CHAPTER 13

dnscrypt コマンド～ dynamic-filter whitelist コマンド

dnscrypt

DNScrypt がデバイスと Cisco Umbrella 間の接続を暗号化できるようにするには、DNS インスペクション ポリシー マップのパラメータ コンフィギュレーション モードで **dnscrypt** コマンドを使用します。DNScrypt を無効にするには、このコマンドの **no** 形式を使用します。

dnscrypt

no dnscrypt

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　DNScrypt は無効になっています。

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
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(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

DNS インスペクション ポリシーマップを設定する際に、次のコマンドを使用します。

DNScrypt を有効にすると、Umbrella リゾルバとのキー交換スレッドが開始されます。キー交換スレッドは、1 時間ごとにリゾルバとのハンドシェイクを実行し、新しい秘密鍵でデバイスを更新します。

DNScrypt では UDP/443 を使用するため、そのポートが DNS インスペクションに使用するクラス マップに含まれていることを確認する必要があります。デフォルトのインスペクション クラスには DNS インスペクションに UDP/443 がすでに含まれています。

例

次の例では、デフォルト ポリシーを使用して Umbrella を有効にし、グローバル DNS インスペクションで使用されるデフォルトのインスペクション ポリシーマップで DNScrypt も有効にします。グローバル DNS インスペクションはすでに UDP/443 に適用されています。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt
```

関連コマンド

コマンド	説明
inspect dns	DNS インスペクションをイネーブルにします。
policy-map type inspect dns	DNS インスペクション ポリシー マップを作成します。
public-key	Cisco Umbrella で使用する公開キーを設定します。
token	Cisco Umbrella への登録に必要な API トークンを指定します。
timeout edns	アイドル タイムアウトを設定します。その時間が経過するまでサーバからの応答がない場合、クライアントから Umbrella サーバへの接続は削除されます。
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。
umbrella	DNS インスペクション エンジンで、DNS ルックアップ要求を Cisco Umbrella にリダイレクトできるようにします。

dns domain-lookup

サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信すること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 **dns domain-lookup** コマンドを使用します。DNS 要求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。

(注) ASA では、機能に応じて DNS サーバの使用が限定的にサポートされます。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、**names** コマンドを使用して名前の使用をイネーブルにした場合だけです。

dns domain-lookup *interface_name*

no dns domain-lookup *interface_name*

構文の説明

interface_name	設定されたインターフェイスの名前を指定します。

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
グローバル コンフィギュレーション	• 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)	このコマンドが追加されました。

使用上のガイドライン

DNS ルックアップをイネーブルにした後で、**dns server-group DefaultDNS** サーバ グループ コマンド、次に **name-server** コマンドを使用して DNS サーバを指定します。アクティブなサーバ グループは、**dns-group** コマンドを使用して変更できます。PN トンネル グループ用に他の DNS サーバ グループを設定できます。詳細については、**tunnel-group** コマンドを参照してください。

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック データベース サーバにアクセスして、スタティック データベースのエントリを解決するために DNS サーバが必要です。さらに、Cisco Smart Software Licensing では、ライセンス機関のアドレスの解決に DNS が必要です。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping や traceroute を実行する名前を入力できるため、ASA は DNS サーバと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。また、アクセス ルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するために、DNS サーバを設定する必要もあります。

例

次に、管理インターフェイス、内部インターフェイス、および DMZ インターフェイスに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにする例を示します。

```
ciscoasa(config)# dns domain-lookup management
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns domain-lookup dmz
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.1 management
ciscoasa(config-dns-server-group)# name-server 10.10.1.1 10.20.2.2
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

dns expire-entry-timer

TTL が期限切れになった後で解決された FQDN の IP アドレスを削除するには、グローバル コンフィギュレーション モードで **dns expire-entry-timer** コマンドを使用します。タイマーを削除するには、このコマンドの **no** 形式を使用します。

dns expire-entry-timer minutes *minutes*

no dns expire-entry-timer minutes *minutes*

構文の説明

minutes *minutes*	タイマーの時間を分単位で指定します。有効な値の範囲は、1 ～ 65535 分です。

デフォルト

デフォルトでは、DNS expire-entry-timer 値は 1 分です。

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 モード	• 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)	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、解決された FQDN の IP アドレスが、その TTL の期限切れ後に削除されるまでの時間を指定します。IP アドレスが削除されると、ASA は tmatch ルックアップ テーブルを再コンパイルします。

このコマンドの指定は、DNS に関連するネットワーク オブジェクトがアクティブ化されている場合にのみ有効です。

デフォルトの DNS expire-entry-timer 値は 1 分です。これは、DNS エントリの TTL の期限が切れた 1 分後に IP アドレスが削除されることを意味します。

(注) 一般的な FQDN ホスト（www.sample.com など）の解決 TTL が短時間である場合、デフォルト設定を使用すると、tmatch ルックアップ テーブルが頻繁に再コンパイルされる可能性があります。セキュリティを確保すると同時に tmatch ルックアップ テーブルの再コンパイル頻度を減らすために、長い DNS expire-entry タイマー値を指定できます。

例

次に、解決されたエントリを 240 分後に削除する例を示します。

```
ciscoasa(config)# dns expire-entry-timer minutes 240
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

dns-group

アクティブな DNS グループを指定するには、グローバル コンフィギュレーション モードで **dns-group** コマンドを使用します。トンネル グループごとに DNS サーバ グループを指定するには、トンネル グループ webvpn 属性コンフィギュレーション モードで **dns-group** コマンドを使用します。デフォルトの DNS グループに戻すには、このコマンドの **no** 形式を使用します。

dns-group *name*

no dns-group

構文の説明

name	アクティブな DNS サーバ グループの名前を指定します。

デフォルト

デフォルト値は DefaultDNS 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	• 対応	• 対応	• 対応	• 対応	—
トンネル グループ webvpn 属性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
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

dns server-group コマンドを使用して、DNS グループを設定します。

例

次に、「dnsgroup1」という名前の DNS グループの使用を指定するカスタマイゼーション コマンドの例を示します。

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# dns-group dnsgroup1
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する config-webvpn モードを開始します。

dns-guard

クエリーごとに 1 つの DNS 応答を実行する DNS Guard 機能をイネーブルにするには、パラメータ コンフィギュレーション モードで **dns-guard** コマンドを使用します。この機能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。

dns-guard

no dns-guard

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

DNS Guard は、デフォルトでイネーブルになっています。この機能は、**policy-map type inspect dns** コマンドを定義していなくても、**inspect dns** コマンドを設定していれば、イネーブルにできます。ディセーブルにするには、ポリシー マップ コンフィギュレーションで **no dns-guard** コマンドを明示的に指定する必要があります。**inspect dns** コマンドが設定されていない場合、動作は **global dns-guard** コマンドが決定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 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)	このコマンドが追加されました。

使用上のガイドライン

DNS ヘッダーの ID フィールドを使用して、DNS 応答と DNS ヘッダーを一致させます。クエリーごとに 1 つの応答が ASA を介して許可されます。

例

次に、DNS インスペクション ポリシー マップで DNS Guard をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# dns-guard
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

dns name-server

アクティブな DNS サーバ グループの DNS サーバを設定するには、グローバル コンフィギュレーション モードで **dns name-server** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。このコマンドは、**name-server** コマンドと同等です。

(注) ASA では、機能に応じて DNS サーバの使用が限定的にサポートされます。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、**names** コマンドを使用して名前の使用をイネーブルにした場合だけです。

dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

no dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

構文の説明

ip_address	DNS サーバの IPv4 または IPv6 アドレスを指定します。最大で 6 個のアドレスを指定できます。

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
グローバル コンフィギュレーション	• 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(2)	このコマンドは、**dns server-group DefaultDNS** サーバ グループに DNS サーバを追加するように変更されました。
9.0(1)	IPv6 アドレスのサポートが追加されました。

使用上のガイドライン

DNS 検索をイネーブルにするには、**dns domain-lookup** コマンドを使用します。DNS ルックアップをイネーブルにしないと、DNS サーバは使用されません。

このコマンドは、アクティブな DNS サーバ グループにサーバを追加します。デフォルトでは、アクティブなグループは **DefaultDNS** と呼ばれます。**dns-group** コマンドを使用してアクティブなグループを変更できます。次に結果の設定を示します。

