CHAPTER 5

wccp コマンド～ zone-member コマンド

wccp

容量を割り当て、サービス グループに参加できるように、指定した Web Cache Communication Protocol（WCCP）サービスのサポートをイネーブルにするには、グローバル コンフィギュレーション モードで **wccp** コマンドを使用します。サービス グループをディセーブルにし、容量の割り当てを解除するには、このコマンドの no 形式を使用します。

wccp {**web-cache** | *service-number*} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]

no wccp {**web-cache** | *service-number*} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [**0** | **7**]]

構文の説明

access-list	アクセス リストの名前を指定します。
group-list	（任意）サービス グループへの参加を許可する Web キャッシュを決定するアクセス リスト。access-list 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。
password	（任意）サービス グループから受信したメッセージに対して Message Digest 5（MD5）認証を指定します。認証で受け入れられなかったメッセージは廃棄されます。
password	認証で使用するパスワードを指定します。password 引数の長さは最大 7 文字です。
redirect-list	（任意）このデバイス グループにリダイレクトされたトラフィックを制御するアクセス リストとともに使用します。access-list 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。アクセス リストには、ネットワーク アドレスだけを含める必要があります。ポート固有のエントリはサポートされていません。

service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 で、255 個まで使用できます。**web-cache** キーワードで指定される Web キャッシュ サービスを含めると、許可される最大数は 256 個です。
web-cache	Web キャッシュ サービスを指定します。 (注) Web キャッシュは、1 つのサービスとしてカウントされます。サービスの最大数（service-number 引数で割り当てられたサービスを含む）は 256 です。

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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、サービス グループに参加できるように WCCP をイネーブルにする例を示します。

```
ciscoasa(config)# wccp web-cache redirect-list jeeves group-list wooster password whatho
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

wccp redirect

Web Cache Communication Protocol（WCCP）を使用したインターフェイスの入口でのパケット リダイレクションをイネーブルにするには、**wccp redirect** コマンドを使用します。WCCP リダイレクションをディセーブルにするには、このコマンドの no 形式を使用します。

wccp interface *interface_name service* **redirect in**

no wccp interface *interface_name service* **redirect in**

構文の説明

in	パケットがこのインターフェイスに着信するときにリダイレクションを実行するように指定します。
interface_name	パケットをリダイレクトするインターフェイスの名前。
service	サービス グループを指定します。**web-cache** キーワードを指定するか、サービスの識別番号（0 ～ 99）を指定できます。

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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、Web キャッシュ サービスの内部インターフェイスでの WCCP リダイレクションをイネーブルにする例を示します。

```
ciscoasa(config)# wccp interface inside web-cache redirect in
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp	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。

web-agent-url（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。

ASA が SiteMinder-type SSO 認証を要求する SSO サーバの URL を指定するには、config-webvpn-sso-siteminder モードで **web-agent-url** コマンドを使用します。

SSO サーバの認証 URL を削除するには、このコマンドの **no** 形式を使用します。

web-agent-url *url*

no web-agent-url *url*

（注） このコマンドは、SiteMinder-type SSO 認証に必要です。

構文の説明

url	SiteMinder-type SSO サーバの認証 URL を指定します。http:// または https:// を含める必要があります。

デフォルト

デフォルトでは、認証 URL は設定されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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、SAML 2.0 のサポートにより廃止されました。

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、ユーザはユーザ名とパスワードを一度だけ入力すれば、さまざまなサーバで各種のセキュアなサービスにアクセスできます。SSO サーバには、認証要求を処理する URL があります。

このコマンドは、SiteMinder-type の SSO サーバにのみ適用されます。

この URL に認証を送信するように ASA を設定するには、**web-agent-url** コマンドを使用します。認証 URL を設定する前に、**sso-server** コマンドを使用して SSO サーバを作成する必要があります。

セキュリティ アプライアンスと SSO サーバ間で https 通信を行うには、SSL 暗号化設定が両側で一致することを確認します。セキュリティ アプライアンスでは、これを **ssl encryption** コマンドで確認します。

例

次に、config-webvpn-sso-siteminder モードで認証 URL として http://www.example.com/webvpn を指定する例を示します。

```
ciscoasa(config-webvpn)# sso-server example type siteminder
ciscoasa(config-webvpn-sso-siteminder)# web-agent-url http://www.example.com/webvpn
ciscoasa(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	ASA が、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder-type SSO サーバ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。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
ssl encryption	SSL/TLS プロトコルで使用される暗号化アルゴリズムを指定します。
sso-server	シングル サインオン サーバを作成します。

web-applications

認証された WebVPN ユーザに表示される WebVPN ホームページの [Web Application] ボックスをカスタマイズするには、webvpn カスタマイゼーション モードで **web-applications** コマンドを使用します。

web-applications {**title** | **message** | **dropdown**} {**text** | **style**} *value*

[**no**] **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

構文の説明

title	タイトルを変更することを指定します。
message	タイトルの下に表示されるメッセージを変更することを指定します。
dropdown	ドロップダウン ボックスを変更することを指定します。
text	テキストを変更することを指定します。
style	HTML スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトルのテキストは「Web Application」です。

デフォルトのタイトルのスタイルは background-color:#99CCCC;color:black;font-weight:bold;text-transform uppercase です。

デフォルトのメッセージのテキストは「Enter Web Address (URL)」です。

デフォルトのメッセージのスタイルは background-color:#99CCCC;color:maroon;font-size:smaller です。

デフォルトのドロップダウンのテキストは「Web Bookmarks」です。

デフォルトのドロップダウンのスタイルは border:1px solid black;font-weight:bold;color:black;font-size:80% です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	• Yes	—	• Yes	—	—

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。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、タイトルを「Applications」に変更し、テキストの色を青に変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# web-applications title text Applications
ciscoasa(config-webvpn-custom)# web-applications title style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。

web-bookmarks

認証された WebVPN ユーザに表示される WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズするには、webvpn カスタマイゼーション モードで **web-bookmarks** コマンドを使用します。

web-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

[**no**] **web-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

構文の説明

link	リンクを変更することを指定します。
title	タイトルを変更することを指定します。
style	HTML スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのリンクのスタイルは color:#669999;border-bottom: 1px solid #669999;text-decoration:none です。

デフォルトのタイトルのスタイルは color:#669999;background-color:#99CCCC;font-weight:bold です。

デフォルトのタイトルのテキストは「Web Bookmarks」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	• Yes	—	• Yes	—	—

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。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[Web Bookmarks] のタイトルを「Corporate Web Bookmarks」にカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] ボックスをカスタマイズします。

webvpn（グローバル）

webvpn モードを開始するには、グローバル コンフィギュレーション モードで **webvpn** コマンドを入力します。このコマンドで入力したコマンドを削除するには、**no webvpn** コマンドを使用します。これらの **webvpn** コマンドは、すべての WebVPN ユーザに適用されます。

これらの **webvpn** コマンドを使用して、AAA サーバ、デフォルト グループ ポリシー、デフォルト アイドル タイムアウト、http プロキシと https プロキシ、WebVPN 用の NBNS サーバ、およびエンド ユーザに表示される WebVPN 画面の外観を設定できます。

webvpn

no webvpn

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。

デフォルト

WebVPN は、デフォルトでは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。

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

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。

使用上のガイドライン

この WebVPN モードでは、WebVPN のグローバル設定を指定できます。グローバル ポリシー モードまたはユーザ名モードから WebVPN モードを開始した場合は、特定のユーザまたはグループ ポリシーの WebVPN コンフィギュレーションをカスタマイズできます。ASA クライアントレス SSL VPN 設定は、それぞれ 1 つの http-proxy コマンドと 1 つの https-proxy コマンドのみサポートしています。

（注） WebVPN が機能するためには、ブラウザ キャッシングをイネーブルにする必要があります。

例

次に、WebVPN コマンド モードを開始する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#
```

