sort p-address</b>	指定した外部 IP アドレス（複数可）で表示内容をソートします。
<b>filter p-ipversion</b> {v4 v6}	出力をフィルタ処理して、IPv4 または IPv6 アドレスを割り当てられたエンドポイントから送信されるすべてのセキュアクライアントセッションに関する情報を表示します。

フィルタ/ソートオプション	説明
<b>filter protocol</b> <i>protocol-name</i>	出力をフィルタリングして、指定したプロトコル（複数可）を使用しているセッションに関する情報だけを表示します。
<b>sort protocol</b>	プロトコルで表示内容をソートします。プロトコルには、IKE、IMAP4S、IPsec、IPsecLAN2LAN、IPsecLAN2LANOverNatT、IPsecOverNatT、IPsecOverTCP、IPsecOverUDP、SMTPS、userHTTPS、vcaLAN2LAN が含まれます。
<b>filter tunnel-group</b> <i>groupname</i>	出力をフィルタリングして、指定したトンネルグループ（複数可）に関する情報だけを表示します。
<b>sort tunnel-group</b>	トンネルグループで表示内容をソートします。
	引数 {begin   include   exclude   grep   [-v]} {reg_exp} を使用して、出力を修正します。

注：コマンド出力には、最大 120 文字のユーザー名のみが表示されます。120 文字を超える場合、超えた分の文字を切り捨ててコマンド出力に表示されます。

## 例

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

```
ciscoasa
#
  show vpn-sessiondb
-----
VPN Session Summary
-----
Active : Cumulative : Peak Concur : Inactive
-----
AnyConnect Client      :    1 :          78 :    2 :    0
  SSL/TLS/DTLS         :    1 :          72 :    2 :    0
  IKEv2 IPsec          :    0 :           6 :    1 :    0
IKEv2 Generic IPsec Client :    0 :           0 :    0 :
Clientless VPN        :    0 :           8 :    2 :
  Browser              :    0 :           8 :    2 :
-----
Total Active and Inactive :    1              Total Cumulative :    86
Device Total VPN Capacity :    750
Device Load               :    0%
-----
Tunnels Summary
-----
Active : Cumulative : Peak Concurrent
-----
IKEv2          :    0 :           6 :    1
IPsecOverNatT :    0 :           6 :    1
Clientless     :    0 :          17 :    2
AnyConnect-Parent :    1 :          69 :    2
SSL-Tunnel     :    1 :          75 :    2
DTLS-Tunnel    :    1 :          56 :    2
-----
```

```
Totals : 3 : 229
```

```
-----
IPv6 Usage Summary
-----
```

```

Active : Cumulative : Peak Concurrent
-----
AnyConnect SSL/TLS/DTLS : : :
IPv6 Peer : 1 : 41 : 2
Tunneled IPv6 : 1 : 70 : 2
AnyConnect IKEv2 : : :
IPv6 Peer : 0 : 4 : 1
Clientless : : :
IPv6 Peer : 0 : 1 : 1
-----
```

次に、**show vpn-sessiondb detail 121** コマンドの出力例を示します。LAN-to-LAN セッションに関する詳細情報が表示されています。

```
ciscoasa
#
show vpn-sessiondb detail 121
Session Type: LAN-to-LAN Detailed
Connection : 172.16.0.0
Index : 1
IP Addr : 172.16.0.0
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 240 Bytes Rx : 160
Login Time : 14:50:35 UTC Tue May 1 2012
Duration : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1
IKEv2:
  Tunnel ID : 1.1
  UDP Src Port : 500 UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption : AES256 Hashing : SHA1
  Rekey Int (T): 86400 Seconds Rekey Left(T): 86389 Seconds
  PRF : SHA1 D/H Group : 5
  Filter Name :
  IPv6 Filter :
IPsec:
  Tunnel ID : 1.2
  Local Addr : 10.0.0.0/255.255.255.0
  Remote Addr : 209.165.201.30/255.255.255.0
  Encryption : AES256 Hashing : SHA1
  Encapsulation: Tunnel PFS Group : 5
  Rekey Int (T): 120 Seconds Rekey Left(T): 107 Seconds
  Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
  Bytes Tx : 240 Bytes Rx : 160
  Pkts Tx : 3 Pkts Rx : 2
NAC:
  Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
  SQ Int (T) : 0 Seconds EoU Age(T) : 13 Seconds
  Hold Left (T): 0 Seconds Posture Token:
  Redirect URL :
The following is sample output from the show vpn-sessiondb detail index 1
command:
AsaNacDev# show vpn-sessiondb detail index 1
```

```

Session Type: Remote Detailed
Username      : user1
Index        : 1
Assigned IP   : 192.168.2.70          Public IP    : 10.86.5.114
Protocol      : IPsec                Encryption   : AES128
Hashing       : SHA1
Bytes Tx      : 0                    Bytes Rx     : 604533
Client Type   : WinNT                Client Ver   : 4.6.00.0049
Tunnel Group  : bxbvplab
Login Time    : 15:22:46 EDT Tue May 10 2005
Duration      : 7h:02m:03s
Filter Name   :
NAC Result    : Accepted
Posture Token : Healthy
VM Result     : Static
VLAN          : 10
IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1
IKE:
  Session ID   : 1
  UDP Src Port : 500                  UDP Dst Port : 500
  IKE Neg Mode : Aggressive          Auth Mode    : preSharedKeysXauth
  Encryption   : 3DES                Hashing      : MD5
  Rekey Int (T): 86400 Seconds       Rekey Left (T): 61078 Seconds
  D/H Group    : 2
IPsec:
  Session ID   : 2
  Local Addr   : 0.0.0.0
  Remote Addr  : 192.168.2.70
  Encryption   : AES128              Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds       Rekey Left (T): 26531 Seconds
  Bytes Tx     : 0                   Bytes Rx     : 604533
  Pkts Tx      : 0                   Pkts Rx     : 8126
NAC:
  Reval Int (T): 3000 Seconds        Reval Left (T): 286 Seconds
  SQ Int (T)   : 600 Seconds         EoU Age (T)  : 2714 Seconds
  Hold Left (T): 0 Seconds           Posture Token: Healthy
  Redirect URL : www.cisco.com

```

次に、**show vpn-sessiondb ospfv3** コマンドの出力例を示します。

```

asa# show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec
Connection   :
Index        : 1                    IP Addr     : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none       Hashing     : IPsec: (1)SHA1
Bytes Tx     : 0                    Bytes Rx    : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012
Duration     : 1d 5h:13m:11s

```

次に、**show vpn-sessiondb detail ospfv3** コマンドの出力例を示します。

```

asa# show vpn-sessiondb detail ospfv3

Session Type: OSPFv3 IPsec Detailed
Connection   :
Index        : 1                    IP Addr     : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none       Hashing     : IPsec: (1)SHA1
Bytes Tx     : 0                    Bytes Rx    : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012

```

```

Duration      : 1d 5h:14m:28s
IPsec Tunnels: 1
IPsec:
  Tunnel ID   : 1.1
  Local Addr  : ::/0/89/0
  Remote Addr : ::/0/89/0
  Encryption  : none
  Hashing     : SHA1
  Encapsulation: Transport
  Idle Time Out: 0 Minutes
  Bytes Tx    : 0
  Pkts Tx     : 0
  Bytes Rx    : 0
  Pkts Rx     : 0
  Idle TO Left : 0 Minutes
  Posture Token:

NAC:
  Reval Int (T): 0 Seconds
  SQ Int (T)   : 0 Seconds
  Hold Left (T): 0 Seconds
  Redirect URL :
  Reval Left(T): 0 Seconds
  EoU Age(T)   : 105268 Seconds

```

次に、**show vpn-sessiondb summary** コマンドの出力例を示します。

```

ciscoasa# show vpn-sessiondb summary

-----
VPN Session Summary
-----
Active : Cumulative : Peak Concur : Inactive
-----
OSPFv3 IPsec      :      1 :           1 :           1
-----
Total Active and Inactive :      1           Total Cumulative :      1
Device Total VPN Capacity : 10000
Device Load          :      0%
-----

```

次に、一般的な IKEv2 IPsec リモートアクセスセッションに関する **show vpn-sessiondb summary** コマンドの出力例を示します。

```

ciscoasa# show vpn-sessiondb summary

-----
VPN Session Summary
-----
Active : Cumulative : Peak Concur : Inactive
-----
Generic IKEv2 Remote Access :      1 :           1 :           1
-----
Total Active and Inactive :      1           Total Cumulative :      1
Device Total VPN Capacity :      250
Device Load                :      0%
-----

Tunnels Summary
-----
Active : Cumulative : Peak Concurrent
-----
IKEv2      :      1 :           1 :           1
IPsec      :      1 :           1 :           1
-----
Totals     :      2 :           2
-----