```
ciscoasa(config)# dns name-server 10.1.1.1
ciscoasa(config)# show running-config dns
dns server-group DefaultDNS
    name-server ip_address
```

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック データベース サーバにアクセスして、スタティック データベースのエントリを解決するために DNS サーバが必要です。さらに、Cisco Smart Software Licensing では、ライセンス機関のアドレスの解決に DNS が必要です。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping や traceroute を実行する名前を入力できるため、ASA は DNS サーバと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。また、アクセス ルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するために、DNS サーバを設定する必要もあります。

例

次に、IPv6 アドレスで DNS サーバを設定する例を示します。

```
ciscoasa(config)# dns domain-lookup
ciscoasa(config)# dns name-server 8080:1:2::2
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

dns poll-timer

ネットワーク オブジェクト グループで定義された完全修飾ドメイン名（FQDN）を解決するために、ASA が DNS サーバに照会する期間のタイマーを指定するには、グローバル コンフィギュレーション モードで **dns poll-timer** コマンドを使用します。タイマーを削除するには、このコマンドの **no** 形式を使用します。

dns poll-timer minutes *minutes*

no dns poll-timer minutes *minutes*

構文の説明

minutes *minutes*	タイマーを分単位で指定します。有効な値は、1 ～ 65535 分です。

デフォルト

デフォルトでは、DNS タイマーは 240 分または 4 時間です。

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	• 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)	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、ネットワーク オブジェクト グループで定義された FQDN を解決するために、ASA が DNS サーバに照会する期間のタイマーを指定します。FQDN は、DNS ポーリング タイマーの期限切れ、または、解決された IP エントリの TTL の期限切れのいずれかが発生した時点で解決されます。

このコマンドは、少なくとも 1 つのネットワーク オブジェクト グループがアクティブ化されている場合にのみ有効です。

例

次に、DNS ポーリング タイマーを 240 分に設定する例を示します。

```
ciscoasa(config)# dns poll-timer minutes 240
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

dns-server（グループ ポリシー）

プライマリおよびセカンダリの DNS 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 **dns-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。

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

no dns-server

構文の説明

none	**dns-server** コマンドをヌル値に設定して、DNS サーバが許可されないようにします。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 DNS 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	• 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。

使用上のガイドライン

このコマンドを使用すると、別のグループ ポリシーの DNS 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、**dns-server none** コマンドを使用します。

dns-server コマンドを実行するたびに、既存の設定が上書きされます。たとえば、DNS サーバ x.x.x.x を設定し、次に DNS サーバ y.y.y.y を設定した場合、2 番めのコマンドは最初のコマンドを上書きし、y.y.y.y が唯一の DNS 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。以前に設定された DNS サーバを上書きする代わりに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 DNS サーバの IP アドレスを含めます。

例

次の例は、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 と 10.10.10.45 である DNS サーバを設定する方法を示しています。

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

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
show running-config dns server-group	現在の実行中の DNS サーバ グループ コンフィギュレーションを表示します。

dns-server（IPv6 DHCP プール）

DHCPv6 サーバを設定するときにステートレス アドレス自動設定（SLAAC）クライアントに DNS サーバの IP アドレスを提供するには、IPv6 DHCP プール コンフィギュレーション モードで **dns-server** コマンドを使用します。DNS サーバを削除するには、このコマンドの **no** 形式を使用します。

dns-server *dns_ipv6_address*

no dns-server *dns_ipv6_address*

構文の説明

dns_ipv6_address	DNS サーバの IPv6 アドレスを指定します。

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
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(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

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求（IR）パケットを ASA に送信したときに、DNS サーバを含め、**ipv6 dhcp プール**内の情報を提供するように ASA を設定できます。ASA は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。DHCPv6 ステートレス サーバを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバを有効にする場合は、**ipv6 dhcp プール**名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
    domain-name eng.example.com
    dns-server 2001:DB8:1::1
ipv6 dhcp pool IT-Pool
    domain-name it.example.com
    dns-server 2001:DB8:1::1
interface gigabitethernet 0/0
    ipv6 address dhcp setroute default
    ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
    ipv6 address Outside-Prefix ::1:0:0:0:1/64
    ipv6 dhcp server Eng-Pool
    ipv6 nd other-config-flag
interface gigabitethernet 0/2
    ipv6 address Outside-Prefix ::2:0:0:0:1/64
    ipv6 dhcp server IT-Pool
    ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。

コマンド	説明
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

dns server-group（グローバル）

DNS サーバ グループを作成して設定するには、グローバル コンフィギュレーション モードで **dns server-group** コマンドを使用します。特定の DNS サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

(注) ASA では、機能に応じて DNS サーバの使用が限定的にサポートされます。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、**names** コマンドを使用して名前の使用をイネーブルにした場合だけです。

dns server -group *name*

no dns server-group

構文の説明

name	DNS サーバ グループの名前を指定します。ASA ルックアップのデフォルトのグループ 名は **DefaultDNS** です。

デフォルト

ASA のデフォルトのアクティブ サーバ グループは DefaultDNS 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	• 対応	• 対応	• 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。

使用上のガイドライン

DNS 検索をイネーブルにするには、**dns domain-lookup** コマンドを使用します。DNS ルックアップをイネーブルにしないと、DNS サーバは使用されません。

ASA では、発信要求に **dns server-group DefaultDNS** サーバ グループを使用します。アクティブなサーバ グループは、**dns-group** コマンドを使用して変更できます。VPN トンネル グループ用他の目的のために他の DNS サーバ グループを設定できます。詳細については、**tunnel-group** コマンドを参照してください。

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック データベース サーバにアクセスして、スタティック データベースのエントリを解決するために DNS サーバが必要です。さらに、Cisco Smart Software Licensing では、ライセンス機関のアドレスの解決に DNS が必要です。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping や traceroute を実行する名前を入力できるため、ASA は DNS サーバと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。また、アクセス ルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するために、DNS サーバを設定する必要もあります。

例

次に、「DefaultDNS」という名前の DNS サーバ グループを設定する例を示します。

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# domain-name cisco.com
ciscoasa(config-dns-server-group)# name-server 192.168.10.10
ciscoasa(config-dns-server-group)# retries 5
ciscoasa(config-dns-server-group)# timeout 7
ciscoasa(config-dns-server-group)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
show running-config dns server-group	現在の実行中の DNS サーバ グループ コンフィギュレーションを表示します。

dns-id

参照 ID オブジェクトで cn-id を設定するには、*ca-reference-identity* モードで **dns-id** コマンドを使用します。dns-id を削除するには、このコマンドの **no** 形式を使用します。*ca-reference-identity* モードにアクセスするには、参照 ID オブジェクトを設定するための **crypto ca reference-identity** コマンドを入力します。

dns-id *value*

no dns-id *value*

構文の説明

value	各参照 ID の値。
dns-id	タイプ dNSName の subjectAltName エントリ。これは DNS ドメイン名です。DNS-ID 参照 ID では、アプリケーション サービスは特定されません。

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。

	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
ca-reference-identity	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(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

参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。

参照 ID の **cn ID** と **dns ID** には、アプリケーション サービスを特定する情報を含めることができず、DNS ドメイン名を特定する情報が含まれている必要があります。

例

次に、syslog サーバの参照 ID を作成する例を示します。

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

関連コマンド

コマンド	説明
crypto ca reference-identity	参照 ID オブジェクトを設定します。
cn-id	参照 ID オブジェクトのコモン ネーム ID を設定します。
srv-id	参照 ID オブジェクトで SRV-ID 識別子を設定します。
uri-id	参照 ID オブジェクトの URI ID を設定します。
logging host	セキュアな接続のために参照 ID オブジェクトを使用できるロギング サーバを設定します。
call-home profile destination address http	安全な接続のために参照 ID オブジェクトを使用できる Smart Call Home サーバを設定します。

dns update

DNS ポーリング タイマーの有効期限を待機せずに、指定されたホスト名を解決する DNS ルックアップを開始するには、特権 EXEC モードで **dns update** コマンドを使用します。

dns update [**host** *fqdn_name*] [**timeout seconds** *seconds*]

構文の説明

host *fqdn_name*	DNS アップデートを実行するホストの完全修飾ドメイン名を指定します。
timeout seconds *seconds*	タイムアウトを秒単位で指定します。

デフォルト

デフォルトでは、タイムアウトは 30 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
特権 EXEC モード	• 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)	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、DNS ポーリング タイマーの有効期限を待機しないで、指定されたホスト名を解決する DNS ルックアップをすぐに開始します。オプションを指定せずに DNS アップデートを実行する場合、アクティブ化されたすべてのホスト グループと FQDN ホストが DNS ルックアップ用に選択されます。コマンドの実行が終了すると、ASA のコマンド プロンプトに [Done] と表示され、syslog メッセージが生成されます。

アップデート操作が開始すると、アップデート開始ログが作成されます。アップデート操作が終了するか、またはタイマーが期限切れになってから中断すると、別の syslog メッセージが生成されます。許可される未処理 DNS アップデート操作は 1 つのみです。

例

次に、DNS アップデートを実行する例を示します。