webvpn（グループポリシー属性、ユーザ名属性）

この webvpn モードを開始するには、グループポリシー属性コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードで **webvpn** コマンドを使用します。webvpn モードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。これらの webvpn コマンドは、設定元のユーザ名またはグループ ポリシーに適用されます。

グループ ポリシーおよびユーザ名に対する webvpn コマンドでは、ファイルへのアクセス、MAPI プロキシ、URL、および WebVPN を介した TCP アプリケーションを定義できます。ACL およびフィルタリングするトラフィックのタイプも指定します。

webvpn

no webvpn

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。

デフォルト

WebVPN は、デフォルトでは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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー属性コンフィギュレーション	• Yes	—	• Yes		—
ユーザ名属性コンフィギュレーション	• Yes	—	• Yes		—

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。

使用上のガイドライン

グローバル コンフィギュレーション モードから webvpn モードを開始した場合は、WebVPN のグローバル設定を指定できます。グループ ポリシー属性コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードで **webvpn** コマンドを使用すると、webvpn コマンドで指定された設定が親コマンドで指定されたグループまたはユーザに適用されます。つまり、ここで説明したグローバル ポリシー モードまたはユーザ名モードから開始した webvpn モードでは、特定のユーザまたはグループ ポリシーの WebVPN コンフィギュレーションをカスタマイズできます。

グループ ポリシー属性モードで特定のグループ ポリシーに対して適用した WebVPN 属性は、デフォルト グループ ポリシーで指定された WebVPN 属性を上書きします。ユーザ名属性モードで特定のユーザに対して適用した WebVPN 属性は、デフォルト グループ ポリシー内およびそのユーザが属しているグループ ポリシー内の WebVPN 属性を上書きします。基本的に、これらのコマンドを使用すると、デフォルト グループまたは指定したグループ ポリシーから継承される設定を調整できます。WebVPN 設定の詳細については、グローバル コンフィギュレーション モードの **webvpn** コマンドに関する説明を参照してください。

次の表に、webvpn グループ ポリシー属性モードおよびユーザ名属性モードで設定できる属性を示します。詳細については、個々のコマンドの説明を参照してください。

属性	説明
auto-signon	WebVPN ユーザのログイン クレデンシャルを内部サーバに自動的に渡すように ASA を設定して、WebVPN ユーザにシングル サインオン方式を提供します。
カスタマイゼーション	適用する設定済み WebVPN カスタマイゼーションを指定します。
deny-message	アクセスが拒否されたときにユーザに表示されるメッセージを指定します。
filter	WebVPN 接続に使用するアクセス リストを指定します。
機能	ファイル アクセスとファイル ブラウジング、MAPI プロキシ、および WebVPN を介した URL エントリを設定します。
homepage	WebVPN ユーザがログインしたときに表示される Web ページの URL を設定します。
html-content-filter	WebVPN セッションでフィルタリングする Java、ActiveX、イメージ、スクリプト、およびクッキーを指定します。
http-comp	使用する HTTP 圧縮アルゴリズムを指定します。
keep-alive-ignore	セッションの更新で無視する最大オブジェクト サイズを指定します。
port-forward	WebVPN アプリケーション アクセスをイネーブルにします。
port-forward-name	エンド ユーザに対する TCP ポート フォワーディングを識別する表示名を設定します。
sso-server	SSO サーバ名を設定します。
svc	SSL VPN クライアント属性を設定します。
url-list	ユーザが WebVPN 経由でアクセスできるサーバと URL のリストを指定します。

例

次に、「FirstGroup」という名前のグループ ポリシーの webvpn モードを開始する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-webvpn)#
```

次に、「test」というユーザ名の webvpn モードを開始する例を示します。

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-webvpn)#
```

関連コマンド

clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy attributes	設定グループ ポリシー モードを開始します。このモードでは、指定したグループ ポリシーへの属性と値の設定、または webvpn モードでのグループの webvpn 属性の設定ができます。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

ホワイトリスト

クラウド Web セキュリティのために、トラフィックのクラスでホワイトリスト アクションを実行するには、クラス コンフィギュレーション モードで **whitelist** コマンドを使用します。クラス コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect scansafe** コマンドを入力し、次に **parameters** コマンドを入力します。ホワイトリスティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ホワイトリスト

no whitelist

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
9.0(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

class-map type inspect scansafe コマンドを使用して、ホワイトリストに記載するトラフィックを識別します。**policy-map type inspect scansafe** コマンドでインスペクション クラス マップを使用し、クラスのホワイトリスト アクションを指定します。**inspect scansafe** コマンドでインスペクション ポリシー マップを呼び出します。

例

次に、HTTP および HTTPS インスペクション ポリシー マップの同じユーザおよびグループをホワイトリストに記載する例を示します。

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
```

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist

ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
http[s]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {primary | backup}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。

who

ASA 上のアクティブな Telnet 管理セッションを表示するには、特権 EXEC モードで **who** コマンドを使用します。

who [*local_ip*]

構文の説明

local_ip	（任意）リストを 1 つの内部 IP アドレスまたはネットワーク アドレス（IPv4 または IPv6）に制限することを指定します。

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。

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

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。

使用上のガイドライン

who コマンドを使用すると、現在 ASA にログインしている各 Telnet クライアントの TTY_ID と IP アドレスを表示できます。

例

次に、クライアントが Telnet セッションを使用して ASA にログインしている場合の **who** コマンドの出力例を示します。