```

次に、**show vpn-sessiondb det anyconnect** コマンドの出力例を示します。

```

ciscoasa# show vpn-sessiondb det anyconnect
Session Type: AnyConnect Detailed
Username      : userab                      Index      : 2
Assigned IP   : 65.2.1.100                 Public IP  : 75.2.1.60
Assigned IPv6 : 2001:1000::10
Protocol      : IKEv2 IPsecOverNatT AnyConnect-Parent
License       : AnyConnect Premium
Encryption    : IKEv2: (1)3DES IPsecOverNatT: (1)3DES AnyConnect-Parent: (1)none
Hashing       : IKEv2: (1)SHA1 IPsecOverNatT: (1)SHA1 AnyConnect-Parent: (1)none
Bytes Tx      : 0                          Bytes Rx   : 21248
Pkts Tx       : 0                          Pkts Rx   : 238
Pkts Tx Drop  : 0                          Pkts Rx Drop : 0
Group Policy  : DfltGrpPolicy              Tunnel Group : test1
Login Time    : 22:44:59 EST Tue Aug 13 2013
Duration      : 0h:02m:42s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                        VLAN       : none
IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1
AnyConnect-Parent:
  Tunnel ID   : 2.1
  Public IP   : 75.2.1.60
  Encryption  : none                      Hashing     : none
  Auth Mode   : userPassword
  Idle Time Out: 400 Minutes              Idle TO Left : 397 Minutes
  Conn Time Out: 500 Minutes              Conn TO Left : 497 Minutes
  Client OS   : Windows
  Client Type : AnyConnect
  Client Ver  : 3.1.05050
IKEv2:
  Tunnel ID   : 2.2
  UDP Src Port : 64251                    UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption  : 3DES                      Hashing     : SHA1
  Rekey Int (T): 86400 Seconds              Rekey Left(T): 86241 Seconds
  PRF         : SHA1                       D/H Group   : 2
  Filter Name : mixed1
  Client OS   : Windows
IPsecOverNatT:
  Tunnel ID   : 2.3
  Local Addr  : 75.2.1.23/255.255.255.255/47/0
  Remote Addr : 75.2.1.60/255.255.255.255/47/0
  Encryption  : 3DES                      Hashing     : SHA1
  Encapsulation: Transport, GRE
  Rekey Int (T): 28400 Seconds              Rekey Left(T): 28241 Seconds
  Idle Time Out: 400 Minutes              Idle TO Left : 400 Minutes
  Conn Time Out: 500 Minutes              Conn TO Left : 497 Minutes
  Bytes Tx    : 0                          Bytes Rx    : 21326
  Pkts Tx     : 0                          Pkts Rx    : 239
NAC:
  Reval Int (T): 0 Seconds                  Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds                  EoU Age(T)   : 165 Seconds
  Hold Left (T): 0 Seconds                  Posture Token:
  Redirect URL :
Output from show vpn-sessiondb detail anyconnect showing a DTLS tunnel.
...
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1

```

```

Bytes Tx      : 10280                Bytes Rx      : 3819
Pkts Tx       : 8                    Pkts Rx       : 45
Pkts Tx Drop  : 0                    Pkts Rx Drop  : 0
Group Policy  : DfltGrpPolicy         Tunnel Group   : DefaultWEBVPNGroup
Login Time    : 09:42:39 UTC Tue Dec 5 2017
Duration      : 0h:00m:07s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                   VLAN           : none
Audt Sess ID  : 00000000000010005a266a0f
Security Grp  : none
...
DTLS-Tunnel:
  Tunnel ID    : 1.3
  Assigned IP  : 95.0.225.240          Public IP     : 85.0.224.13
  Encryption   : AES256                Hashing       : SHA1
  Ciphersuite  : AES256-SHA
  Encapsulation: DTLSv1.2              UDP Src Port  : 51008
  UDP Dst Port : 443                   Auth Mode     : userPassword
  Idle Time Out: 30 Minutes            Idle TO Left  : 30 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.x

```

次に、**show vpn-sessiondb ra-ikev2-ipsec** コマンドの出力例を示します。

```

ciscoasa(config)# show vpn-sessiondb detail ra-ikev2-ipsec
Session Type: Generic Remote-Access IKEv2 IPsec Detailed
Username      : IKEV2TG                Index         : 1
Assigned IP   : 95.0.225.200          Public IP     : 85.0.224.12
Assigned IPv6 : 2001:db8::1
Protocol      : IKEv2 IPsec
License       : AnyConnect Essentials
Encryption    : IKEv2: (1)3DES IPsec: (1)AES256
Hashing       : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx      : 0                      Bytes Rx      : 17844
Pkts Tx       : 0                      Pkts Rx       : 230
Pkts Tx Drop  : 0                      Pkts Rx Drop  : 0
Group Policy  : GroupPolicy_IKEV2TG    Tunnel Group   : IKEV2TG
Login Time    : 11:39:54 UTC Tue May 6 2014
Duration      : 0h:03m:17s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                   VLAN           : none
Audt Sess ID  : 5f00e105000010005368ca0a
Security Grp  : none
IKEv2 Tunnels: 1
IPsec Tunnels: 1

```

次に、**show vpn-sessiondb license-summary** コマンドの出力例を示します。

```

-----
VPN Licenses and Configured Limits Summary
-----
                                Status : Capacity : Installed : Limit
-----
AnyConnect Premium              : DISABLED : 250 : 10 : NONE
AnyConnect Essentials           : ENABLED  : 250 : 250 : NONE
Other VPN (Available by Default) : ENABLED  : 250 : 250 : NONE
Shared License Server           : DISABLED
Shared License Participant       : DISABLED
AnyConnect for Mobile           : DISABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment     : DISABLED(Requires Premium)
AnyConnect for Cisco VPN Phone  : DISABLED
VPN-3DES-AES                    : ENABLED

```



```

VPN-DES                               :   ENABLED
-----
VPN Licenses Usage Summary
-----
                Local : Shared :   All :   Peak :   Eff. :
                In Use : In Use : In Use : In Use : Limit : Usage
-----
AnyConnect Essentials :     1 :     0 :     1 :     1 :   250 :   0%
  AnyConnect Client   :           :           :     0 :     0 :       :   0%
    AnyConnect Mobile :           :           :     0 :     0 :       :   0%
  Generic IKEv2 Client :           :           :     1 :     1 :       :   0%
Other VPN              :           :           :     0 :     0 :   250 :   0%
  Cisco VPN Client    :           :           :     0 :     0 :       :   0%
-----
Shared License Network Summary
-----
AnyConnect Premium
Total shared licenses in network           : 500
Shared licenses held by this participant   : 0
Shared licenses held by all participants in the network : 0
-----

```

例に示すとおり、**show vpn-sessiondb** コマンドの応答に表示されるフィールドは、入力するキーワードによって異なります。表 14-2 で、これらのフィールドについて説明します。

表 2: **show vpn-sessiondb** コマンドのフィールド

フィールド	説明
Auth Mode	このセッションを認証するためのプロトコルまたはモード。
割り当てられている IP	現在のセッションのリモートクライアントに割り当てられたプライベート IP アドレス。
割り当てられている IPv6	現在のセッションのリモートクライアントに割り当てられたプライベート IPv6 アドレス。
Bytes Rx	ASA がリモートのピアまたはクライアントから受信した合計バイト数。
バイト Tx (Bytes Tx)	ASA がリモートのピアまたはクライアントに送信した合計バイト数。
クライアント タイプ	リモート ピア上で実行されるクライアント ソフトウェア (利用できる場合)。
Client Ver	リモート ピア上で実行されるクライアント ソフトウェアのバージョン。
Connection	接続名またはプライベート IP アドレス。
D/H Group	Diffie-Hellman グループ。IPsec SA 暗号キーを生成するためのアルゴリズムおよびキー サイズ。