```
ciscoasa# dns update
ciscoasa# …
ciscoasa# [Done] dns update
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

domain-name (dns server-group)

未修飾のホスト名に追加するデフォルトのドメイン名を設定するには、dns server-group コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

domain-name *name*

no domain-name [*name*]

構文の説明

name	ドメイン名を最大 63 文字で設定します。

デフォルト

デフォルト ドメイン名は default.domain.invalid 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
DNS サーバ グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

ASA は、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。

例

次に、ドメインを「dnsgroup1」に対して「example.com」に設定する例を示します。

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# domain-name example.com
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ コンフィギュレーション モードを開始します。

コマンド	説明
domain-name	デフォルトのドメイン名をグローバルに設定します。
show running-config dns-server group	現在の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

domain-name（グローバル）

デフォルトのドメイン名を設定するには、グローバル コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

domain-name *name*

no domain-name [*name*]

構文の説明

name	ドメイン名を最大 63 文字で設定します。

デフォルト

デフォルト ドメイン名は default.domain.invalid 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	• 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。

使用上のガイドライン

ASA は、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。マルチ コンテキスト モードでは、システム実行スペース内だけではなく、各コンテキストに対してドメイン名を設定できます。

例

次に、ドメインを example.com に設定する例を示します。

```
ciscoasa(config)# domain-name example.com
```

関連コマンド

コマンド	説明
dns domain-lookup	ASA によるネーム ルックアップの実行をイネーブルにします。
dns name-server	ASA の DNS サーバを指定します。

コマンド	説明
hostname	ASA のホスト名を設定します。
show running-config domain-name	ドメイン名のコンフィギュレーションを表示します。

domain-name（IPv6 DHCP プール）

DHCPv6 サーバを設定するときにステートレス アドレス自動設定（SLAAC）クライアントにドメイン名を提供するには、IPv6 DHCP プール コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

domain-name *domain_name*

no domain-name *domain_name*

構文の説明

domain_name	ドメイン名を指定します。

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
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(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

クライアントがプレフィックス委任機能とともに SLAAC を使用する場合、クライアントが情報要求（IR）パケットを ASA に送信するときに **IPv6 DHCP プール**内の情報（ドメイン名など）を提供するように ASA を設定できます。ASA は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。DHCPv6 ステートレス サーバを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバを有効にする場合は、**ipv6 dhcp プール**名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
    domain-name eng.example.com
    dns-server 2001:DB8:1::1
```

```
ipv6 dhcp pool IT-Pool
    domain-name it.example.com
    dns-server 2001:DB8:1::1
interface gigabitethernet 0/0
    ipv6 address dhcp setroute default
    ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
    ipv6 address Outside-Prefix ::1:0:0:0:1/64
    ipv6 dhcp server Eng-Pool
    ipv6 nd other-config-flag
interface gigabitethernet 0/2
    ipv6 address Outside-Prefix ::2:0:0:0:1/64
    ipv6 dhcp server IT-Pool
    ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。

コマンド	説明
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

domain-password

IS-IS ルーティング ドメイン認証パスワードを設定するには、ルータ ISIS コンフィギュレーション モードで **domain-password** コマンドを使用します。パスワード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。

domain-name *password* [**authenticate snp** {**validate** | **send-only**}]

no domain-name *password*

構文の説明

password	割り当てるパスワード。
authenticate snp	(任意) これを指定すると、システムは SNP PDU にパスワードを挿入するようになります。
validate	(任意) これを指定すると、システムはパスワードを SNP に挿入し、受け取ったパスワードを SNP で確認するようになります。
send-only	(任意) これを指定すると、システムは SNP へのパスワードの挿入だけは行うようになりますが、SNP での受け取ったパスワードの確認は行われません。このキーワードは、ソフトウェアのアップグレード中、移行をスムーズに行うために使用します。