```
ciscoasa# who
0: 100.0.0.2
ciscoasa# who 100.0.0.2
0: 100.0.0.2
ciscoasa#
```

関連コマンド

コマンド	説明
kill	Telnet セッションを終了します。
Telnet	ASA コンソールへの Telnet アクセスを追加して、アイドル タイムアウトを設定します。

window-variation

さまざまなウィンドウ サイズの接続をドロップするには、tcp マップ コンフィギュレーション モードで **window-variation** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

window variation {**allow-connection** | **drop-connection**}

no window variation {**allow-connection** | **drop-connection**}

構文の説明

allow-connection	接続を許可します。
drop-connection	接続をドロップします。

デフォルト

デフォルト アクションは、接続の許可です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **window-variation** コマンドを使用して、ウィンドウ サイズが縮小されたすべての接続をドロップします。

ウィンドウ サイズ メカニズムによって、TCP は大きなウィンドウをアドバタイズでき、続いて、過剰な量のデータを受け入れずに、はるかに小さなウィンドウをアドバタイズできます。TCP 仕様により、「ウィンドウの縮小」は極力避けることが推奨されています。この条件が検出された場合に、接続をドロップできます。

例

次に、さまざまなウィンドウ サイズの接続をすべてドロップする例を示します。

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# window-variation drop-connection
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

wins-server

プライマリおよびセカンダリ WINS サーバの IP アドレスを設定するには、グループ ポリシー コンフィギュレーション モードで **wins-server** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、他のグループ ポリシーから WINS サーバを継承できます。サーバが継承されないようにするには、**wins-server none** コマンドを使用します。

wins-server value {*ip_address*} [*ip_address*] | none

no wins-server

構文の説明

none	WINS サーバをヌル値に設定して、WINS サーバを許可しないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
value *ip_address*	プライマリおよびセカンダリ WINS サーバの IP アドレスを指定します。

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。

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

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。

使用上のガイドライン

wins-server コマンドを発行するたびに、既存の設定が上書きされます。たとえば、WINS サーバ x.x.x.x を設定してから WINS サーバ y.y.y.y を設定すると、2 番めのコマンドによって最初の設定が上書きされ、y.y.y.y が唯一の WINS サーバになります。複数のサーバを設定する場合も同様です。設定済みのサーバを上書きするのではなく、WINS サーバを追加するには、このコマンドを入力するときに、すべての WINS サーバの IP アドレスを含めます。

例

次に、FirstGroup という名前のグループ ポリシーに IP アドレスが 10.10.10.15、10.10.10.30、および 10.10.10.45 の WINS サーバを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

without-csd

特定のユーザがグループ URL テーブル内のいずれかのエントリを入力して VPN セッションを確立する場合に、そのユーザに対して接続ごとのプロファイルに基づく Cisco Secure Desktop の Hostscan アプリケーションの実行を免除するには、トンネル webvpn コンフィギュレーション モードで **without-csd** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

without-csd [**anyconnect**]

no without-csd [**anyconnect**]

構文の説明

anyconnect	（オプション）AnyConnect 接続だけに影響するようにコマンドを変更します。

デフォルト

デフォルト値はありません。インストールしている場合、Hostscan が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.2(1)	**anyconnect** キーワードが追加されました。

使用上のガイドライン

このコマンドを使用すると、ユーザがこの接続プロファイル（CLI ではトンネル グループと呼ばれます）に設定された URL グループ リスト内の URL を入力した場合に、Cisco Secure Desktop の Hostscan アプリケーションがエンドポイントで実行されません。このコマンドを入力すると、これらのセッションのエンドポイント状態が検出されないため、ダイナミック アクセス ポリシー（DAP）コンフィギュレーションを調整する必要があります。

例

次の例では、最初のコマンドでグループ URL を作成しています。「example.com」が ASA のドメイン、「no-csd」が URL の一意の部分です。ユーザがこの URL を入力すると、ASAは、この接続プロファイルをセッションに割り当てます。**group-url** コマンドは、**without-csd** コマンドを有効にするために必要です。**without-csd** コマンドは、ユーザに対して Cisco Secure Desktop の実行を免除します。

```
ciscoasa(config-tunnel-webvpn)# group-url https://example.com/no-csd enable
ciscoasa(config-tunnel-webvpn)# without-csd
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
csd enable	without-csd コマンドが含まれていないすべての接続プロファイルに対して Cisco Secure Desktop をイネーブルにします。
csd image	コマンドで指定された Cisco Secure Desktop イメージを、パスで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。
group-url	この接続プロファイルに固有のグループ URL を作成します。

write erase

スタートアップ コンフィギュレーションを消去するには、特権 EXEC モードで **write erase** コマンドを使用します。実行コンフィギュレーションはそのまま残ります。

write erase

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。

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。

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

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。

使用上のガイドライン

このコマンドは、セキュリティ コンテキスト内ではサポートされません。コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドで指定します。コンテキスト コンフィギュレーションを削除する場合は、ファイルをリモート サーバ（指定されている場合）から手動で削除するか、またはシステム実行スペースで **delete** コマンドを使用してファイルをフラッシュ メモリからクリアできます。

ASAv の場合、このコマンドは**リロード**後に導入設定（初期の仮想導入設定）を復元します。コンフィギュレーションを完全に消去するには、**clear configure all** コマンドを使用します。導入設定を消去し、ASA アプライアンスの場合と同じ工場出荷時のデフォルト設定を適用するには、**configure factory-default** を参照してください。

（注） ASAv は現在実行されているイメージをブートするため、元のブート イメージには戻りません。

リロード前にコンフィギュレーションを保存しないでください。

フェールオーバー ペアの ASAv の場合は、最初にスタンバイ ユニットの電源をオフにします。スタンバイ ユニットがアクティブになることを防ぐために、電源をオフにする必要があります。電源を入れたままにした場合、アクティブ装置の設定を消去すると、スタンバイ装置がアクティブになります。以前のアクティブ ユニットをリロードし、フェールオーバー リンクを介して再接続すると、古い設定は新しいアクティブ ユニットから同期し、必要な導入コンフィギュレーションが消去されます。アクティブ ユニットのリロード後、スタンバイ ユニットの電源をオンにすることができます。その後、導入コンフィギュレーションはスタンバイ ユニットに同期します。