フィールド	説明
持続時間	セッションのログイン時刻から直前の画面リフレッシュまでの経過時間 (HH:MM:SS)。
EAPoUDP Session Age	正常に完了した直前のポスチャ確認からの経過秒数。
カプセル化	IPsec ESP (暗号ペイロードプロトコル) の暗号化と認証 (つまり、ESP を適用した元の IP パケットの一部) を適用するためのモード。
暗号化	このセッションが使用しているデータ暗号化アルゴリズム (ある場合)。
EoU Age (T)	EAPoUDP セッションの経過時間。正常に完了した直前のポスチャ確認からの経過秒数。
Filter Name	セッション情報の表示を制限するよう指定されたユーザー名。
ハッシュ	パケットのハッシュを生成するためのアルゴリズム。IPsec データ認証に使用されます。
Hold Left (T)	Hold-Off Time Remaining。直前のポスチャ確認が正常に完了した場合は、0秒です。それ以外の場合は、次のポスチャ確認試行までの秒数です。
Hold-Off Time Remaining	直前のポスチャ確認が正常に完了した場合は、0秒です。それ以外の場合は、次のポスチャ確認試行までの秒数です。
IKE Neg Mode	キー情報を交換し、SA を設定するための IKE (IPsec フェーズ 1) モード (アグレッシブまたはメイン)。
IKE Sessions	IKE (IPsec フェーズ 1) セッションの数で、通常は 1。これらのセッションにより、IPsec トラフィックのトンネルが確立されます。
索引	このレコードの固有識別情報。
IP Addr	このセッションのリモートクライアントに割り当てられたプライベート IP アドレス。このアドレスは、「内部」または「仮想」IP アドレスとも呼ばれています。このアドレスを使用すると、クライアントはプライベート ネットワーク内のホストと見なされます。
IPsec Sessions	IPsec (フェーズ 2) セッション (トンネル経由のデータトラフィックセッション) の数。各 IPsec リモートアクセスセッションには、2つの IPsec セッションがあります。1つはトンネルエンドポイントで構成されるセッション、もう1つはトンネル経由で到達可能なプライベート ネットワークで構成されるセッションです。
ライセンス情報	共有 SSL VPN ライセンスに関する情報を表示します。

フィールド	説明
Local IP Addr	トンネルのローカルエンドポイント（ASA 上のインターフェイス）に割り当てられた IP アドレス。
Login Time	セッションにログインした日時（MMM DD HH:MM:SS）。時刻は 24 時間表記で表示されます。
NAC Result	ネットワークアドミッションコントロールポスチャ検証の状態。次のいずれかを指定できます。 <ul style="list-style-type: none"> <li>• [Accepted] : ACS は正常にリモートホストのポスチャを検証しました。</li> <li>• [Rejected] : ACS はリモートホストのポスチャの検証に失敗しました。</li> <li>• [Exempted] : ASA に設定されたポスチャ検証免除リストに従って、リモートホストはポスチャ検証を免除されています。</li> <li>• [Non-Responsive] : リモートホストは EAPoUDP Hello メッセージに応答しませんでした。</li> <li>• [Hold-off] : ポスチャ検証に成功した後、ASA とリモートホストの EAPoUDP 通信が途絶えました。</li> <li>• [N/A] : VPN NAC グループポリシーに従い、リモートホストの NAC はディセーブルにされています。</li> <li>• [Unknown] : ポスチャ検証が進行中です。</li> </ul>
NAC Sessions	ネットワークアドミッションコントロール（EAPoUDP）セッションの数。
Packets Rx	ASA がリモートピアから受信したパケット数。
Packets Tx	ASA がリモートピアに送信したパケット数。
PFS Group	完全転送秘密グループ番号。
Posture Token	Access Control Server 上で設定可能な情報テキストストリング。ACS は情報提供のために ASA にポスチャトークンをダウンロードし、システムモニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャトークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
Protocol	セッションが使用しているプロトコル。
Public IP	クライアントに割り当てられた、公開されているルーティング可能な IP アドレス。

フィールド	説明
リダイレクト URL	<p>ポストチャ検証またはクライアントレス認証に続いて、ACSはセッションのアクセスポリシーをASAにダウンロードします。Redirect URLは、アクセスポリシーペイロードのオプションの一部です。ASAは、リモートホストのすべてのHTTP（ポート80）要求とHTTPS（ポート443）要求をRedirect URL（存在する場合）にリダイレクトします。アクセスポリシーにRedirect URLが含まれていない場合、ASAはリモートホストからのHTTP要求やHTTPS要求をリダイレクトしません。</p> <p>Redirect URLは、IPsecセッションが終了するか、ポストチャ再検証が実行されるまで有効です。ACSは、異なるRedirect URLが含まれるか、Redirect URLが含まれない新しいアクセスポリシーをダウンロードします。</p>
Rekey Int（TまたはD）	IPsec（IKE）SA暗号キーの有効期限。T値は時間でのライフタイム、D値は送信済みデータでのライフタイムです。リモートアクセスVPNではT値のみが表示されます。
Rekey Left（TまたはD）	IPsec（IKE）SA暗号キーの残りのライフタイム。T値は時間でのライフタイム、D値は送信済みデータでのライフタイムです。リモートアクセスVPNではT値のみが表示されます。
Rekey Time Interval	IPsec（IKE）SA暗号キーの有効期限。
Remote IP Addr	トンネルのリモートエンドポイント（リモートピア上のインターフェイス）に割り当てられたIPアドレス。
Reval Int（T）	Revalidation Time Interval。正常に完了した各ポストチャ確認間に、設ける必要のある間隔（秒単位）。
Reval Left（T）	Time Until Next Revalidation。直前のポストチャ確認試行が正常に完了しなかった場合は0です。それ以外の場合は、Revalidation Time Intervalと、正常に完了した直前のポストチャ確認からの経過秒数との差です。
Revalidation Time Interval	正常に完了した各ポストチャ確認間に、設ける必要のある間隔（秒単位）。
Session ID	セッションコンポーネント（サブセッション）のID。各SAには独自のIDがあります。
Session Type	セッションのタイプ（LAN-to-LANまたはRemote）。
SQ Int（T）	Status Query Time Interval。正常に完了した各ポストチャ確認またはステータスクエリー応答から、次のステータスクエリー応答までの間に空けることができる秒数です。ステータスクエリーは、直前のポストチャ確認以降にホストでポストチャが変化したかどうかを確認するために、ASAがリモートホストに発行する要求です。

フィールド	説明
Status Query Time Interval	正常に完了した各ポスチャ確認またはステータスクエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、ASA がリモートホストに発行する要求です。
Time Until Next Revalidation	直前のポスチャ確認試行が正常に完了しなかった場合は0です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
Tunnel Group	属性値を求めるために、このトンネルが参照するトンネルグループの名前。
UDP Dst Port または UDP Destination Port	リモートピアが使用する UDP のポート番号。
UDP Src Port または UDP Source Port	ASA が使用する UDP のポート番号。
Username	セッションを確立したユーザーのログイン名。
VLAN	このセッションに割り当てられた出力VLANインターフェイス。ASAは、すべてのトラフィックをこのVLANに転送します。次のいずれかの要素で値を指定します。 <ul style="list-style-type: none"> <li>• グループ ポリシー</li> <li>• 継承されたグループ ポリシー</li> </ul>

## 関連コマンド

コマンド	説明
<b>show running-configuration vpn-sessiondb</b>	VPNセッションデータベースの実行コンフィギュレーション (max-other-vpn-limit、max-anyconnect-premium-or-essentials-limit) を表示します。
<b>show vpn-sessiondb ratio</b>	VPNセッションの暗号化またはプロトコルの比率を表示します。

## show vpn-sessiondb ratio

現在のセッションについて、プロトコルごと、または暗号化アルゴリズムごとの比率をパーセンテージで表示するには、特権 EXEC モードで **show vpn-sessiondb ratio** コマンドを使用します。

**show vpn-sessiondb ratio** { **protocol** | **encryption** } [ **filter** *groupname* ]

### 構文の説明

**encryption** 表示する暗号化プロトコルを指定します。フェーズ 2 暗号化に関して指定します。暗号化アルゴリズムには次の種類があります。

aes128	des
aes192	3des
aes256	rc4

**filter** *groupname* 出力をフィルタリングして、指定するトンネルグループについてのみセッションの比率を表示します。

**protocol** 表示するプロトコルを指定します。プロトコルには次の種類があります。

IKEv1	L2TPOverIPsecOverNatT
IKEv2	クライアントレス
IPSec	ポート転送
IPsecLAN2LAN	IMAP4S
IPsecLAN2LANOverNatT	POP3S
IPsecOverNatT	SMTPS
IPsecOverTCP	AnyConnect-Parent
IPsecOverUDP	SSL トンネル
L2TPOverIPsec	DTLS トンネル