デフォルト

ドメイン パスワードは指定されていません。また、レベル 2 ルーティング情報のやり取りを行うための認証はイネーブルにされていません。

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
ルータ isis 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
9.6(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

このパスワードはプレーン テキストとしてやり取りされるため、この機能が提供するセキュリティは限定されています。

このパスワードは、レベル 2（エリア ルータ レベル）の PDU リンクステート パケット（LSP）、Complete Sequence Number PDU（CSNP）、および Partial Sequence Number PDU（PSNP）に挿入されます。

authenticate snp キーワードを指定して、**validate** または **send-only** キーワードを指定しなかった場合、IS-IS ルーティング プロトコルは SNP にパスワードを挿入しません。

例

次に、ルーティング ドメインに認証パスワードを割り当て、このパスワードを SNP に挿入し、システムが受け取った SNP で確認するように指定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。

コマンド	説明
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

downgrade

ソフトウェア バージョンをダウングレードするには、グローバル コンフィギュレーション モードで **downgrade** コマンドを使用します。

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

構文の説明

activation-key *old_key*	（オプション）アクティベーション キーを復元する必要がある場合、古いアクティベーション キーを入力できます。
old_config_url	保存されている移行前のコンフィギュレーションへのパスを指定します（デフォルトでは、disk0 に保存されます）。
old_image_url	disk0、disk1、tftp、または smb で古いイメージへのパスを指定します。
/noconfirm	（任意）プロンプトを出さずにダウングレードします。

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	• 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、次の機能を完了するためのショートカットです。

1. ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
2. 古いイメージへのブート イメージの設定（**boot system**）。
3. （任意）新たなアクティベーション キーの入力（**activation-key**）。
4. 実行コンフィギュレーションのスタートアップ コンフィギュレーションへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
5. 古いコンフィギュレーションのスタートアップ コンフィギュレーションへのコピー（**copy** *old_config_url* **startup-config**）。
6. リロード（**reload**）。

例

次に、確認なしでダウングレードする例を示します。

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

関連コマンド

コマンド	説明
activation-key	アクティベーション キーを入力します。
boot system	ブートするイメージを設定します。
clear configure boot	ブート イメージ コンフィギュレーションをクリアします。
copy startup-config	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。

download-max-size

(注) **download-max-size** コマンドは機能しません。使用しないでください。ただし、実行コンフィギュレーションでは表示される場合があり、CLI で使用できます。

ダウンロードするオブジェクトの最大許容サイズを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **download-max-size** コマンドを使用します。このオブジェクト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** バージョンを使用します。

download-max-size *size*

no download-max-size

構文の説明

size	ダウンロードするオブジェクトの最大許容サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。

デフォルト

デフォルトのサイズは 2147483647 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
グループ ポリシー webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

関連コマンド

コマンド	説明
post-max-size	ポストするオブジェクトの最大サイズを指定します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

drop

match コマンドまたは **class** コマンドに一致するすべてのパケットをドロップするには、一致またはクラス コンフィギュレーション モードで、**drop** コマンドを使用します。このア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。

drop [**send-protocol-error**] [**log**]

no drop [**send-protocol-error**] [**log**]

構文の説明

ログ	一致をログに記録します。syslog メッセージの番号は、アプリケーションによって異なります。
send-protocol-error	プロトコル エラー メッセージを送信します。

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
一致コンフィギュレーションおよびクラス コンフィギュレーション	• 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)	このコマンドが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **drop** コマンドを使用して、**match** コマンドまたはクラス マップと一致するパケットをドロップします。この drop アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションでこのアクションが許可されているわけではありません。

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを識別（**class** コマンドは **match** コマンドを含む既存の **class-map type inspect** コマンドを指す）した後は、**drop** コマンドを入力して **match** コマンドまたは **class** コマンドと一致するすべてのパケットをドロップできます。

パケットをドロップすると、インスペクション ポリシー マップで以降のアクションは実行されません。たとえば、最初のアクションでパケットをドロップした場合は、それ以降、**match** コマンドまたは **class** コマンドと一致しません。最初のアクションがパケットのロギングである場合は、パケットのドロップなどの別のアクションが発生する可能性があります。同じ **match** コマンドまたは **class** コマンドに対して **drop** アクションと **log** アクションの両方を設定できます。その場合、パケットは所定の一致箇所でドロップされる前にロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットをドロップし、HTTP トラフィック クラス マップと一致した場合にログを送信する例を示します。同じパケットが 2 番めの **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

drop-connection

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **drop-connection** コマンドを使用してパケットをドロップし、**match** コマンドまたはクラス マップと一致するトラフィックの接続を閉じます。このア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。

drop-connection [**send-protocol-error**] [**log**]

no drop-connection [**send-protocol-error**] [**log**]

構文の説明

send-protocol-error	プロトコル エラー メッセージを送信します。
ログ	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

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
一致コンフィギュレーションおよびクラス コンフィギュレーション	• **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)	このコマンドが追加されました。

使用上のガイドライン

接続は、ASA 上の接続データベースから削除されます。接続がドロップされた ASA に入る後続パケットはすべて廃棄されます。この drop-connection アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションでこのアクションが許可されているわけではありません。インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを識別（**class** コマンドは **match** コマンドを含む既存の **class-map type inspect** コマンドを指す）した後は、**drop-connection** コマンドを入力してパケットをドロップし、**match** コマンドまたは **class** コマンドと一致するトラフィックの接続を閉じます。

パケットをドロップするか、または接続を閉じると、インスペクション ポリシー マップで以降のアクションは実行されません。たとえば、最初のアクションがパケットをドロップし接続を閉じることである場合、それ以降は **match** コマンドまたは **class** コマンドに対応しません。最初のアクションがパケットのロギングである場合は、パケットのドロップなどの別のアクションが発生する可能性があります。同じ **match** コマンドまたは **class** コマンドに対して **drop-connection** アクションと **log** アクションの両方を設定できます。その場合、パケットは所定の一致箇所でドロップされる前にロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにすると、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットをドロップし、接続を閉じて、http-traffic クラス マップと一致した場合にログを送信する例を示します。同じパケットが 2 番めの **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

dtls port

DTLS 接続用のポートを指定するには、webvpn コンフィギュレーション モードで **dtls port** 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。

dtls port *number*

no dtls port *number*

構文の説明

number	UDP ポート番号（1 ～ 65535）。

デフォルト

デフォルトのポート番号は 443 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 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
8.0(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