例

次に、スタートアップ コンフィギュレーションを消去する例を示します。

```
ciscoasa# write erase
Erase configuration in flash memory? [confirm] y
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
delete	フラッシュ メモリからファイルを削除します。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

write memory

実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存するには、特権 EXEC モードで **write memory** コマンドを使用します。

write memory [**all** [**/noconfirm**]]

構文の説明

/noconfirm	**all** キーワードを使用するときに、確認プロンプトを表示しません。
all	マルチ コンテキスト モードのシステム実行スペースでこのキーワードを使用すると、すべてのコンテキスト コンフィギュレーションおよびシステム コンフィギュレーションが保存されます。

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。

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

コマンド履歴

リリース	変更内容
7.2(1)	**all** キーワードを使用して、すべてのコンテキスト コンフィギュレーションを保存できるようになりました。

使用上のガイドライン

実行コンフィギュレーションとは、コマンドラインで行ったすべての変更内容を含む、メモリ内にある現在実行中のコンフィギュレーションです。変更内容は、起動時に実行メモリにロードされるスタートアップ コンフィギュレーションに保存した場合、次のリブートまでの間のみ保持されます。シングル コンテキスト モードまたはマルチ コンテキスト モードにおけるシステムのスタートアップ コンフィギュレーションの場所は、**boot config** コマンドを使用して、デフォルトの場所（隠しファイル）から選択した場所に変更できます。マルチ コンテキスト モードの場合、コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドで指定された場所にあります。

マルチ コンテキスト モードでは、各コンテキストで **write memory** コマンドを入力して、現在のコンテキスト コンフィギュレーションを保存できます。すべてのコンテキスト コンフィギュレーションを保存するには、システム実行スペースで **write memory all** コマンドを入力します。コンテキストのスタートアップ コンフィギュレーションは、外部サーバに配置できます。この場合、ASA は、コンフィギュレーションをサーバに戻して保存できない HTTP および HTTPS の URL を除き、**config-url** コマンドで指定されたサーバにコンフィギュレーションを戻して保存します。ASA が **write memory all** コマンドを使用して各コンテキストを保存した後、次のメッセージが表示されます。

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

エラーのためにコンテキストが保存されない場合もあります。エラーについては、次の情報を参照してください。

- メモリ不足のためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- リモートの宛先に到達できないためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- コンテキストがロックされているために保存されない場合は、次のメッセージが表示されます。

  ```
  Unable to save the configuration for the following contexts as these contexts are
  locked.
  context 'a' , context 'x' , context 'z' .
  ```

  コンテキストがロックされるのは、別のユーザがすでにコンフィギュレーションを保存している場合、またはコンテキストを削除している場合のみです。

- スタートアップ コンフィギュレーションが読み取り専用であるために（たとえば、HTTP サーバで）コンテキストが保存されない場合は、他のすべてのメッセージの最後に次のメッセージ レポートが出力されます。

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context 'a' , context 'b' , context 'c' .
  ```

- フラッシュ メモリに不良セクターがあるためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unknown errors
  ```

システムでは、コンテキストのスタートアップ コンフィギュレーションにアクセスするために管理コンテキスト インターフェイスが使用されるため、**write memory** コマンドでも管理コンテキスト インターフェイスを使用します。ただし、**write net** コマンドでは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。

write memory コマンドは、**copy running-config startup-config** コマンドと同じです。

例

次に、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存する例を示します。

```
ciscoasa# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454

19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
ciscoasa#
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

write net

実行コンフィギュレーションを TFTP サーバに保存するには、特権 EXEC モードで **write net** コマンドを使用します。

write net [*server*:[*filename*] | :*filename*]

構文の説明

:*filename*	パスとファイル名を指定します。**tftp-server** コマンドを使用してすでにファイル名を設定してある場合、この引数はオプションです。 ファイル名をこのコマンドと **tftp-server** コマンドで指定した場合、ASA は **tftp-server** コマンドのファイル名をディレクトリとして処理し、**write net** コマンドのファイル名をそのディレクトリの下にファイルとして追加します。 **tftp-server** コマンドの値を上書きするには、パスとファイル名の前にスラッシュを入力します。スラッシュは、パスが tftpboot ディレクトリに対する相対パスではなく、絶対パスであることを示します。このファイル用に生成される URL には、ファイル名パスの前にダブル スラッシュ(//)が含まれます。必要なファイルが tftpboot ディレクトリにある場合は、ファイル名パスに tftpboot ディレクトリへのパスを含めることができます。TFTP サーバでこのタイプの URL がサポートされていない場合は、代わりに **copy running-config tftp** コマンドを使用します。 **tftp-server** コマンドを使用して TFTP サーバのアドレスを指定した場合は、コロン(:)の後にファイル名だけを入力できます。
server:	TFTP サーバの IP アドレスまたは名前を設定します。**tftp-server** コマンドで設定したアドレスがあっても、このアドレスが優先されます。 デフォルトのゲートウェイ インターフェイスは最もセキュリティが高いインターフェイスですが、**tftp-server** コマンドを使用して別のインターフェイス名を設定できます。

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。

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

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。

使用上のガイドライン

実行コンフィギュレーションとは、コマンドラインで行ったすべての変更内容を含む、メモリ内にある現在実行中のコンフィギュレーションです。

マルチ コンテキスト モードの場合、このコマンドは現在のコンフィギュレーションを保存します。1 つのコマンドですべてのコンテキストを保存することはできません。このコマンドを、システムおよび各コンテキストに対して個別に入力する必要があります。**write net** コマンドでは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。ただし、**write memory** コマンドでは、管理コンテキスト インターフェイスを使用してスタートアップ コンフィギュレーションに保存します。これは、システムで、コンテキストのスタートアップ コンフィギュレーションにアクセスするために管理コンテキスト インターフェイスが使用されるからです。

write net コマンドは、**copy running-config tftp** コマンドと同じです。

例

次に、**tftp-server** コマンドで TFTP サーバおよびファイル名を設定する例を示します。

```
ciscoasa# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
ciscoasa# write net
```

次に、**write net** コマンドにサーバとファイル名を設定する例を示します。**tftp-server** コマンドは入力されていません。

```
ciscoasa# write net 10.1.1.1:/configs/contextbackup.cfg
```