### コマンド デフォルト

デフォルトの動作や値はありません。

### 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。

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

## コマンド履歴

リリース 変更内容

7.0(1) このコマンドが追加されました。

8.4(1) 出力が拡張され、IKEv2 が含まれるようになりました。

9.0(1) マルチコンテキストモードのサポートが追加されました。

## 例

次に、引数として **encryption** を指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
ciscoasa# show vpn-sessiondb ratio encryption
Filter Group      : All
Total Active Sessions: 5
Cumulative Sessions : 9
Encryption        Sessions      Percent
none              0             0%
DES               1             20%
3DES              0             0%
AES128            4             80%
AES192            0             0%
AES256            0             0%
```

次に、引数として **protocol** を指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
ciscoasa# show vpn-sessiondb ratio protocol
Filter Group      : All
Total Active Sessions: 6
Cumulative Sessions : 10
Protocol          Sessions      Percent
IKE               0             0%
IPsec             1             20%
IPsecLAN2LAN     0             0%
IPsecLAN2LANOverNatT 0             0%
IPsecOverNatT    0             0%
IPsecOverTCP     1             20%
IPsecOverUDP     0             0%
L2TP              0             0%
L2TPOverIPsec    0             0%
L2TPOverIPsecOverNatT 0             0%
PPPoE            0             0%
vpnLoadBalanceMgmt 0             0%
userHTTPS        0             0%
IMAP4S           3             30%
POP3S            0             0%
SMTPS            3             30%
```

## 関連コマンド

コマンド	説明
<b>show vpn-sessiondb</b>	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。

コマンド	説明
<b>show vpn-sessiondb summary</b>	セッションの要約を表示します。現在のセッションの合計数、各タイプの現在のセッション数、ピーク時の数および累積合計数、最大同時セッション数を含んでいます。



## show vpn-sessiondb summary

IPsec、Cisco セキュアクライアント、および NAC の各セッションの数を表示するには、特権 EXEC モードで **show vpn-sessiondb summary** コマンドを使用します。

### show vpn-sessiondb summary

**コマンド デフォルト** デフォルトの動作や値はありません。

**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。

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

### コマンド履歴

リリース 変更内容

7.0(7) このコマンドが追加されました。

8.0(2) VLAN Mapping Sessions テーブルが追加されました。

8.0(5) active (アクティブ)、cumulative (累積)、peak concurrent (ピーク時の同時発生)、および inactive (非アクティブ) に関する新しい出力が追加されました。

9.0(1) マルチ コンテキスト モードのサポートが追加されました。

### 例

次に、1つの IPsec IKEv1 および1つのクライアントレスセッションを指定した **show vpn-sessiondb summary** コマンドの出力例を示します。



(注) スタンバイ状態のデバイスでは、アクティブなセッションと非アクティブなセッションが区別されません。

```
ciscoasa# show vpn-sessiondb summary
VPN Session Summary
Sessions:
  Active : Cumulative : Peak Concurrent : Inactive :
Clientless VPN      : 1:  2:  1 Browser      : 1:  2:  1 IKEv1 IPsec/L2TP
IPsec      0      : 1:  1:  1
Total Active and Inactive: 2          Total Cumulative: 3
Device Total VPN Capacity: 10000
```

```

Device Load      : 0%
License Information:
Shared VPN License Information:
  SSL VPN        : 12000
    Allocated to this device      : 0
    Allocated to network          : 0
    Device limit                   : 750
IPsec : 750 Configured : 750 Active : 0 Load : 0%
SSL VPN : 750 Configured : 750 Active : 0 Load : 0%
    Active : Cumulative : Peak Concurrent
SSL VPN : 0 : 1 : 1
Totals : 0 : 1 :
Active NAC Sessions:
  Accepted : 0
  Rejected : 0
  Exempted : 0
  Non-responsive : 0
Hold-off : 0
N/A : 0
Active VLAN Mapping Sessions:
  Static : 0
  Auth : 0
  Access : 0
  Guest : 0
  Quarantine : 0
  N/A : 0
ciscoasa#

```

SSL 出力を使用して、ライセンス数に関する物理デバイスリソースを特定できます。単一のユーザーセッションがライセンスを占有し、かつ複数のトンネルを使用することがあります。たとえば、DTLS を使用するセキュアクライアントユーザーは、多くの場合、関連する親セッション、SSL トンネル、およびDTLS トンネルを使用します。



- (注) 親セッションは、クライアントがアクティブに接続されていない場合を示します。暗号化トンネルは表しません。クライアントがシャットダウンしたかスリープ中である場合、IPsec、IKE、TLS、およびDTLS トンネルは閉じられますが、アイドル時間または最大接続時間の制限に到達するまで親セッションが維持されます。これにより、ユーザーは再認証しないで再接続できます。

この例では、ログインしているユーザーが 1 人の場合でも、デバイスに割り当てられている 3 つのトンネルが表示されます。IPsec LAN-to-LAN トンネルは 1 セッションとしてカウントされ、トンネルを通じて多くのホスト間接続を可能にします。IPsec リモートアクセスセッションは、1 つのユーザー接続をサポートする 1 リモートアクセストンネルです。

出力から、アクティブなセッションを確認できます。セッションに関連付けられた、基本となるトンネルがない場合、ステータスは再開待ちモードになります（セッション出力にクライアントレスとして表示されます）。このモードは、ヘッドエンドデバイスからのデッドピア検出が開始され、ヘッドエンドデバイスがクライアントと通信できないことを意味します。この状態が発生した場合は、ユーザーがネットワークをローミングしたり、スリープにしたり、セッションを再開したりすることができるように、セッションを保持できます。これらのセッションは、アクティブに接続された

セッション（ライセンスの観点から）にカウントされ、ユーザーのアイドルタイムアウト、ユーザーのログアウト、または元のセッション再開でクリアされます。

SSL VPN With Client の Active 列には、データを送信しているアクティブな接続の数が表示されます。SSL VPN With Client の Cumulative 列には、確立されているアクティブなセッションの数が表示されます。この数には非アクティブなセッションの数が含まれており、新しいセッションが追加された場合にのみ値が増加します。SSL VPN With Client の Peak Concurrent 列には、データを送信中で、同時にアクティブなセッションのピーク数が表示されます。SSL VPN With Client の Inactive 列には、セキュアクライアントが切断されている期間が表示されます。この非アクティブビティタイムアウト値を使用して、ライセンスをいつ期限切れにするかを決定できます。ASA は、再接続が可能かどうかを決定できます。これらは、アクティブな SSL トンネルが関連付けられていないセキュアクライアントセッションです。

表 14-3 に、Active Sessions テーブルと Session Information テーブルにあるフィールドの説明を示します。

表 3: show vpn-sessiondb summary コマンド : Active Sessions および Session Information のフィールド

フィールド	説明
Concurrent Limit	この ASA 上で許可された、同時にアクティブなセッションの最大数。
Cumulative Sessions	ASA が最後に起動またはリセットされたとき以降のすべてのタイプのセッション数。
LAN-to-LAN	現在アクティブな IPsec LAN-to-LAN セッションの数。
Peak Concurrent	ASA が最後に起動またはリセットされたとき以降に同時に有効（アクティブおよび非アクティブ）であった、すべてのタイプのセッションの最大数。
Percent Session Load	<p>使用中の vpn セッション割り当てのパーセンテージ。この値は、Total Active Sessions を利用可能なセッションの最大数で除算した値に等しく、パーセンテージで表示されます。利用可能なセッションの最大数は、次のいずれかの値です。</p> <ul style="list-style-type: none"> <li>• ライセンスのある IPsec セッションおよび SSL VPN セッションの最大数</li> <li>• <b>vpn-sessiondb ?</b>（設定された最大セッション数）</li> <li>• <b>max-anyconnect-premium-or-essentials-limit</b>（AnyConnect Premium または AnyConnect Essentials セッションの最大制限）</li> <li>• <b>max-other-vpn-limit</b>（その他の VPN セッションの最大制限）</li> </ul>
Remote Access	ra-ikev1-ipsec : 現在アクティブな IKEv1 IPsec リモートアクセスユーザー、L2TP over IPsec、および IPsec through NAT セッションの数。

例

フィールド	説明
Total Active Sessions	現在アクティブなすべてのタイプのセッションの数。

Active NAC Sessions テーブルには、ポストチャ検証の対象であるリモートピアに関する一般的な統計情報が表示されます。

Cumulative NAC Sessions テーブルには、ポストチャ検証の対象である、または以前から対象であったリモートピアに関する一般的な統計情報が表示されます。

表 14-2 に、Active NAC Sessions テーブルおよび Total Cumulative NAC Sessions テーブルにあるフィールドの説明を示します。

表 4: show vpn-sessiondb summary コマンド : Active NAC Sessions および Total Cumulative NAC Sessions のフィールド

