

Flexconfigを使用したNetFlow設定の削除または変更

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[初期設定](#)

[NetFlow設定の削除](#)

[既存のNetFlow設定の変更](#)

[関連資料](#)

はじめに

このドキュメントでは、Firepower経由でFirepower Threat Defense(FTD)のNetFlow設定を削除または変更する方法について説明します Management Center (FMC ; 管理センター) の略。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FMCに関する知識
- FTDの知識
- FlexConfigポリシーの知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- FTDバージョン7.4未満
- FMCバージョン7.4未満

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。



注：Firepowerバージョン7.2.xの重要な注意事項：NetFlowを設定する際に、Flexオブジェクトが並べ替わり、クラスマップが設定されていないために導入が失敗するという既知のCisco Bug ID [CSCwh29167](#)があります。この問題を解決するには、Cisco Bug ID [CSCwf99848](#)(Cisco Bug ID [CSCwh29167](#)の重複)に記載されている回避策を実装します。

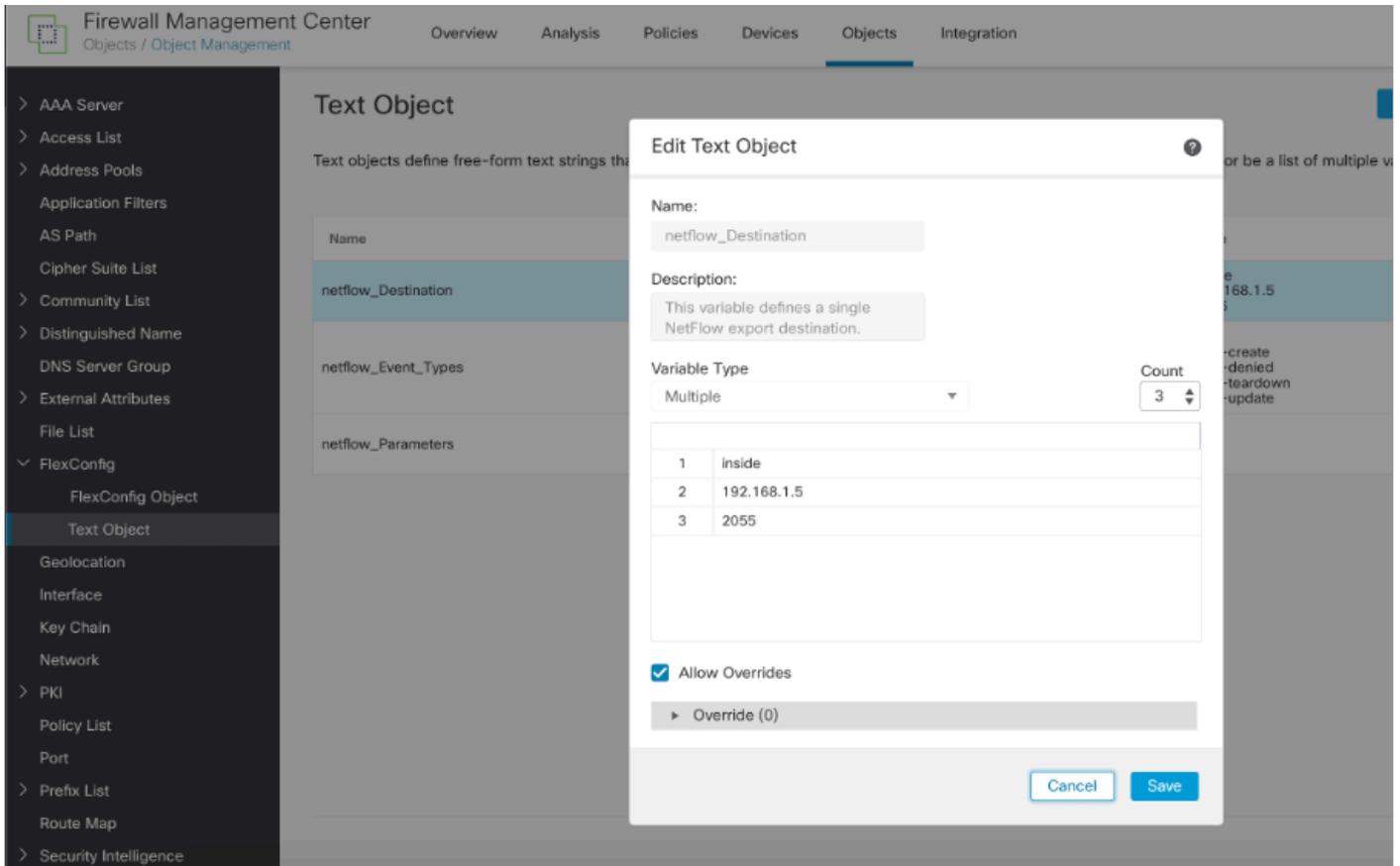
初期設定

```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
  match access-list flow_export_acl
!
policy-map global_policy
  class flow_export_class
    flow-export event-type flow-create destination 192.168.1.5
    flow-export event-type flow-denied destination 192.168.1.5
    flow-export event-type flow-teardown destination 192.168.1.5
    flow-export event-type flow-update destination 192.168.1.5
```