次に、**write net** コマンドにサーバとファイル名を設定する例を示します。**tftp-server** コマンドでディレクトリ名が設定され、サーバ アドレスは上書きされます。

```
ciscoasa# tftp-server 10.1.1.1 configs
ciscoasa# write net 10.1.2.1:context.cfg
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
copy running-config tftp	実行コンフィギュレーションを TFTP サーバにコピーします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	他のコマンドで使用するためのデフォルトの TFTP サーバおよびパスを設定します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

write standby

フェールオーバー スタンバイ装置に ASA またはコンテキストの実行コンフィギュレーションをコピーするには、特権 EXEC モードで **write standby** コマンドを使用します。

write standby

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。

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。

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

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。

使用上のガイドライン

このコマンドは、コンフィギュレーションのスタンバイ ユニットまたはスタンバイ フェールオーバー グループと、アクティブなユニットまたはフェールオーバー グループのコンフィギュレーションとの同期が失われた場合にのみ、使用します。通常、この状態は、コマンドがスタンバイ ユニットまたはスタンバイ フェールオーバー グループで直接入力された場合に発生します。

アクティブ/スタンバイ フェールオーバーの場合、アクティブ ユニットで入力された **write standby** コマンドは、スタンバイ ユニットの実行コンフィギュレーションにアクティブ フェールオーバー ユニットの実行コンフィギュレーションを書き込みます。

アクティブ/アクティブ フェールオーバーの場合、**write standby** コマンドは次のように動作します。

- システム実行スペースで **write standby** コマンドを入力した場合は、ASA 上のシステム コンフィギュレーションおよびすべてのセキュリティ コンテキストのコンフィギュレーションがピア ユニットに書き込まれます。これには、スタンバイ状態のセキュリティ コンテキストのコンフィギュレーション情報が含まれています。このコマンドの入力は、フェールオーバー グループ 1 がアクティブ状態の装置上のシステム実行スペースで行う必要があります。
- セキュリティ コンテキストで **write standby** コマンドを入力すると、セキュリティ コンテキストのコンフィギュレーションだけがピア装置に書き込まれます。このコマンドの入力は、セキュリティ コンテキストがアクティブ状態で表示される装置のセキュリティ コンテキストで行う必要があります。

write standby コマンドは、コンフィギュレーションをピア ユニットの実行コンフィギュレーションに複製します。コンフィギュレーションは、スタートアップ コンフィギュレーションに保存されません。コンフィギュレーションの変更をスタートアップ コンフィギュレーションに保存するには、**write standby** コマンドを入力したユニットで **copy running-config startup-config** コマンドを使用します。コマンドはピア ユニットに複製され、コンフィギュレーションはスタートアップ コンフィギュレーションに保存されます。

ステートフル フェールオーバーがイネーブルの場合、**write standby** コマンドは、コンフィギュレーションのレプリケーションが完了した後、状態情報もスタンバイ ユニットに複製します。マルチ コンテキスト モードでは、ステート情報を複製するには、コンテキスト内で **write standby** を入力して状態情報を複製します。

(注) **write standby** コマンドを入力した後、設定が再同期されるまでの間、フェールオーバー インターフェイスが一時的に停止します。また、これにより、フェールオーバー状態のインターフェイスの検出に一時的な障害が発生します。

例

次に、現在の実行コンフィギュレーションをスタンバイ ユニットに書き込む例を示します。

```
ciscoasa# write standby
Building configuration...
[OK]
ciscoasa#
```

関連コマンド

コマンド	説明
failover reload-standby	スタンバイ ユニットを強制的にリブートします。

write terminal

端末で実行コンフィギュレーションを表示するには、特権 EXEC モードで **write terminal** コマンドを使用します。

write terminal

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。

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。

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

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。

使用上のガイドライン

このコマンドは、**show running-config** コマンドと同じです。

例

次に、実行コンフィギュレーションを端末に書き込む例を示します。

```
ciscoasa# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。

xlate block-allocation

キャリアグレードまたは大規模な PAT 向けにポート ブロック割り当ての特性を設定するには、グローバル コンフィギュレーション モードで **xlate block-allocation** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

xlate block-allocation {**size** *value* | **maximum-per-host** *number*}

no xlate block-allocation {**size** *value* | **maximum-per-host** *number*}

構文の説明

size *value*	ブロック割り当てサイズ。これは、各ブロックのポート数です。 指定できる範囲は 32 ～ 4096 です。デフォルトは 512 です。 デフォルトを使用しない場合、選択したサイズが 64,512（1024 ～ 65535 の範囲でのポート数）に均等に分割されることを確認しますそうしなければ、割り当てることができないポートが発生します。たとえば、100 を指定すると 12 個の未使用ポートが生じます。
maximum-per-host *number*	ホスト 1 つあたりに割り当てることができる最大ブロック。制限はプロトコルごとです。そのため、制限 4 は、ホスト 1 つにつき最大 4 つの UDP ブロック、4 つの TCP ブロック、および 4 つの ICMP ブロックの意味になります。 指定できる範囲は 1 ～ 8 です。デフォルトは 4 です。

コマンド デフォルト

デフォルトの割り当てサイズは 512 です。ホスト 1 つあたりのデフォルトの上限値は 4 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.5(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

キャリアグレードまたは大規模な PAT では、NAT に一度に 1 つのポート変換を割り当てるのではなく、各ホストのポート ブロックを割り当てることができます（RFC 6888 を参照）。ポートのブロックを割り当てる場合、ホストからの後続の接続はブロック内の新しい任意選択されたポートを使用します。必要に応じて、元のブロックにすべてのポートに対するアクティブな接続がホストにある場合は、追加のブロックが割り当てられます。ブロックのポートを使用する最後の xlate が削除されると、ブロックが解放されます。

ポート ブロックは、1024 ～ 65535 の範囲でのみ割り当てられます。そのため、小さいポート番号（1 ～ 1023）がアプリケーションに必要な場合、これは機能しません。たとえば、ポート 22（SSH）を要求するアプリケーションは、1024 ～ 65535 の範囲内およびホストに割り当てられたブロック内でマップされるポートを取得します。

xlate block-allocation コマンドは、これらのポート ブロックの特性を設定します。PAT プールの使用時に PAT ルールに従って ポート ブロック割り当てを有効にするには、**nat** コマンドで block-allocation キーワードを使用します。

例

次に、ポート ブロック割り当て特性の変更例と、オブジェクト NAT ルールで PAT プール用にポート ブロック割り当てを実装する例を示します。

```
xlate block-allocation size 128
xlate block-allocation maximum-per-host 6

object network mapped-pat-pool
   range 10.100.10.1 10.100.10.2
object network src_host
   host 10.111.10.15
object network src_host
   nat dynamic pat-pool mapped-pat-pool block-allocation
```