フィールド	説明
Accepted	ポストチャ検証が成功し、Access Control Server によってアクセス ポリシーが付与されたピアの数。
Exempted	ASA 上に設定されたポストチャ検証免除リストのエントリに一致しているため、ポストチャ検証の対象とならないピアの数。
Hold-off	ASA がポストチャ検証に成功した後、EAPoUDP 通信が途絶えたピアの数。このタイプのイベントが発生してから各ピアに対して次にポストチャ検証が試行されるまでの遅延は、NAC Hold Timer 属性 ([Configuration] > [VPN] > [NAC]) によって決まります。
該当なし	VPN NAC グループ ポリシーに従って NAC がディセーブルになっているピアの数。
Non-responsive	ポストチャ検証のための拡張認証プロトコル (EAP) over UDP 要求に応答しないピアの数。CTA が実行されていないピアは、この要求に応答しません。ASA のコンフィギュレーションがクライアントレス ホストをサポートしている場合、Access Control Server は、クライアントレス ホストに関連付けられているアクセス ポリシーをこれらのピアの ASA にダウンロードします。クライアントレス ホストをサポートしていない場合、ASA は NAC デフォルト ポリシーを割り当てます。
Rejected	ポストチャ検証に失敗したか、または Access Control Server によってアクセス ポリシーが付与されなかったピアの数。

Active VLAN Mapping Sessions テーブルには、ポストチャ検証の対象であるリモートピアに関する一般的な統計情報が表示されます。

Cumulative VLAN Mapping Sessions テーブルには、ポストチャ検証の対象である、または以前から対象であったリモートピアに関する一般的な統計情報が表示されます。

表 14-5 に、Active VLAN Mapping Sessions テーブルおよび Cumulative VLAN Mapping Sessions テーブルにあるフィールドの説明を示します。

表 5: `show vpn-sessiondb summary` コマンド : **Active VLAN Mapping Sessions** および **Cumulative Active VLAN Mapping Sessions** のフィールド

フィールド	説明
アクセス	将来的な使用のために予約されています。
認証	将来的な使用のために予約されています。
Guest	将来的な使用のために予約されています。
該当なし	将来的な使用のために予約されています。
Quarantine	将来的な使用のために予約されています。
スタティック	このフィールドには、事前設定された VLAN に割り当てられている VPN セッションの数が表示されます。

#### 関連コマンド

コマンド	説明
<code>show vpn-sessiondb</code>	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
<code>show vpn-sessiondb ratio</code>	VPN セッションの暗号化またはプロトコルの比率を表示します。

# show wccp

Web Cache Communication Protocol (WCCP) に関連するグローバル統計情報を表示するには、特権 EXEC モードで **show wccp** コマンドを使用します。

**show wccp** { **web-cache** | *service-number* } [ *detail* / *view* ]

## 構文の説明

<i>detail</i>	(任意) ルータおよびすべての Web キャッシュに関する情報を表示します。
<i>service-number</i>	(任意) キャッシュが制御する Web キャッシュ サービスグループの ID 番号。指定できる番号の範囲は 0 ~ 256 です。Cisco Cache Engine を使用する Web キャッシュの場合、逆プロキシ サービスの値には 99 を指定します。
<i>view</i>	(任意) 特定のサービス グループの他のメンバーが検出されたかどうかを表示します。
<b>web-cache</b>	Web キャッシュ サービスの統計情報を指定します。

## コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## 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。

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

## コマンド履歴

リリース 変更内容  
ス

7.2(1) このコマンドが追加されました。

## 例

次に、WCCP 情報を表示する例を示します。

```
ciscoasa(config)# show wccp
Global WCCP information:
  Router information:
    Router Identifier:                -not yet determined-
    Protocol Version:                2.0
  Service Identifier: web-cache
    Number of Cache Engines:         0
    Number of routers:               0
    Total Packets Redirected:        0
    Redirect access-list:            foo
```

```
Total Connections Denied Redirect: 0
Total Packets Unassigned: 0
Group access-list: foobar
Total Messages Denied to Group: 0
Total Authentication failures: 0
Total Bypassed Packets Received: 0
ciscoasa(config)#
```

## 関連コマンド

コマンド	説明
<b>wccp</b>	サービスグループを使用して、WCCPのサポートをイネーブルにします。
<b>wccp redirect</b>	WCCP リダイレクションのサポートをイネーブルにします。

# show webvpn anyconnect

ASA にインストールされ、キャッシュメモリにロードされる SSL VPN クライアントイメージに関する情報を表示したり、ファイルをテストして有効なクライアントイメージかどうかを確認したりするには、特権 EXEC モードで `show webvpn anyconnect` コマンドを使用します。

`show webvpn anyconnect` [ *image filename* ]

構文の説明	<b>image filename</b>	SSL VPN クライアント イメージファイルとしてテストするファイルの名前を指定します。
-------	-----------------------	---

コマンド デフォルト このコマンドに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。

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

コマンド履歴	リリー 変更内容 ス
	7.1(1) このコマンドが追加されました。
	8.4(1) コマンドの <b>show webvpn anyconnect</b> 形式が <code>show webvpn svc</code> と置き換わりました。
	9.0(1) マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン キャッシュメモリにロードされ、リモート PC にダウンロード可能な SSL VPN クライアントイメージに関する情報を表示するには、**show webvpn anyconnect** コマンドを使用します。ファイルをテストして有効なイメージかどうかを確認するには、**image filename** のキーワードと引数を使用します。ファイルが有効なイメージではない場合、次のメッセージが表示されます。

```
ERROR: This is not a valid SSL VPN Client image file.
```

例 次に、現在インストールされているイメージに対する `show webvpn anyconnect` コマンドの出力例を示します。

```
ciscoasa# show webvpn anyconnect
```



```

1. windows.pkg 1
SSL VPN Client
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
2. window2.pkg 2
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43

```

次に、有効なイメージに対する **show webvpn anyconnect image filename** コマンドの出力例を示します。

```

ciscoasa(config-webvpn)# show webvpn anyconnect image sslclient-win-1.0.2.127.pkg
This is a valid SSL VPN Client image:
  CISCO STC win2k+ 1.0.0
  1,0,2,127
  Fri 07/22/2005 12:14:45.43

```

#### 関連コマンド

コマンド	説明
<b>anyconnect enable</b>	ASA で SSL VPN クライアントをリモート PC にダウンロードできるようにします。
<b>anyconnect image</b>	セキュリティ アプライアンスがフラッシュ メモリからキャッシュメモリに SSL VPN クライアント ファイルをロードするようにします。クライアント イメージをオペレーティング システムと照合するときに、セキュリティ アプライアンスがクライアント イメージの各部分をリモート PC にダウンロードする順序を指定します。
<b>vpn-tunnel-protocol</b>	SSL VPN クライアントが使用する SSL を含め、リモート VPN ユーザーの特定の VPN トンネル プロトコルをイネーブルにします。

## show webvpn anyconnect external-browser-pkg

シングルサインオン外部ブラウザパッケージファイルに関する情報を表示するには、特権EXECモードで `show webvpn anyconnect external-browser-pkg` コマンドを使用します。

**show webvpn anyconnect external-browser-pkg** [ *package-path* ]

### 構文の説明

*package-path* AnyConnect 外部ブラウザパッケージがインストールされているパスを指定します。

### コマンド デフォルト

このコマンドに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。

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

### コマンド履歴

リリー 変更内容  
ス

9.17(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 webvpn anyconnect external-browser-pkg** コマンドは、AnyConnect 外部ブラウザパッケージに関する情報を表示する場合に使用します。*package-path* キーワードと引数を使用して、パッケージがインストールされているパスを指定します。

### 例

次に、`show webvpn anyconnect external-browser-pkg` コマンドの出力例を示します。

```
ciscoasa# show webvpn anyconnect external-browser-pkg
disk0:/external-sso-98.161.00015-webdeploy-k9.pkg
Cisco AnyConnect External Browser Headend Package
 98.161.00015
Wed 07/15/21 15:49:27.81738
```

## 関連コマンド

コマンド	説明
<b>anyconnect image</b>	セキュリティ アプライアンスがフラッシュ メモリからキャッシュメモリに SSL VPN クライアント ファイルをロードするようにします。クライアント イメージをオペレーティング システムと照合するときに、セキュリティ アプライアンスがクライアント イメージの各部分をリモート PC にダウンロードする順序を指定します。
<b>external-browser</b>	デフォルトのオペレーティングシステムによるシングルサインオン認証を設定します。