!
flow-export destination Inside 192.168.1.5 2055

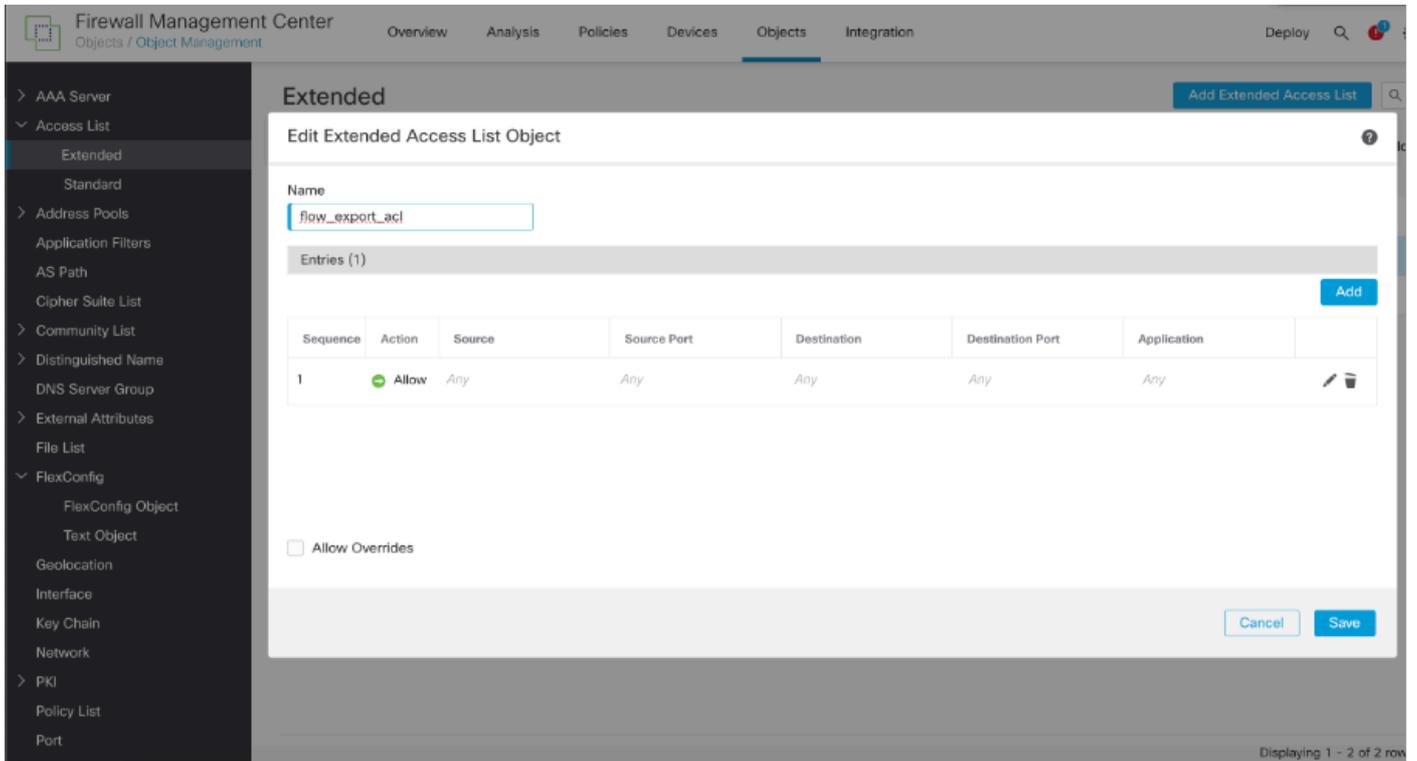
これらの初期設定を行うために使用するflex configオブジェクトは次のとおりです。