関連コマンド

コマンド	説明
nat（グローバル）	Twice NAT ルールを追加します。
nat（オブジェクト）	オブジェクト NAT ルールを追加します。
show local-host	ホストに割り当てられたポート ブロックを示します。
show running-config xlate	**xlate** 設定を示します。

xlate per-session

Multi-Session PAT を使用するには、グローバル コンフィギュレーション モードで **xlate per-session** コマンドを使用します。Multi-Session PAT ルールを削除するには、このコマンドの **no** 形式を使用します。

xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip operator dest_port*

no xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip operator dest_port*

構文の説明

deny	拒否ルールを作成します。
destination_ip	宛先 IP アドレスについて、次のように設定できます。 • **host** *ip_address*：IPv4 ホスト アドレスを指定します。 • *ip_address mask*：IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。 • *ipv6-address/prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。 • **any4** および **any6**：**any4** は IPv4 トラフィックだけを指定します。**any6** は any6 トラフィックを指定します。
operator dest_port	*operator* は、宛先で使用されるポート番号に一致します。使用できる演算子は、次のとおりです。 • lt：より小さい • gt：より大きい • eq：等しい • neq：等しくない • range：値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200`
operator src_port	（オプション）*operator* は、ソースで使用されるポート番号に一致します。使用できる演算子は、次のとおりです。 • lt：より小さい • gt：より大きい • eq：等しい • neq：等しくない • range：値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200`
permit	許可ルールを作成します。

source_ip	送信元 IP アドレスについて、次のように設定できます。 • **host** *ip_address*：IPv4 ホスト アドレスを指定します。 • *ip_address mask*：IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。 • *ipv6-address/prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。 • **any4** および **any6**：**any4** は IPv4 トラフィックだけを指定します。**any6** は any6 トラフィックを指定します。
tcp	TCP トラフィックを指定します。
udp	UDP トラフィックを指定します。

コマンド デフォルト

デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。次のデフォルト ルールがインストールされています。

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

(注) これらのルールは削除できません。これらのルールは常に、手動作成されたルールの後に存在します。ルールは順番に評価されるので、デフォルト ルールを無効にすることができます。たとえば、これらのルールを完全に反転させるには、次の拒否ルールを追加します。

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(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

Per-session PAT 機能によって PAT の拡張性が向上し、クラスタリングの場合に各メンバー ユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスター ユニットに転送してマスター ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「ヒットエンドラン」トラフィック、たとえば HTTP や HTTPS の場合は、Per-session 機能によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。Per-session 機能を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-session 機能を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。

デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。H.323、SIP、Skinny など、Multi-Session PAT による利点があるトラフィックの場合、Per-Session PAT 拒否ルールを作成して、Per-Session PAT をディセーブルにできます。

Per-Session PAT ルールを追加する場合、ルールはデフォルト ルールの上位に配置されますが、他の手動で作成されたルールの下位に配置されます。ルールは必ず、適用する順序で作成してください。

例

次の例では、H.323 トラフィックのための拒否ルールを作成します。このトラフィックには Multi-Session PAT が使用されるようにするためです。

```
ciscoasa(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
ciscoasa(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

関連コマンド

コマンド	説明
clear configure xlate	**xlate per-session** ルールをクリアします。
nat（グローバル）	Twice NAT ルールを追加します。
nat（オブジェクト）	オブジェクト NAT ルールを追加します。
show running-config xlate	**xlate per-session** ルールを表示します。

zone

トラフィック ゾーンを追加するには、グローバル コンフィギュレーション モードで **zone** コマンドを使用します。ゾーンを削除するには、このコマンドの **no** 形式を使用します。

zone *name*

no zone *name*

構文の説明

name	最大 48 文字でゾーン名を設定します。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• **Yes**	—	• **Yes**	• **Yes**	—

コマンド履歴

リリース	変更内容
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

1 つの *トラフィック ゾーン*に複数のインターフェイスを割り当てることができます。これにより、ゾーン内の任意のインターフェイスで、既存のフローのトラフィックが ASA に出入りできるようになります。この機能により、ASA 上での Equal-Cost Multi-Path（ECMP）ルーティング、および ASA へのトラフィックの複数のインターフェイスにわたる外部ロード バランシングが可能になります。

ゾーンを使用すると、トラフィックはゾーン内のすべてのインターフェイスで出入りを許可されますが、セキュリティ ポリシー自体（アクセス ルール、NAT など）は、ゾーン単位ではなく、インターフェイス単位で適用されます。ゾーン内のすべてのインターフェイスに同じセキュリティ ポリシーを設定すると、そのトラフィックの ECMP およびロード バランシングを適切に実装できます。

最大 256 ゾーンを作成できます。

例

次の例では、4 つのメンバー インターフェイスを含む外部ゾーンを設定します。

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

関連コマンド

コマンド	説明
clear configure zone	ゾーンのコンフィギュレーションをクリアします。
clear conn zone	ゾーン接続をクリアします。
clear local-host zone	ゾーンのホストをクリアします。
show asp table routing	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。
show asp table zone	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。
show conn long	ゾーンの接続情報を表示します。
show local-host zone	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。
show nameif zone	インターフェイス名およびゾーン名を表示します。
show route zone	ゾーン インターフェイスのルートを表示します。
show running-config zone	ゾーンのコンフィギュレーションを表示します。
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します。
zone-member	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。

zonelabs-integrity fail-close

ASA と Zone Labs Integrity ファイアウォール サーバとの間の接続で障害が発生したときに VPN クライアントへの接続が閉じるように ASA を設定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-close** コマンドを使用します。Zone Labs 接続で障害が発生しても VPN 接続を開いたままにするデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

zonelabs-integrity fail-close

no zonelabs-integrity fail-close

構文の説明説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、接続は障害が発生しても開いたままです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

デフォルトでは、プライマリの Zone Labs Integrity ファイアウォール サーバが ASA に応答しない場合も、ASA はプライベート ネットワークとの VPN クライアントの接続を確立します。既存の開いている接続も維持されます。これにより、企業 VPN はファイアウォール サーバで障害が発生しても中断されません。ただし、Zone Labs Integrity ファイアウォール サーバで障害が発生した場合に、VPN 接続を運用可能な状態に維持しないようにするには、**zonelabs-integrity fail-close** コマンドを使用します。

Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生しても ASA によってクライアント VPN 接続が維持されるデフォルト状態に戻すには、**zonelabs-integrity fail-open** コマンドを使用します。

例

次に、Zone Labs Integrity ファイアウォール サーバが応答しない場合、または接続が中断された場合に、VPN クライアント接続を閉じるように ASA を設定する例を示します。

```
ciscoasa(config)# zonelabs-integrity fail-close
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-open	ASA と Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生した後も、ASA への VPN クライアント接続を開いたままにするように指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイアウォール サーバを ASA が到達不能と見なすまでの秒数を指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。

zonelabs-integrity fail-open

ASA と Zone Labs Integrity ファイアウォール サーバとの間の接続で障害が発生した後も、ASA へのリモート VPN クライアント接続を開いたままにするには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-open** コマンドを使用します。Zone Labs サーバ接続で障害が発生した場合に VPN クライアントへの接続を閉じるには、このコマンドの **no** 形式を使用します。

zonelabs-integrity fail-open

no zonelabs-integrity fail-open

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。

デフォルト

デフォルトでは、ASA で Zone Labs Integrity ファイアウォール サーバへの接続が確立または維持されない場合、リモート VPN 接続は開いたままになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