## show webvpn csd (廃止)



(注) このコマンドをサポートする最後のリリースは、Version 9.5(1)でした。

CSD がイネーブルかどうかを特定したり、実行コンフィギュレーションの CSD バージョンを表示したり、ホストスキャンパッケージを提供しているイメージを特定したり、ファイルをテストして有効な CSD 配布パッケージかどうかを確認したりするには、特権 EXEC モードで show webvpn csd コマンドを使用します。

**show webvpn csd** [ *image filename* ]

### 構文の説明

*filename* CSD 配布パッケージとしての有効性をテストするファイルの名前を指定します。  
**csd\_n.n.n-k9.pkg** の形式にする必要があります。

### コマンド デフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリース 変更内容

7.1(1) このコマンドが追加されました。

9.5(2) このコマンドは廃止されました。 **show webvpn hostscan** によって置き換えられました。

9.0(1) マルチ コンテキスト モードのサポートが追加されました。

### 例

CSD の動作ステータスを確認するには、**show webvpn csd** コマンドを使用します。CLI は、CSD がインストールされ、イネーブルになっているかどうか、ホストスキャンパッケージがインストールされ、イネーブルになっているかどうかを示すメッセージで応答します。また、CSD パッケージとホストスキャンパッケージの両方がインス

トールされている場合は、どちらのイメージがホストスキャンパッケージを提供しているかも、メッセージに示されます。

```
ciscoasa# show webvpn csd
```

受信する可能性があるメッセージは、次のとおりです。

- Secure Desktop is not installed

Hostscan is not installed

- Secure Desktop version n.n.n.n is currently installed but not enabled

Standalone Hostscan package is not installed (Hostscan is currently installed via the CSD package but not enabled)

- Secure Desktop version n.n.n.n is currently installed and enabled

Standalone Hostscan package is not installed (Hostscan is currently installed and enabled via the CSD package)

「Secure Desktop version n.n.n.n is currently installed ...」というメッセージは、イメージがASAにロードされ、実行コンフィギュレーションにあることを意味します。イメージは、**enabled** または **not enabled** のいずれかになります。webvpn コンフィギュレーションモードを開始し、**csd enable** コマンドを入力することで、CSD をイネーブルにすることができます。

メッセージ「(Hostscan is currently installed and enabled via the CSD package)」は、CSD パッケージとともに提供されたホストスキャンパッケージが使用中のホストスキャンパッケージであることを意味します。

- Secure Desktop version n.n.n.n is currently installed and enabled

Hostscan version n.n.n.n is currently installed and enabled

「Secure Desktop version n.n.n.n is currently installed and enabled Hostscan version n.n.n.n is currently installed and enabled」というメッセージは、CSD と、スタンドアロンパッケージまたはセキュアクライアントイメージの一部として配布されたホストスキャンパッケージの両方がインストールされていることを意味します。ホストスキャンが有効で、ホストスキャンを使用する CSD およびセキュアクライアントイメージの両方またはスタンドアロンのホストスキャンパッケージがインストールされ、有効になっている場合、スタンドアロンパッケージとして、またはセキュアクライアントイメージの一部として提供されるホストスキャンパッケージは、CSD パッケージに付属しているパッケージよりも優先されます。

- Secure Desktop version n.n.n.n is currently installed but not enabled

Hostscan version n.n.n.n is currently installed but not enabled

ファイルをテストして、CSD 配布パッケージが有効かどうかを確認するには、**show webvpn csd image filename** コマンドを使用します。

```
ciscoasa# show webvpn csd image csd_n.n.n-k9.pkg
```

このコマンドが入力されると、CLI は次のいずれかのメッセージで応答します。

- ERROR: This is not a valid Secure Desktop image file.

ファイル名は必ず **csd\_n.n.n\_k9.pkg** の形式にしてください。CSD パッケージがこの命名規則に従っていない場合、次の Web サイトから取得したファイルに置き換えます。

<http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop>

その後 **show webvpn csd image** コマンドを再入力します。イメージが有効な場合は、webvpn コンフィギュレーション モードで **csd image** コマンドおよび **csd enable** コマンドを使用し、CSD をインストールしてイネーブルにします。

- This is a valid Cisco Secure Desktop image:

Version : 3.6.172.0

Hostscan Version : 3.6.172.0

Built on : Wed Feb 23 15:46:44 MST 2011

ファイルが有効な場合は、CLI にバージョンおよび日付スタンプが表示されます。

#### 関連コマンド

コマンド	説明
csd enable	管理およびリモートユーザー アクセスの CSD をイネーブルにします。
csd image	コマンドに指定された CSD イメージを、パスに指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。

# show webvpn debug-condition

WebVPN デバッグフィルタに関する情報を表示するには、特権 EXEC モードで **show webvpn debug-condition** コマンドを使用します。

## show webvpn debug-condition

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンドデフォルト

このコマンドに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。

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

### コマンド履歴

リリース 変更内容  
ス

9.14 コマンドが追加されました。

### 使用上のガイドライン

**show webvpn debug-condition** コマンドを入力する場合は、WebVPN が実行されている必要があります。

### 例

次に、webvpn デバッグフィルタに関する情報の例を示します。

```
ciscoasa#show webvpn debug-condition
INFO: Webvpn conditional debug is turned OFF
```

# show webvpn group-alias

特定のトンネルグループまたはすべてのトンネルグループのエイリアスを表示するには、特権 EXEC モードで **group-alias** コマンドを使用します。

**show webvpn group-alias** [ *tunnel-group* ]

## 構文の説明

*tunnel-group* (任意) グループエイリアスを表示する特定のトンネルグループを指定します。

## コマンド デフォルト

トンネルグループ名が入力されなかった場合は、すべてのトンネルグループのすべてのエイリアスが表示されます。

## 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。

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

## コマンド履歴

リリース 変更内容

7.1 このコマンドが追加されました。

9.0 マルチコンテキストモー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 webvpn group-alias** コマンドを入力する場合は、WebVPN が実行されている必要があります。

各トンネルグループには複数のエイリアスがあることも、エイリアスがまったくないこともあります。

## 例

次に、トンネルグループ「devtest」のエイリアスを表示する **show webvpn group-alias** コマンドと、このコマンドの出力例を示します。

```
ciscoasa# show webvpn group-alias devtest
QA
Fra-QA
```

## 関連コマンド

コマンド	説明
group-alias	グループに対して1つ以上の URL を指定します。



コマンド	説明
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

# show webvpn group-url

特定のトンネルグループまたはすべてのトンネルグループの URL を表示するには、特権 EXEC モードで **group-url** コマンドを使用します。

**show webvpn group-url** [ *tunnel-group* ]

## 構文の説明

*tunnel-group* (任意) URL を表示する特定のトンネルグループを指定します。

## コマンド デフォルト

トンネルグループ名が入力されなかった場合は、すべてのトンネルグループのすべての URL 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。

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

## コマンド履歴

リリース 変更内容  
ス

7.1(1) このコマンドが追加されました。

9.0(1) マルチコンテキストモー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 webvpn group-url** コマンドを入力する場合は、WebVPN が実行されている必要があります。各グループには複数の URL があることも、URL がまったくないこともあります。

## 例

次に、トンネルグループ「frn-eng1」の URL を表示する **show webvpn group-url** コマンドと、このコマンドの出力例を示します。

```
ciscoasa# show webvpn group-url
http://www.cisco.com
https://fra1.example.com
https://fra2.example.com
```

## 関連コマンド

コマンド	説明
group-url	グループに対して 1 つ以上の URL を指定します。

コマンド	説明
tunnel-group webvpn-attributes	WebVPN トンネルグループ属性を設定する設定 webvpn モードを開始します。

## show webvpn hostscan

ホストスキャンが有効かどうかを特定したり、実行コンフィギュレーションのホストスキャンバージョンを表示したり、ホストスキャンパッケージを提供しているイメージを特定したり、ファイルをテストして有効なホストスキャン配布パッケージかどうかを確認したりするには、特権 EXEC モードで `show webvpn hostscan` コマンドを使用します。

`show webvpn hostscan` [ *image filename* ]

### 構文の説明

*filename* ホストスキャン配布パッケージとしての有効性をテストするファイルの名前を指定します。**hostscan\_4.1.04011-k9.pkg** の形式にする必要があります。

### コマンド デフォルト

デフォルトの動作や値はありません。

### 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。

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

### コマンド履歴

リリース 変更内容  
ス

9.5(2) このコマンドが追加されました。

9.0(1) マルチコンテキストモードのサポートが追加されました。

### 例

ホストスキャンの動作ステータスを確認するには、**show webvpn hostscan** コマンドを使用します。CLI は、ホストスキャンがインストールされているかどうか、それが有効になっているかどうか、どのイメージがホストスキャンパッケージを提供しているかを示すメッセージで応答します。

```
ciscoasa# show webvpn hostscan
```

受信する可能性があるメッセージは、次のとおりです。

- Hostscan is not installed
- Hostscan n.n.n is currently installed and enabled

「Hostscan version n.n.n is currently installed ...」というメッセージは、イメージが ASA にロードされ、実行コンフィギュレーションに含まれていることを意味します。イメージは、**enabled** または **not enabled** のいずれかになります。webvpn コンフィギュレーションモードを開始し、**hostscan enable** コマンドを入力することで、CSD をイネーブルにすることができます。

- Hostscan version n.n.n is currently installed but not enabled

ファイルをテストして、ホストスキャン配布パッケージが有効かどうかを確認するには、**show webvpn hostscan image filename** コマンドを使用します。

```
ciscoasa# show webvpn hostscan image hostscan_4.1.04011-k9.pkg
```

このコマンドが入力されると、CLI は次のいずれかのメッセージで応答します。

- ERROR: This is not a valid Hostscan image file.