このコマンドは、DTLS を使用する SSL VPN 接続用の UDP ポートを指定します。

DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

例

次に、webvpn コンフィギュレーション モードを開始し、DTLS 用にポート 444 を指定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# dtls port 444
```

関連コマンド

コマンド	説明
dtls enable	インターフェイスに対して DTLS をイネーブルにします。
svc dtls	SSL VPN 接続を確立するグループまたはユーザに対して、DTLS をイネーブルにします。
vpn-tunnel-protocol	ASA がリモート アクセス用に許可する VPN プロトコル（SSL を含む）を指定します。

duplex

銅線イーサネット インターフェイス（RJ-45）のデュプレックス方式を設定するには、インターフェイス コンフィギュレーション モードで **duplex** コマンドを使用します。デュプレックス設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

duplex {**auto** | **full** | **half**}

no duplex

構文の説明

[auto]	デュプレックス モードを自動検出します。
full	デュプレックス モードを全二重に設定します。
half	デュプレックス モードを半二重に設定します。

デフォルト

デフォルトは auto 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
インターフェイス コンフィギュレーション	• 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)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モード コマンドに移されました。

使用上のガイドライン

デュプレックス モードは、物理インターフェイス上にだけ設定します。

duplex コマンドは、ファイバ メディアでは使用できません。

ネットワークで自動検出がサポートされていない場合は、デュプレックス モードを特定の値に設定します。

ASA 5500 シリーズの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

PoE ポート上でデュプレックス方式を **auto** 以外に設定した場合は、IEEE 802.3af をサポートしない Cisco IP Phone およびシスコ ワイヤレス アクセス ポイントは検出されず、電源が供給されません。

例

次に、デュプレックス モードを全二重に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。
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 running-config interface	インターフェイス コンフィギュレーションを表示します。
speed	インターフェイスの速度を設定します。

dynamic-access-policy-config

DAP レコードとそれに関連付けられたアクセス ポリシー属性を設定するには、グローバル コンフィギュレーション モードで **dynamic-access-policy-config** コマンドを使用します。既存の DAP コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

dynamic-access-policy-config *name* | *activate*

no dynamic-access-policy-config

構文の説明

activate	DAP 選択コンフィギュレーション ファイルをアクティブ化します。
name	DAP レコードの名前を指定します。名前は 64 文字以内で指定できます。スペースを含めることはできません。

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
グローバル コンフィギュレーション(name)	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC(activate)	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(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。

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 モードで **dynamic-access-policy-config** コマンドを使用して、1 つまたは複数の DAP レコードを作成します。DAP 選択コンフィギュレーション ファイルをアクティブにするには、*activate* 引数を指定して **dynamic-access-policy-config** コマンドを使用します。

このコマンドを使用するには、ダイナミック アクセス ポリシー レコード モードを開始します。このモードでは、指定した DAP レコードの属性を設定できます。ダイナミック アクセス ポリシー レコード モードで使用できるコマンドは、次のとおりです。

- **アクション**
- **説明**
- **network-acl**

- **priority**
- **user-message**
- **webvpn**

例

次に、user1 という名前の DAP レコードを設定する例を示します。

```
ciscoasa(config)# dynamic-access-policy-config user1
ciscoasa(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードにアクセス ポリシー属性を入力します。
show running-config dynamic-access-policy-record	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

dynamic-access-policy-record

DAP レコードを作成してアクセス ポリシー属性を入力するには、グローバル コンフィギュレーション モードで **dynamic-access-policy-record** コマンドを使用します。既存の DAP レコードを削除するには、このコマンドの **no** 形式を使用します。

dynamic-access-policy-record *name*

no dynamic-access-policy-record *name*

構文の説明

name	DAP レコードの名前を指定します。名前は 64 文字以内で指定できます。スペースを含めることはできません。

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
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
8.0(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

グローバル コンフィギュレーション モードで **dynamic-access-policy-record** コマンドを使用して、1 つまたは複数の DAP レコードを作成します。このコマンドを使用するには、ダイナミック アクセス ポリシー レコード モードを開始します。このモードでは、指定した DAP レコードの属性を設定できます。ダイナミック アクセス ポリシー レコード モードで使用できるコマンドは、次のとおりです。

- **action**（**continue**、**terminate**、または **quarantine**）
- **説明**
- **network-acl**
- **priority**
- **user-message**
- **webvpn**