1. NetFlow送信先テキストオブジェクト



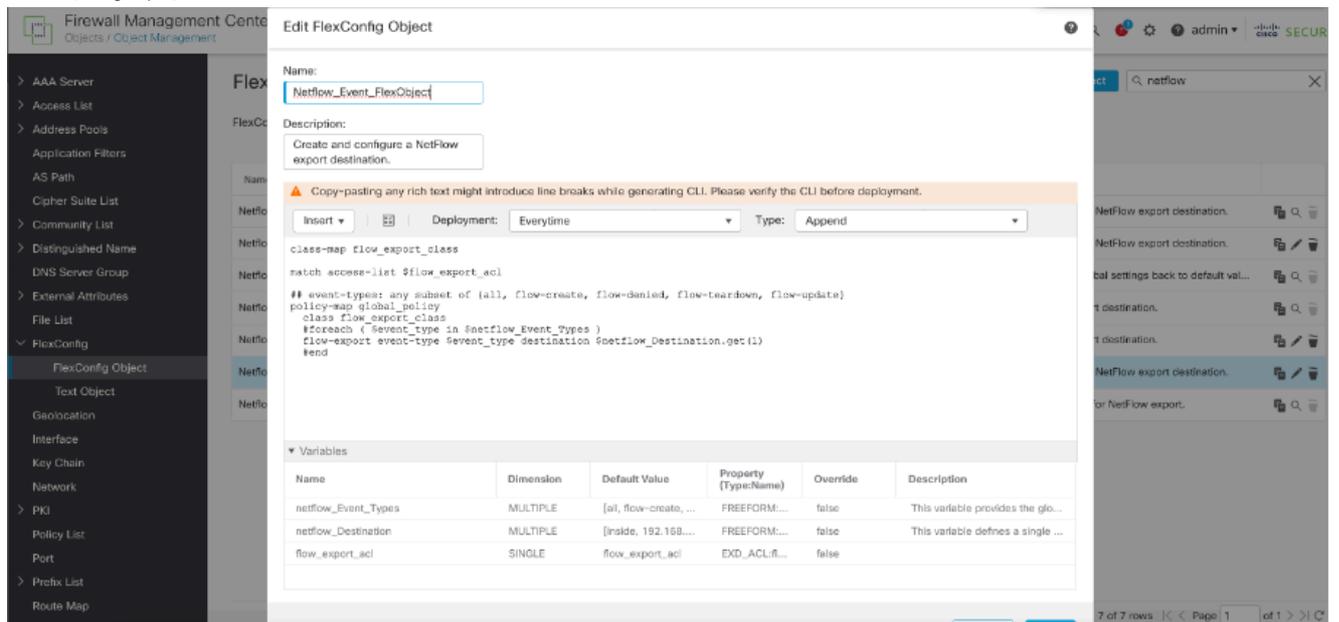
Netflow送信先テキストオブジェクト

2. flow_export_aclという拡張ACL



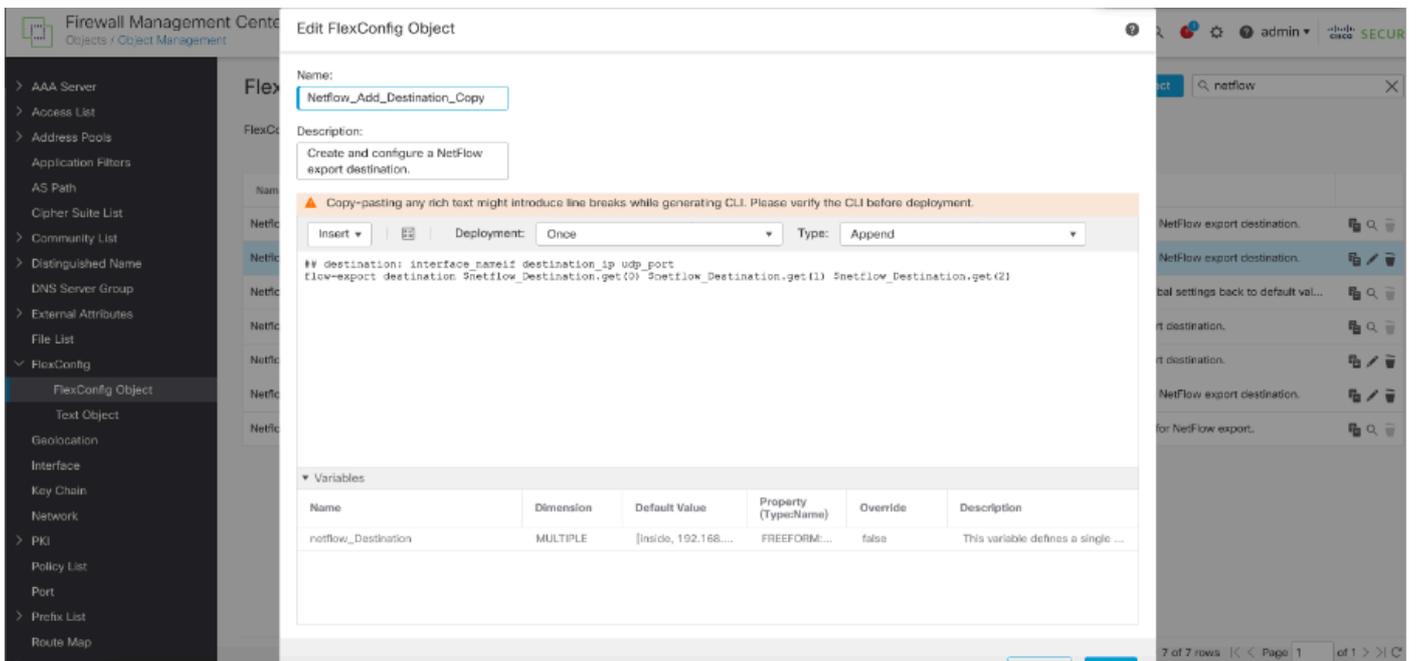
フローエクスポートACL

3. フローエクスポート宛先でこのクラスマップを適用するために使用されるクラスマップとサービスポリシー