ファイル名は必ず **hostscan\_n.n.n-k9.pkg** の形式にしてください。ホストスキャンパッケージにこの命名規則が使用されていない場合は、使用しているセキュアクライアントのバージョンに適したファイルを Cisco ダウンロードサイトから取得して置き換えます。

その後 **show webvpn hostscan image** コマンドを再入力します。イメージが有効な場合は、webvpn コンフィギュレーションモードで **hostscan image** コマンドと **hostscan enable** コマンドを使用して、ホストスキャンをインストールして有効にします。

- This is a valid Hostscan image:

Version : 4.1.4011

Built on : Mon July 27 15:46:44 MST 2015

ファイルが有効な場合は、CLI にバージョンおよび日付スタンプが表示されます。

## 関連コマンド

コマンド	説明
hostscan enable	管理およびリモートユーザー アクセスのホストスキャンをイネーブルにします。
hostscan image	コマンドに指定されたホストスキャンイメージを、パスに指定されたフラッシュドライブから実行コンフィギュレーションにコピーします。

# show webvpn hsts

ASA の HTTP Strict-Transport-Security (HSTS) に関する情報を表示するには、特権 EXEC モードで **show webvpn hsts** コマンドを使用します。

**show webvpn hsts host** { **all** | **name** *hsts\_hostname* }

## 構文の説明

**all** すべての HSTS ホストに関する情報を表示します。

**name** 特定の HSTS ホストに関する情報を表示します。

*hsts\_hostname* 特定の HSTS ホストを指定します。

## コマンド デフォルト

このコマンドに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。

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

## コマンド履歴

リリース 変更内容  
ス

9.14 コマンドが追加されました。

## 使用上のガイドライン

**show webvpn hsts** コマンドを入力する場合は、WebVPN が実行されている必要があります。

## 例

次の例では、すべての HSTS ホストに関する情報を示します。

```
ciscoasa#show webvpn hsts all
```

## show webvpn kcd

ASA のドメインコントローラの情報およびドメイン参加ステータスを表示するには、webvpn コンフィギュレーション モードで **show webvpn kcd** コマンドを使用します。

### show webvpn kcd

#### 構文の説明

なし。

#### コマンドデフォルト

このコマンドにはデフォルトはありません。

#### 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。

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

#### コマンド履歴

リリース 変更内容  
ス

8.4(1) このコマンドが追加されました。

9.0(1) マルチコンテキストモードのサポートが追加されました。

#### 使用上のガイドライン

webvpn コンフィギュレーション モードで **show webvpn kcd** コマンドを使用すると、ASA のドメインコントローラの情報およびドメイン参加ステータスが表示されます。

#### 例

次に、**show webvpn kcd** コマンドで注意する必要がある重要な詳細と、ステータスメッセージの解釈の例を示します。

次に、登録が進行中で終了していない例を示します。

```
ciscoasa# show webvpn kcdKerberos Realm: CORP.TEST.INTERNALDomain Join: In-Progress
```

次に、登録が成功し、ASA がドメインに参加している例を示します。

```
ciscoasa# show webvpn kcd
Kerberos Realm: CORP.TEST.INTERNALDomain Join: Complete
```

## 関連コマンド

コマンド	説明
<b>clear aaa kerberos</b>	ASA でキャッシュされたすべての Kerberos チケットをクリアします。
kcd-server	ASA は Active Directory ドメインに参加できます。
<b>show aaa kerberos</b>	ASA でキャッシュされているすべての Kerberos チケットを表示します。



# show webvpn mus

モバイルユーザー セキュリティ (MUS) に関する情報を表示するには、特権 EXEC モードで **show webvpn mus** コマンドを使用します。

## show webvpn mus

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンドデフォルト

このコマンドに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。

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

### コマンド履歴

リリース 変更内容  
ス

9.14 コマンドが追加されました。

### 使用上のガイドライン

**show webvpn mus** コマンドを入力する場合は、WebVPN が実行されている必要があります。

### 例

次に、モバイルユーザー セキュリティに関する情報の例を示します。

```
ciscoasa#show webvpn mus
No active WSA connections
```

# show webvpn saml

SAML ID プロバイダーに関する情報を表示するには、特権 EXEC モードで **show webvpn saml idp** コマンドを使用します。

## show webvpn saml idp

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンド デフォルト

このコマンドに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。

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

### コマンド履歴

リリース 変更内容  
ス

9.14 コマンドが追加されました。

### 使用上のガイドライン

**show webvpn saml idp** コマンドを入力する場合は、WebVPN が実行されている必要があります。

### 例

次に、SAML ID プロバイダーに関する情報の例を示します。

```
ciscoasa#show webvpn saml idp
```

# show webvpn sso-server (廃止)



(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

WebVPN シングルサインオンサーバーに関する運用統計情報を表示するには、特権 EXEC モードで **show webvpn sso-server** コマンドを使用します。

**show webvpn sso-server** [ *name* ]

## 構文の説明

*name* (任意) SSO サーバーの名前を指定します。サーバー名の長さは 4 ~ 31 文字にする必要があります。

## コマンドデフォルト

デフォルトの値や動作はありません。

## 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。

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

## コマンド履歴

リリース 変更内容

7.1(1) このコマンドが追加されました。

9.5(2) SAML 2.0 がサポートされたため、このコマンドは廃止されました。

9.0(1) マルチ コンテキスト モードのサポートが追加されました。

## 使用上のガイドライン

シングルサインオンは、WebVPN でのみサポートされています。これにより、ユーザーはユーザー名とパスワードを一度だけ入力すれば、別のサーバーでさまざまなセキュアなサービスにアクセスできます。**show webvpn sso-server** コマンドは、セキュリティ デバイスに設定されているすべての SSO サーバーの運用統計情報を表示します。

SSO サーバー名引数が入力されていない場合は、すべての SSO サーバーの統計情報が表示されます。

## 例

次に、特権 EXEC モードでコマンドを入力し、タイプが SiteMinder、名前が example である SSO サーバーの統計情報を表示する例を示します。

```
ciscoasa# show webvpn sso-server example
Name: example
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL: http://www.example.com/webvpn
Number of pending requests:      0
Number of auth requests:         0
Number of retransmissions:       0
Number of accepts:               0
Number of rejects:               0
Number of timeouts:              0
Number of unrecognized responses: 0
ciscoasa#
The following example of the command issued without a specific SSO server name, displays
statistics for all configured SSO servers on the ASA:
ciscoasa#(config-webvpn)# show webvpn sso-server
Name: high-security-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:      0
Number of auth requests:         0
Number of retransmissions:       0
Number of accepts:               0
Number of rejects:               0
Number of timeouts:              0
Number of unrecognized responses: 0
Name: my-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:      0
Number of auth requests:         0
Number of retransmissions:       0
Number of accepts:               0
Number of rejects:               0
Number of timeouts:              0
Number of unrecognized responses: 0
Name: server
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL:
Number of pending requests:      0
Number of auth requests:         0
Number of retransmissions:       0
Number of accepts:               0
Number of rejects:               0
Number of timeouts:              0
Number of unrecognized responses: 0
ciscoasa(config-webvpn)#
```

## 関連コマンド

コマンド	説明
max-retry-attempts	SSO 認証に失敗した場合に ASA が再試行する回数を設定します。
policy-server-secret	SiteMinder-type SSO サーバーへの認証要求の暗号化に使用される秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
sso-server	シングルサインオンサーバーを作成します。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバーの URL を指定します。