例

次に、Finance という名前の DAP レコードを作成する例を示します。

```
ciscoasa(config)# dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
clear config dynamic-access-policy-record	すべての DAP レコードまたは指定された DAP レコードを削除します。
dynamic-access-policy-config url	DAP 選択コンフィギュレーション ファイルを設定します。
show running-config dynamic-access-policy-record	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

dynamic-authorization

AAA サーバ グループの RADIUS の動的認可（認可変更）サービスをイネーブルにするには、AAA サーバ グループ コンフィギュレーション モードで **dynamic-authorization** コマンドを使用します。動的認可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。

dynamic-authorization [**port** *number*]

no dynamic-authorization [**port** *number*]

構文の説明

port *number*	（オプション）ASA で動的認可ポートを指定します。指定できる範囲は、1024 ～ 65535 です。

デフォルト

デフォルトのリスニング ポートは 1700 です。デフォルトでは、dynamic-authorization はイネーブルになりません。

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
aaa サーバ グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
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

このコマンドは、ISE 認可変更（CoA）のために RADIUS サーバ グループを設定するために使用します。定義されると、対応する RADIUS サーバ グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。

ISE Change of Authorization（CoA）機能は、認証、認可、およびアカウンティング（AAA）セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザまたはユーザ グループのポリシーを変更すると、ISE から ASA へ CoA パケットを直接送信して認証を再初期化し、新しいポリシーを適用できます。インライン ポスチャ実施ポイント（IPEP）で、ASA と確立された各 VPN セッションのアクセス コントロール リスト（ACL）を適用する必要がなくなりました。

エンド ユーザが VPN 接続を要求すると、ASA はユーザに対して ISE 認証を実行し、ネットワークへの制限付きアクセスを提供する ACL を受領します。アカウンティング開始メッセージが ISE に送信され、セッションが登録されます。ポスチャ アセスメントが NAC エージェントと ISE 間で直接行われます。このプロセスは、ASA に透過的です。ISE が CoA の「ポリシー プッシュ」を介して ASA にポリシーの更新を送信します。これにより、ネットワーク アクセス権限を高める新しいユーザ ACL が識別されます。後続の CoA 更新を介し、接続のライフタイム中に追加のポリシー評価が ASA に透過的に行われる場合があります。

例

次の例は、ISE サーバ グループに、動的認可（CoA）のアップデートと時間ごとの定期的なアカウンティングを設定する方法を示しています。ISE によるパスワード認証を設定するトンネル グループ設定が含まれています。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

次に、ISE でローカル証明書の検証と認可用のトンネル グループを設定する例を示します。この場合、サーバ グループは認証用に使用されないため、**authorize-only** コマンドをサーバ グループ コンフィギュレーションに組み込みます。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

関連コマンド

コマンド	説明
authorize-only	RADIUS サーバ グループ用の認可専用モードをイネーブルにします。
interim-accounting-update	RADIUS 中間アカウンティング アップデート メッセージの生成をイネーブルにします。
without-csd	特定のトンネル グループに行われる接続のホストスキャン処理をオフに切り替えます。

dynamic-filter ambiguous-is-black

ボットネット トラフィック フィルタのグレイリストに記載されているトラフィックを、ドロップするためにブラックリストに記載されているトラフィックとして扱うには、グローバル コンフィギュレーション モードで **dynamic-filter ambiguous-is-black** コマンドを使用します。グレイリストに記載されているトラフィックを許可するには、このコマンドの **no** 形式を使用します。

dynamic-filter ambiguous-is-black

no dynamic-filter ambiguous-is-black

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

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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(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

dynamic-filter enable コマンドを設定してから **dynamic-filter drop blacklist** コマンドを設定すると、このコマンドでは、グレイリストに記載されているトラフィックが、ドロップするためにブラックリストに記載されているトラフィックとして扱われます。このコマンドをイネーブルにしない場合、グレーリストに記載されているトラフィックはドロップされません。

複数のドメイン名にあいまいなアドレスが関連付けられていますが、これらのドメイン名がすべてブラックリストに記載されてるわけではありません。これらのアドレスはグレーリストに記載されます。

例

次に、外部インターフェイスでポート 80 のすべてのトラフィックをモニタし、ブラックリストおよびグレイリストに記載されているトラフィックを脅威レベル moderate 以上でドロップする例を示します。

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
ciscoasa(config)# dynamic-filter ambiguous-is-black
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。

コマンド	説明
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter blacklist

ボットネット トラフィック フィルタのブラックリストを編集するには、グローバル コンフィギュレーション モードで **dynamic-filter blacklist** コマンドを使用します。ブラックリストを削除するには、このコマンドの **no** 形式を使用します。

dynamic-filter blacklist

no dynamic-filter blacklist

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
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

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。

使用上のガイドライン

ダイナミック フィルタ ブラックリスト コンフィギュレーション モードを開始した後に、**address** コマンドおよび **name** コマンドを使用して、ブラックリストで信用できない名前としてタグ付けするドメイン名または IP アドレス（ホストまたはサブネット）を手動で入力できます。また、syslog メッセージおよびレポートで、ダイナミック ブラックリストおよびホワイトリストの両方に記載されている名前または IP アドレスがホワイトリスト アドレスとしてのみ識別されるように、ホワイトリストに名前や IP アドレスを入力できます（**dynamic-filter whitelist** コマンドを参照）。アドレスがダイナミック ブラックリストに記載されていない場合でも、ホワイトリストに記載されたアドレスの syslog メッセージは表示されます。

スタティック ブラックリスト エントリは、常に Very High 脅威レベルに指定されます。

スタティック データベースにドメイン名を追加した場合、ASA は、1 分間待機してからそのドメイン名の DNS 要求を送信し、ドメイン名と IP アドレスの組を *DNS ホスト キャッシュ*に追加します（このアクションはバックグラウンド プロセスで、ASA の設定の続行に影響しません）。ボットネット トラフィック フィルタ スヌーピングによる DNS パケット インスペクションもイネーブルにすることを推奨します（**inspect dns dynamic-filter-snooping** コマンドを参照してください）。次の場合、ASAは、通常の DNS lookup ではなく、ボットネット トラフィック フィルタ スヌーピングを使用してスタティック ブラックリストのドメイン名を解決します。

- ASA DNS サーバが使用できない。
- ASA が通常の DNS 要求を送信する前の 1 分間の待機期間中に接続が開始された。

DNS スヌーピングを使用すると、感染ホストがスタティック データベースに記載されている名前に対する DNS 要求を送信したときに、ASA がドメイン名と関連付けられている IP アドレスを DNS パケット内から検出し、その名前と IP アドレスを DNS 逆ルックアップ キャッシュに追加します。

スタティック データベースを使用すると、ブラックリストに記載するドメイン名または IP アドレスを使用してダイナミック データベースを増強できます。

ボットネット トラフィック フィルタ スヌーピングをイネーブルにせず、上記の状況のいずれかが発生した場合、このトラフィックは、ボットネット トラフィック フィルタでモニタされません。

(注) このコマンドは、ASA が DNS サーバを使用することが必須です。**dns domain-lookup** コマンドおよび **dns server-group** コマンドを参照してください。

例

次に、ブラックリストおよびホワイトリストのエントリを作成する例を示します。

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0

ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。

コマンド	説明
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter database fetch

ボットネット トラフィック フィルタのダイナミック データベースのダウンロードをテストするには、特権 EXEC モードで **dynamic-filter database fetch** コマンドを使用します。

dynamic-filter database fetch

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	• 対応	• 対応	• 対応	• 対応	• 対応

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。

使用上のガイドライン

実際のデータベースは ASA で保存されません。ダウンロードされてから廃棄されます。このコマンドは、テスト用にのみ使用してください。

例

次に、ダイナミック データベースのダウンロードをテストする例を示します。

```
ciscoasa# dynamic-filter database fetch
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。

コマンド	説明
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。

コマンド	説明
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter database find

ボットネット トラフィック フィルタのダイナミック データベースにドメイン名または IP アドレスが含まれているかどうかを確認するには、特権 EXEC モードで **dynamic-filter database find** コマンドを使用します。

dynamic-filter database find *string*

構文の説明

string	*string* には、ドメイン名または IP アドレスのすべてまたは一部を、3 文字以上の検索文字列で指定できます。データベース検索では、正規表現はサポートされません。

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	• 対応	• 対応	• 対応	• 対応	• 対応

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。

使用上のガイドライン

一致する項目が複数見つかった場合は、最初の 2 つの項目が表示されます。一致する項目を絞り込むために詳細な検索条件を指定するには、より長い文字列を入力します。

例

次に、文字列「example.com」で検索する例を示します。この例では、一致する項目が 1 つ見つかります。

```
ciscoasa# dynamic-filter database find bad.example.com

   bad.example.com
Found 1 matches
```

次に、文字列「bad」で検索する例を示します。この例では、一致する項目が 3 つ以上見つかります。

```
ciscoasa# dynamic-filter database find bad

   bad.example.com
   bad.example.net
Found more than 2 matches, enter a more specific string to find an exact
match
```

関連コマンド

コマンド	説明
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。

コマンド	説明
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter database purge

実行メモリからボットネット トラフィック フィルタのダイナミック データベースを手動で削除するには、特権 EXEC モードで **dynamic-filter database purge** コマンドを使用します。

dynamic-filter database purge

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	• 対応	• 対応	• 対応	• 対応	• 対応

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。

使用上のガイドライン

データベース ファイルは実行メモリに保存されます。フラッシュ メモリには保存されません。データベースを削除する必要がある場合、**dynamic-filter database purge** コマンドを使用します。

データベース ファイルを消去するには、**no dynamic-filter use-database** コマンドを使用して、データベースの使用をディセーブルにしておく必要があります。