デフォルトでは、プライマリの Zone Labs Integrity ファイアウォール サーバが ASA に応答しない場合も、ASA はプライベート ネットワークとの VPN クライアントの接続を確立します。既存の開いている接続も維持されます。これにより、企業 VPN はファイアウォール サーバで障害が発生しても中断されません。ただし、Zone Labs Integrity ファイアウォール サーバで障害が発生した場合に、VPN 接続を運用可能な状態に維持しないようにするには、**zonelabs-integrity fail-close** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生しても ASA によってクライアント VPN 接続が維持されるデフォルト状態に戻すには、**zonelabs-integrity fail-open** コマンドまたは **no zonelabs-integrity fail-open** コマンドを使用します。

例

次に、Zone Labs Integrity ファイアウォール サーバへの接続で障害が発生しても VPN クライアント接続を開いたままにするデフォルト状態に戻す例を示します。

```
ciscoasa(config)# zonelabs-integrity fail-open
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-close	ASA と Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、ASA が VPN クライアント接続を閉じるように指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイアウォール サーバを ASA が到達不能と見なすまでの秒数を指定します。

zonelabs-integrity fail-timeout

ASA において、何秒経過すると応答のない Zone Labs Integrity ファイアウォール サーバを到達不能であると見なすかを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-timeout** コマンドを使用します。デフォルトのタイムアウト（10 秒）に戻すには、このコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity fail-timeout *timeout*

no zonelabs-integrity fail-timeout

構文の説明

timeout	ASA において、応答のない Zone Labs Integrity ファイアウォール サーバを到達不能であると見なすまでの秒数。設定可能な値の範囲は、5 ～ 20 秒です。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

ASA が指定された秒数待機しても Zone Labs サーバから応答がない場合、サーバは応答不能と見なされます。VPN クライアントへの接続は、デフォルトまたは **zonelabs-integrity fail-open** コマンドの設定に従って開いたままになります。ただし、**zonelabs-integrity fail-close** コマンドが発行されている場合は、ASA で Integrity サーバが応答不能と見なされると接続は閉じます。

例

次に、12 秒経過後にアクティブな Zone Labs Integrity サーバを到達不能と見なすように ASA を設定する例を示します。

```
ciscoasa(config)# zonelabs-integrity fail-timeout 12
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-open	ASA と Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生した後も、ASA への VPN クライアント接続を開いたままにするように指定します。
zonelabs-integrity fail-close	ASA と Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、ASA が VPN クライアント接続を閉じるように指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。

zonelabs-integrity interface

Zone Labs Integrity サーバとの通信で使用する ASA インターフェイスを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity interface** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバのインターフェイスをデフォルト（none）にリセットするには、このコマンドの **no** 形式を使用します。

zonelabs-integrity interface *interface*

no zonelabs-integrity interface

構文の説明

interface	Zone Labs Integrity ファイアウォール サーバが通信する ASA インターフェイスを指定します。これは、多くの場合、**nameif** コマンドで作成されたインターフェイス名です。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール インターフェイスは none に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、IP アドレス範囲 10.0.0.5 ～ 10.0.0.7 を使用して 3 台の Zone Labs Integrity サーバを設定する例を示します。また、これらのコマンドでは、ポート 300 および inside というインターフェイスでサーバをリッスンするように ASA を設定しています。

```
ciscoasa(config)# zonelabs-integrity server-address 10.0.0.5 10.0.0.6 10.0.0.7
ciscoasa(config)# zonelabs-integrity port 300
ciscoasa(config)# zonelabs-integrity interface inside
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するための ASA 上のポートを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続する ASA のポートを指定します。
zonelabs-integrity ssl-client-authentication	ASA による、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity port

Zone Labs Integrity ファイアウォール サーバとの通信で使用する ASA 上のポートを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity port** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバのデフォルト ポート 5054 に戻すには、このコマンドの **no** 形式を使用します。

zonelabs-integrity port *port_number*

no zonelabs-integrity port *port_number*

構文の説明

port	ASA 上の Zone Labs Integrity ファイアウォール サーバのポートを指定します。
port_number	Zone Labs Integrity ファイアウォール サーバのポートの番号。指定できる範囲は、10 ～ 10000 です。

デフォルト

Zone Labs Integrity ファイアウォール サーバのデフォルト ポートは 5054 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

ASA は、**zonelabs-integrity port** コマンドと **zonelabs-integrity interface** コマンドでそれぞれ設定されたポートとインターフェイスで Zone Labs Integrity ファイアウォール サーバをリッスンします。

(注) ユーザ インターフェイスが最大 5 つの Integrity サーバのコンフィギュレーションをサポートしている場合でも、現在のリリースの ASA が一度にサポートする Integrity サーバは 1 つです。アクティブなサーバに障害が発生した場合は、ASA 上で別の Integrity サーバを設定して、クライアント VPN セッションを再確立してください。

例

次に、IP アドレス 10.0.0.5 を使用して Zone Labs Integrity サーバを設定する例を示します。また、これらのコマンドでは、デフォルト ポート 5054 ではなくポート 300 でアクティブな Zone Labs サーバをリッスンするように ASA を設定しています。

```
ciscoasa(config)# zonelabs-integrity server-address 10.0.0.5
ciscoasa(config)# zonelabs-integrity port 300
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するための ASA インターフェイスを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続する ASA のポートを指定します。
zonelabs-integrity ssl-client-authentication	ASA による、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity server-address

Zone Labs Integrity ファイアウォール サーバを ASA コンフィギュレーションに追加するには、グローバル コンフィギュレーション モードで **zonelabs-integrity server-address** コマンドを使用します。Zone Labs サーバを IP アドレスまたはホスト名で指定します。

Zone Labs Integrity ファイアウォール サーバを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity server-address {*hostname1* | *ip-address1*}

no zonelabs-integrity server-address

(注) ユーザ インターフェイスは複数の Integrity サーバのコンフィギュレーションをサポートしているように見えますが、現在のリリースの ASA では同時に 1 台のサーバのみがサポートされます。

構文の説明

hostname	Zone Labs Integrity ファイアウォール サーバのホスト名を指定します。ホスト名のガイドラインについては、**name** コマンドを参照してください。
ip-address	Zone Labs Integrity ファイアウォール サーバの IP アドレスを指定します。

コマンド デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバは設定されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

このリリースでは、1 台の Zone Labs Integrity ファイアウォール サーバを設定できます。そのサーバで障害が発生した場合は、まず別の Integrity サーバを設定してからクライアント VPN セッションを再確立します。

サーバをホスト名で指定するには、まず **name** コマンドを使用して Zone Labs サーバ名を設定する必要があります。**name** コマンドを使用する前に、**names** コマンドを使用してコマンドをイネーブルにします。