## show webvpn statistics

WebVPN イベントの統計情報を表示するには、特権 EXEC モードで **show webvpn statistics** コマンドを使用します。

### show webvpn statistics

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンド デフォルト

このコマンドに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。

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

#### コマンド履歴

リリース 変更内容  
ス

9.14 コマンドが追加されました。

#### 使用上のガイドライン

**show webvpn statistics** コマンドを入力する場合は、WebVPN が実行されている必要があります。

#### 例

次に、WebVPN イベントの統計情報に関する情報の例を示します。

```
ciscoasa#show webvpn statistics
Total number of objects served          0
html                                     0
js                                       0
css                                      0
vb                                       0
java archive                            0
java class                              0
image                                    0
undetermined                             0
Server compression statistics
Decompression success from server        0
Unsolicited compression from server     0
Unsupported compression algorithm used by server 0
Decompression failure for server responses 0
IOBuf failure statistics
uib_create_with_channel                  0
```

```
uib_create_with_string          0
uib_create_with_string_and_channel 0
uib_transfer                    0
uib_add_filter                  0
uib_yyread                     0
uib_read                       0
uib_set_buffer_max             0
uib_set_eof_symbol            0
    uib_get_capture_handle      0
    uib_set_capture_handle      0
    uib_bufflen                 0
    uib_bufptr                  0
    uib_buf_endptr             0
    uib_get_buf_offset         0
    uib_get_buf_offset_addr    0
    uib_get_nth_char           0
    uib_consume                 0
    uib_advance_bufptr         0
```

## show xlate

NAT セッション (xlates) の情報を表示するには、特権 EXEC モードで **show xlate** コマンドを使用します。

```
show xlate [ global ip1 [ -ip2 ] [ netmask mask ] ] [ local ip1 [ -ip2 ] [ netmask mask ] ] [ gport port1 [ -port2 ] ] [ lport port1 [ -port2 ] ] [ interface if_name ] [ type type ]
```

### 構文の説明

<b>count</b>	変換数を表示します。
<b>global</b> <i>ip1</i> [ <i>-ip2</i> ]	(任意) アクティブな変換をマッピングされた IP アドレスまたはアドレスの範囲別に表示します。
<b>gport</b> <i>port1</i> [ <i>-port2</i> ]	(任意) アクティブな変換をマッピングされたポートまたはポートの範囲別に表示します。
<b>interface</b> <i>if_name</i>	(任意) アクティブな変換をインターフェイス別に表示します。
<b>local</b> <i>ip1</i> [ <i>-ip2</i> ]	(任意) アクティブな変換を実際の IP アドレスまたはアドレスの範囲別に表示します。
<b>lport</b> <i>port1</i> [ <i>-port2</i> ]	(任意) アクティブな変換を実際のポートまたはポートの範囲別に表示します。
<b>netmask</b> <i>mask</i>	(任意) マッピングされた、または実際の IP アドレスを限定するネットワーク マスクを指定します。
<b>type</b> <i>type</i>	(任意) アクティブな変換をタイプ別に表示します。次のタイプを 1 つ以上入力できます。 <ul style="list-style-type: none"> <li>• <b>static</b></li> <li>• <b>portmap</b></li> <li>• <b>dynamic</b></li> <li>• <b>twice-nat</b></li> </ul> 複数のタイプを指定する場合は、タイプをカンマで区切ります。

**コマンド デフォルト** デフォルトの動作や値はありません。

**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。



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

## コマンド履歴

リリース 変更内容

8.3(1) このコマンドは、新しい NAT 実装をサポートするように変更されました。

8.4(3) 拡張 PAT の使用を表示するために **e** フラグが追加されました。また、**xlate** が拡張された宛先アドレスが表示されます。

9.0(1) このコマンドは、IPv6 をサポートするように変更されました。

## 使用上のガイドライン

**show xlate** コマンドは、変換スロットの内容を表示します。

**vpnclient** クライアント コンフィギュレーションがイネーブルで、内部ホストが DNS 要求を送信している場合に **show xlate** コマンドを実行すると、1つのスタティック変換に対応する複数の **xlate** が表示されることがあります。

ASA クラスタリング環境では、PAT セッションを処理するために、最大 3 つの **xlate** が、クラスタ内の異なるノードに複製される可能性があります。1つの **xlate** は、接続を所有するユニットで作成されます。1つの **xlate** は、PAT アドレスをバックアップするために別のユニットで作成されます。最後の 1 つの **xlate** は、フローを複製するディレクタにあります。バックアップとディレクタが同じユニットである場合、3 つではなく 2 つの **xlate** が作成されることがあります。

宛先変換を指定せずに 2 回 NAT ルールを作成すると、システムはそれをあらゆるアドレスに対する静的変換と解釈します。そのため、NAT テーブルには、0.0.0.0/0 から 0.0.0.0/0 への変換が含まれます。このルールは、2 度目の NAT ルールから暗黙的に示されます。

## 例

次に、**show xlate** コマンドの出力例を示します。

```
ciscoasa# show xlate
5 in use, 5 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
NAT from any:10.90.67.2 to any:10.9.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.90.67.2 to any:10.86.94.0
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.9.0.9, 10.9.0.10/31, 10.9.0.12/30,
10.9.0.16/28, 10.9.0.32/29, 10.9.0.40/30,
10.9.0.44/31 to any:0.0.0.0
    flags idle 277:05:26 timeout 0:00:00
```

```
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
  flags idle 277:05:14 timeout 0:00:00
```

次に、**e - extended** フラグと **xlate** が拡張されている宛先アドレスの使用を示す **show xlate** コマンドの出力例を示します。

```
ciscoasa# show xlate
1 in use, 1 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
ICMP PAT from inside:10.2.1.100/6000 to outside:172.16.2.200/6000(172.16.2.99)
  flags idle 0:00:06 timeout 0:00:30
TCP PAT from inside:10.2.1.99/5 to outside:172.16.2.200/5(172.16.2.90)
  flags idle 0:00:03 timeout 0:00:30
UDP PAT from inside:10.2.1.101/1025 to outside:172.16.2.200/1025(172.16.2.100)
  flags idle 0:00:10 timeout 0:00:30
```

次に、IPv4 から IPv6 への変換を示す **show xlate** コマンドの出力例を示します。

```
ciscoasa# show xlate
1 in use, 2 most used
NAT from outside:0.0.0.0/0 to in:2001::/96
  flags sT idle 0:16:16 timeout 0:00:00
```

#### 関連コマンド

コマンド	説明
<b>clear xlate</b>	現在の変換および接続情報をクリアします。
<b>show conn</b>	すべてのアクティブ接続を表示します。
<b>show local-host</b>	ローカルホストネットワーク情報を表示します。
<b>show uauth</b>	現在認証済みのユーザーを表示します。

# show zone

ゾーンID、コンテキスト、セキュリティレベル、およびメンバーを表示するには、特権EXECモードで **show zone** コマンドを使用します。

**show zone** [ *name* ]

## 構文の説明

*name* (任意) **zone** コマンドで設定されたゾーン名を指定します。

## コマンド デフォルト

デフォルトの動作や値はありません。

## 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。

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

## コマンド履歴

リリース 変更内容  
ス

9.3(2) このコマンドが追加されました。

## 使用上のガイドライン

ゾーン設定を表示するには、**show running-config zone** コマンドを使用します。

## 例

**show zone** コマンドについては、次の出力を参照してください。

```
ciscoasa# show zone outside-zone
Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
Zone Member(s) : 2
  outsidel GigabitEthernet0/0
  outside2 GigabitEthernet0/1
```

## 関連コマンド

コマンド	説明
<b>clear configure zone</b>	ゾーンのコンフィギュレーションをクリアします。
<b>clear conn zone</b>	ゾーン接続をクリアします。

コマンド	説明
<b>clear local-host zone</b>	ゾーンのホストをクリアします。
<b>show asp table routing</b>	デバッグ目的で高速セキュリティパステーブルを表示し、各ルートに関連付けられたゾーンを表示します。
<b>show asp table zone</b>	デバッグ目的で高速セキュリティパステーブルを表示します。
<b>show conn long</b>	ゾーンの接続情報を表示します。
<b>show local-host zone</b>	ゾーン内のローカルホストのネットワーク状態を表示します。
<b>show nameif zone</b>	インターフェイス名およびゾーン名を表示します。
<b>show route zone</b>	ゾーンインターフェイスのルートを表示します。
<b>show running-config zone</b>	ゾーンのコンフィギュレーションを表示します。
<b>show zone</b>	ゾーンID、コンテキスト、セキュリティレベル、およびメンバーを表示します。
<b>zone</b>	トラフィックゾーンを設定します。
<b>zone-member</b>	トラフィックゾーンにインターフェイスを割り当てます。

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。