例

次に、データベースの使用をディセーブルにしてからデータベースを消去する例を示します。

```
ciscoasa(config)# no dynamic-filter use-database
ciscoasa(config)# dynamic-filter database purge
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。

コマンド	説明
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。

コマンド	説明
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter drop blacklist

ボットネット トラフィック フィルタを使用して、ブラックリストに記載されたトラフィックを自動的にドロップするには、グローバル コンフィギュレーション モードで **dynamic-filter drop blacklist** コマンドを使用します。自動ドロップ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。

dynamic-filter drop blacklist [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** {**eq** *level* | **range** *min max*}]

no dynamic-filter drop blacklist [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** {**eq** *level* | **range** *min max*}]

構文の説明

action-classify-list *sub_access_list*	(任意) ドロップするトラフィックのサブセットを指定します。アクセス リストの作成については、**access-list extended** コマンドを参照してください。 ドロップされるトラフィックは、常に **dynamic-filter enable** コマンドで指定したモニタ トラフィックと同じか、またはモニタ トラフィックのサブセットである必要があります。たとえば、**dynamic-filter enable** コマンドに対してアクセス リストを指定し、このコマンドに対して **action-classify-list** を指定する場合、**dynamic-filter enable** アクセス リストのサブセットになります。
interface *name*	(任意) 特定のインターフェイスへのモニタリングを制限します。ドロップされるトラフィックは、常に **dynamic-filter enable** コマンドで指定したモニタ トラフィックと同じか、またはモニタ トラフィックのサブセットである必要があります。 インターフェイス固有のコマンドは、グローバル コマンドより優先されます。
threat-level {***eq*** *level* | ***range*** *min max*}	(任意) 脅威レベルの設定によってドロップされるトラフィックを制限します。明示的に脅威レベルを設定しない場合、使用されるレベルは、**threat-level range moderate very-high** です。 **(注)** デフォルト設定を変更する確固たる理由がない限り、デフォルト設定を使用することを強くお勧めします。 *level*、*min*、および *max* の各オプションは次のとおりです。 • **very-low** • **low** • **moderate** • **high** • **very-high** **(注)** スタティック ブラックリスト エントリは、常に Very High 脅威レベルに指定されます。

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。

デフォルトの脅威レベルは **threat-level range moderate very-high** 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。

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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(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

最初に、ドロップするトラフィックに対して **dynamic-filter enable** コマンドを設定するようにしてください。ドロップされるトラフィックは、常に、モニタされるトラフィックと同じであるか、またはこのトラフィックのサブセットである必要があります。

このコマンドは、各インターフェイスおよびグローバル ポリシーに対して複数回入力できます。所定のインターフェイス/グローバル ポリシーに対する複数のコマンドで、重複トラフィックを指定しないでください。コマンド照合順を完全に制御することはできないので、重複トラフィックは、照合されたコマンドを把握できないことになります。たとえば、所定のインターフェイスに対してすべてのトラフィックに一致するコマンド（**action-classify-list** キーワードを使用しない）と **action-classify-list** キーワードを使用するコマンドの両方を指定しないでください。この場合、トラフィックと **action-classify-list** キーワードを使用するコマンドとの照合が行われないことがあります。同様に、**action-classify-list** キーワードを使用する複数のコマンドを指定する場合、アクセス リストが固有であり、ネットワークが重複していないことを確認してください。

例

次に、外部インターフェイスの 80 番ポートのトラフィックをすべてモニタし、脅威レベルが moderate 以上のトラフィックをドロップする例を示します。

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。

コマンド	説明
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter enable

ボットネット トラフィック フィルタ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 **dynamic-filter enable** コマンドを使用します。ボットネット トラフィック フィルタ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。

dynamic-filter enable [**interface** *name*] [**classify-list** *access_list*]

no dynamic-filter enable [**interface** *name*] [**classify-list** *access_list*]

構文の説明

classify-list *access_list*	拡張アクセス リストを使用してモニタするトラフィックを指定します（**access-list extended** コマンドを参照）。アクセス リストを作成しない場合、デフォルトでは、すべてのトラフィックをモニタします。
interface *name*	特定のインターフェイスへのモニタリングを制限します。

デフォルト

デフォルトでは、ボットネット トラフィック フィルタ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	• 対応	• 対応	• 対応	• 対応	—

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。

使用上のガイドライン

ボットネット トラフィック フィルタは、各初期接続パケットの送信元 IP アドレスおよび宛先 IP アドレスを、ダイナミック データベース、スタティック データベース、DNS 逆ルックアップ キャッシュ、および DNS ホスト キャッシュの IP アドレスと比較し、syslog メッセージを送信するか、または一致するトラフィックをドロップします。

マルウェアとは、知らないうちにホストにインストールされている悪意のあるソフトウェアです。個人情報（パスワード、クレジット カード番号、キー ストローク、または独自データ）の送信などのネットワーク アクティビティを試みるマルウェアは、マルウェアが既知の不正な IP アドレスへの接続を開始したときにボットネット トラフィック フィルタによって検出できます。Botnet Traffic Filter は、悪意のある既知のドメイン名および IP アドレスを含む動的データベースと、着信接続および発信接続とを照合して、疑わしいアクティビティをすべてログに記録します。また、ローカルの「ブラックリスト」または「ホワイトリスト」に IP アドレスやドメイン名を入力して、スタティック データベースでダイナミック データベースを補完できます。

DNS スヌーピングは個別にイネーブルになります(**inspect dns dynamic-filter-snoop** コマンドを参照)。一般的に、Botnet Traffic Filter を最大限に利用するには、DNS スヌーピングをイネーブルにする必要がありますが、必要に応じて、Botnet Traffic Filter のロギングだけを単独で使用できます。ダイナミック データベースに DNS スヌーピングが設定されていない場合、ボットネット トラフィック フィルタでは、スタティック データベースのエントリとダイナミック データベースの IP アドレスだけが使用されます。ダイナミック データベースのドメイン名は使用されません。

ボットネット トラフィック フィルタのアドレス カテゴリ

ボットネット トラフィック フィルタのモニタ対象のアドレスは次のとおりです。

- 既知のマルウェア アドレス:これらのアドレスは、「ブラックリスト」に記載されます。
- 既知の許可アドレス:これらのアドレスは、「ホワイトリスト」に記載されます。
- あいまいなアドレス:ブラックリストに記載されていないドメイン名を 1 つ以上含む複数のドメイン名に関連付けられているアドレス。これらのアドレスは「グレーリスト」に記載されます。
- リストに記載されていないアドレス:どのリストにも記載されていない不明アドレス。

既知のアドレスに対するボットネット トラフィック フィルタのアクション

dynamic-filter enable コマンドを使用して、不審なアクティビティをロギングするようボットネット トラフィック フィルタを設定できます。また、任意で、**dynamic-filter drop blacklist** コマンドを使用して、不審なトラフィックを自動的にブロックするようボットネット トラフィック フィルタを設定できます。

リストに記載されていないアドレスについては、syslog メッセージは生成されません。ただし、ブラックリスト、ホワイトリスト、およびグレイリストに記載されているアドレスについては、タイプ別の syslog メッセージが生成されます。ボットネット トラフィック フィルタでは、338*nnn* という番号が付いた詳細な syslog メッセージが生成されます。メッセージでは、着信接続と発信接続、ブラックリスト アドレス、ホワイトリスト アドレス、またはグレイリスト アドレス、およびその他の多数の変数が区別されます(グレイリストには、ブラックリストに記載されていないドメイン名を 1 つ以上含む複数のドメイン名に関連付けられているアドレスが含まれています)。