(注) 現在のリリースのセキュリティ アプライアンスでは同時に 1 台の Integrity サーバのみがサポートされていますが、ユーザ インターフェイスでは最大 5 台の Integrity サーバの設定がサポートされています。アクティブなサーバに障害が発生した場合は、ASA 上で別の Integrity サーバを設定して、クライアント VPN セッションを再確立してください。

例

次に、IP アドレス 10.0.0.5 にサーバ名 ZL-Integrity-Svr を割り当て、その名前を使用して Zone Labs Integrity サーバを設定する例を示します。

```
ciscoasa(config)# names
ciscoasa(config)# name 10.0.0.5 ZL-Integrity-Svr
ciscoasa(config)# zonelabs-integrity server-address ZL-Integrity-Svr
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-close	ASA と Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、ASA が VPN クライアント接続を閉じるように指定します。
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するための ASA インターフェイスを指定します。
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するための ASA 上のポートを指定します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続する ASA のポートを指定します。
zonelabs-integrity ssl-client-authentication	ASA による、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity ssl-certificate-port

SSL 証明書を取得する場合に Zone Labs Integrity ファイアウォール サーバが接続する ASA のポートを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity ssl-certificate-port** コマンドを使用します。デフォルト ポート番号（80）に戻すには、このコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity ssl-certificate-port *cert-port-number*

no zonelabs-integrity ssl-certificate-port

構文の説明

cert-port-number	SSL 証明書を要求する場合に Zone Labs Integrity ファイアウォール サーバが接続する ASA のポート番号を指定します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバは SSL 証明書を ASA のポート 80 で要求します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

ASA と Zone Labs Integrity ファイアウォール サーバとの SSL 通信では、ASA が SSL サーバであり、Zone Labs サーバは SSL クライアントです。SSL 接続を開始する場合は、SSL サーバ（ASA）の証明書がクライアント（Zone Labs サーバ）によって認証される必要があります。
zonelabs-integrity ssl-certificate-port コマンドで、Zone Labs サーバが SSL サーバ証明書を要求する場合に接続するポートを指定します。

例

次に、ASA のポート 30 で Zone Labs Integrity サーバから SSL 証明書要求を受信するように設定する例を示します。

```
ciscoasa(config)# zonelabs-integrity ssl-certificate-port 30
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するための ASA 上のポートを指定します。
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するための ASA インターフェイスを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。
zonelabs-integrity ssl-client-authentication	ASA による、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity ssl-client-authentication

Zone Labs Integrity ファイアウォール サーバの SSL 証明書を ASA で認証できるようにするには、グローバル コンフィギュレーション モードで **zonelabs-integrity ssl-client-authentication** コマンドを *enable* 引数を指定して使用します。Zone Labs の SSL 証明書の認証をディセーブルにするには、*disable* 引数を使用するか、またはこのコマンドの **no** 形式を引数なしで使用します。

zonelabs-integrity ssl-client-authentication {*enable* | *disable*}

no zonelabs-integrity ssl-client-authentication

構文の説明

disable	Zone Labs Integrity ファイアウォール サーバの IP アドレスを指定します。
イネーブル化	ASA で Zone Labs Integrity ファイアウォール サーバの SSL 証明書を認証することを指定します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバの SSL 証明書の ASA による認証は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。

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

コマンド履歴

リリース	変更内容
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

ASA と Zone Labs Integrity ファイアウォール サーバとの SSL 通信では、ASA が SSL サーバであり、Zone Labs サーバは SSL クライアントです。SSL 接続を開始する場合は、SSL サーバ（ASA）の証明書がクライアント（Zone Labs サーバ）によって認証される必要があります。ただし、クライアント証明書の認証は任意です。Zone Labs サーバの（SSL クライアント）証明書の ASA による認証をイネーブルまたはディセーブルにするには、**zonelabs-integrity ssl-client-authentication** コマンドを使用します。

例

次に、Zone Labs Integrity サーバの SSL 証明書を認証するように ASA を設定する例を示します。

```
ciscoasa(config)# zonelabs-integrity ssl-client-authentication enable
ciscoasa(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するための ASA インターフェイスを指定します。
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するための ASA 上のポートを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバを ASA のコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続する ASA のポートを指定します。

zone-member

トラフィック ゾーンにインターフェイス追加するには、インターフェイス コンフィギュレーション モードで **zone-member** コマンドを使用します。インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

zone-member *name*

no zone-member *name*

構文の説明

name	**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。

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

コマンド履歴

リリース	変更内容
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

名前、IP アドレス、およびセキュリティ レベルを含むすべてのインターフェイス パラメータを設定します。ゾーンに最初に追加するインターフェイスによってゾーンのセキュリティ レベルが決まります。追加のインターフェイスは、すべて同じセキュリティ レベルにする必要があります。ゾーン内のインターフェイスのセキュリティ レベルを変更するには、1 つのインターフェイスを除くすべてのインターフェイスを削除してからセキュリティ レベルを変更し、インターフェイスを再度追加します。

ゾーンにインターフェイスを割り当てる場合、そのインターフェイスのすべての接続が削除されます。接続を再確立する必要があります。

ゾーンからインターフェイスを削除する場合、そのインターフェイスをプライマリ インターフェイスとしているすべての接続が削除されます。接続を再確立する必要があります。そのインターフェイスが現在のインターフェイスの場合、ASA は接続をプライマリ インターフェイスに戻します。ゾーンのルート テーブルも更新されます。

次のタイプのインターフェイスをゾーンに追加できます。

- 物理
- VLAN
- EtherChannel
- Redundant

次のタイプのインターフェイスは追加できません。

- 管理専用
- 管理アクセス
- フェールオーバーまたはステート リンク
- クラスタ制御リンク
- EtherChannel インターフェイスまたは冗長インターフェイスのメンバー インターフェイス

1 つのインターフェイスがメンバーになることができるゾーンは 1 つだけです。

ゾーンごとに最大 8 つのインターフェイスを含めることができます。

例

次の例では、4 つのメンバー インターフェイスを含む外部ゾーンを設定します。

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

関連コマンド

コマンド	説明
clear configure zone	ゾーンのコンフィギュレーションをクリアします。
clear conn zone	ゾーン接続をクリアします。
clear local-host zone	ゾーンのホストをクリアします。
show asp table routing	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。
show asp table zone	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。
show conn long	ゾーンの接続情報を表示します。
show local-host zone	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。
show nameif zone	インターフェイス名およびゾーン名を表示します。
show route zone	ゾーン インターフェイスのルートを表示します。
show running-config zone	ゾーンのコンフィギュレーションを表示します。
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します。
zone	トラフィック ゾーンを設定します。