syslog メッセージの詳細については、syslog メッセージ ガイドを参照してください。

デバイス サポート

ボットネット トラフィック フィルタを有効にできるデバイス モデルは次のとおりです。

- ASA 5505
- ASA 5510、5520、5540、5550
- ASA 5512-X、5515-X、5525-X、5545-X、5555-X
- ASA 5580
- ASA 5585-X
- ASASM

例

次に、外部インターフェイスの 80 番ポートのトラフィックをすべてモニタし、脅威レベルが moderate 以上のトラフィックをドロップする例を示します。

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。

コマンド	説明
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter updater-client enable

ボットネット トラフィック フィルタについて、シスコの更新サーバからのダイナミック データベースのダウンロード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 **dynamic-filter updater-client enable** コマンドを使用します。ダイナミック データベースのダウンロード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。

dynamic-filter updater-client enable

no dynamic-filter updater-client enable

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、ダウンロード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	• 対応	• 対応	• 対応	—	• 対応

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。

使用上のガイドライン

ASA にデータベースをまだインストールしていない場合は、約 2 分後にデータベースが適応型セキュリティ アプライアンスにダウンロードされます。アップデート サーバは、将来のアップデートのために ASA がサーバにポーリングする頻度を決定します（通常は 1 時間ごと）。

ボットネット トラフィック フィルタでは、Cisco アップデート サーバからダイナミック データベースの定期アップデートを受け取ることができます。

このデータベースには、数千もの既知の不正なドメイン名と IP アドレスが含まれています。DNS 応答のドメイン名とダイナミック データベースのドメイン名が一致した場合、ボットネット トラフィック フィルタは、このドメイン名と IP アドレスを *DNS 逆ルックアップ キャッシュ*に追加します。感染したホストがマルウェア サイトの IP アドレスへの接続を開始すると、ASA によって、この不審なアクティビティに関する syslog メッセージ情報が送信されます。

データベースを使用するには、ASA 用のドメイン ネーム サーバを設定して、適応型セキュリティ アプライアンスが URL にアクセスできるようにしてください。ダイナミック データベースでドメイン名を使用するには、DNS パケット インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにする必要があります。ASA は、ドメイン名とそれに関連付けられている IP アドレスを DNS パケット内から検出します。

場合によっては、IP アドレス自体がダイナミック データベースに入力され、ボットネット トラフィック フィルタは DNS 要求を検査せずに、その IP アドレスへのすべてのトラフィックをログに記録します。

データベース ファイルは実行メモリに保存されます。フラッシュ メモリには保存されません。データベースを削除する必要がある場合は、**dynamic-filter database purge** コマンドを使用します。

(注) このコマンドは、ASA が DNS サーバを使用することが必須です。**dns domain-lookup** コマンドおよび **dns server-group** コマンドを参照してください。

例

次のマルチ モードの例では、ダイナミック データベースのダウンロードと、context1 および context2 でのデータベースの使用をイネーブルにします。

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

次のシングル モードの例では、ダイナミック データベースのダウンロードおよび使用をイネーブルにします。

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns name-server	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。

コマンド	説明
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter use-database

ボットネット トラフィック フィルタのダイナミック データベースの使用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 **dynamic-filter use-database** コマンドを使用します。ダイナミック データベースの使用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。

dynamic-filter use-database

no dynamic-filter use-database

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、データベースの使用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。

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	• 対応	• 対応	• 対応	• 対応	—

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。

使用上のガイドライン

ダウンロードされたデータベースのディセーブル化は、マルチ コンテキスト モードでデータベースの使用をコンテキストごとに設定できるようにする場合に有用です。ダイナミック データベースのダウンロードのイネーブル化については、**dynamic-filter updater-client enable** コマンドを参照してください。

例

次のマルチ モードの例では、ダイナミック データベースのダウンロードと、context1 および context2 でのデータベースの使用をイネーブルにします。

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

次のシングル モードの例では、ダイナミック データベースのダウンロードおよび使用をイネーブルにします。

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。

コマンド	説明
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter whitelist

ボットネット トラフィック フィルタのホワイトリストを編集するには、グローバル コンフィギュレーション モードで **dynamic-filter whitelist** コマンドを使用します。ホワイトリストを削除するには、このコマンドの **no** 形式を使用します。

dynamic-filter whitelist

no dynamic-filter 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。

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	• 対応	• 対応	• 対応	• 対応	—

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。

使用上のガイドライン

スタティック データベースを使用すると、ホワイトリストに記載するドメイン名または IP アドレスを使用してダイナミック データベースを増強できます。ダイナミック フィルタ ホワイトリスト コンフィギュレーション モードを開始した後に、**address** コマンドおよび **name** コマンドを使用して、ホワイトリストで信用できる名前としてタグ付けするドメイン名または IP アドレス（ホストまたはサブネット）を手動で入力できます。ダイナミック ブラックリストとスタティック ホワイトリストの両方に記載された名前やアドレスは、syslog メッセージおよびレポートでは、ホワイトリスト アドレスとしてのみ示されます。アドレスがダイナミック ブラックリストに記載されていない場合でも、ホワイトリストに記載されたアドレスの syslog メッセージは表示されます。スタティック ブラックリストに名前や IP アドレスを入力するには、**dynamic-filter blacklist** コマンドを使用します。

スタティック データベースにドメイン名を追加した場合、ASA は、1 分間待機してからそのドメイン名の DNS 要求を送信し、ドメイン名と IP アドレスの組を *DNS ホスト キャッシュ*に追加します(このアクションはバックグラウンド プロセスで、ASA の設定の続行に影響しません)。ボットネット トラフィック フィルタ スヌーピングによる DNS パケット インスペクションもイネーブルにすることを推奨します(**inspect dns dynamic-filter-snooping** コマンドを参照してください)。次の場合、ASA は、通常の DNS lookup ではなく、ボットネット トラフィック フィルタ スヌーピングを使用してスタティック ブラックリストのドメイン名を解決します。

- ASA DNS サーバが使用できない。
- ASA が通常の DNS 要求を送信する前の 1 分間の待機期間中に接続が開始された。

DNS スヌーピングを使用すると、感染ホストがスタティック データベースに記載されている名前に対する DNS 要求を送信したときに、ASA がドメイン名と関連付けられている IP アドレスを DNS パケット内から検出し、その名前と IP アドレスを DNS 逆ルックアップ キャッシュに追加します。

ボットネット トラフィック フィルタ スヌーピングをイネーブルにせず、上記の状況のいずれかが発生した場合、このトラフィックは、ボットネット トラフィック フィルタでモニタされません。

(注) このコマンドは、ASA が DNS サーバを使用することが必須です。**dns domain-lookup** コマンドおよび **dns server-group** コマンドを参照してください。

例

次に、ブラックリストおよびホワイトリストのエントリを作成する例を示します。

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0

ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。

コマンド	説明
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。