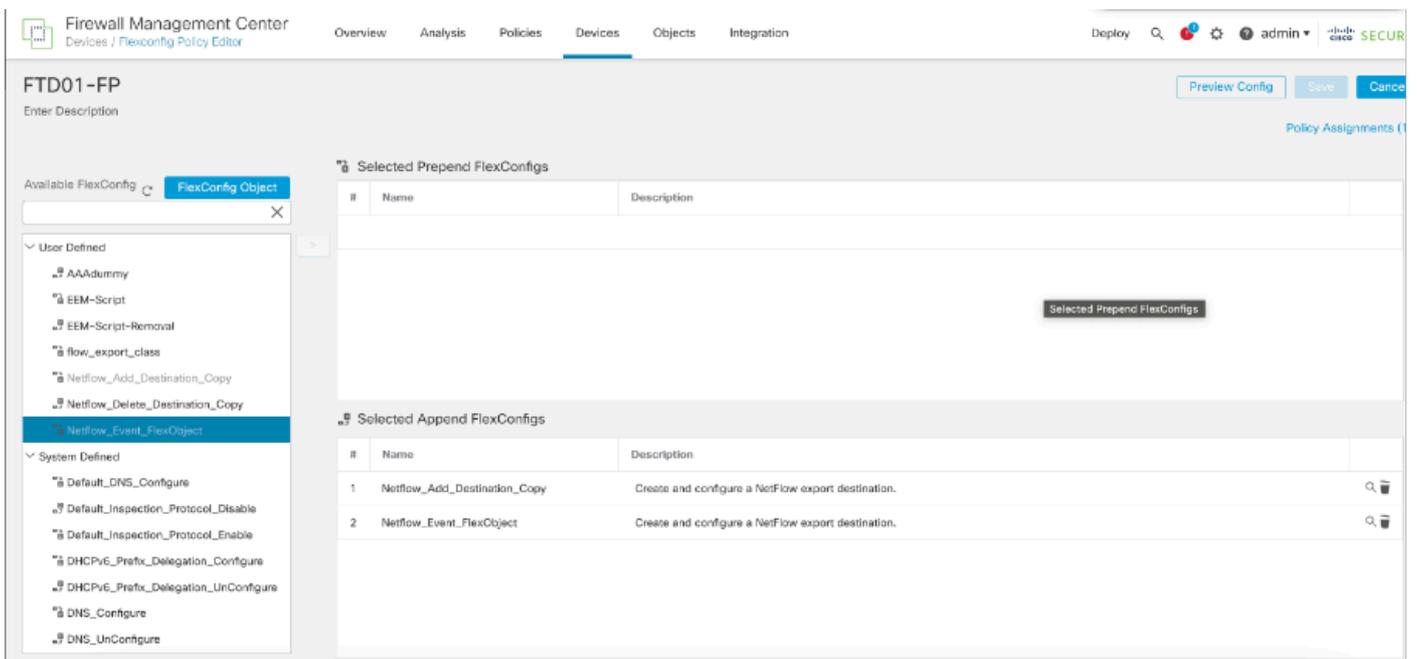
クラスマップとサービスポリシー

4. フローエクスポート先



フローエクスポート宛先

5. 次に、これら2つのオブジェクトをflex configポリシーに追加し、展開しました。



FlexConfigポリシー

NetFlow設定の削除

ステップ1：フレックスポリシーからフレックスオブジェクトを削除します。

既存のflexconfigの削除

手順2：ポリシーを展開します。コマンドラインから、削除された設定は次のように表示されます。

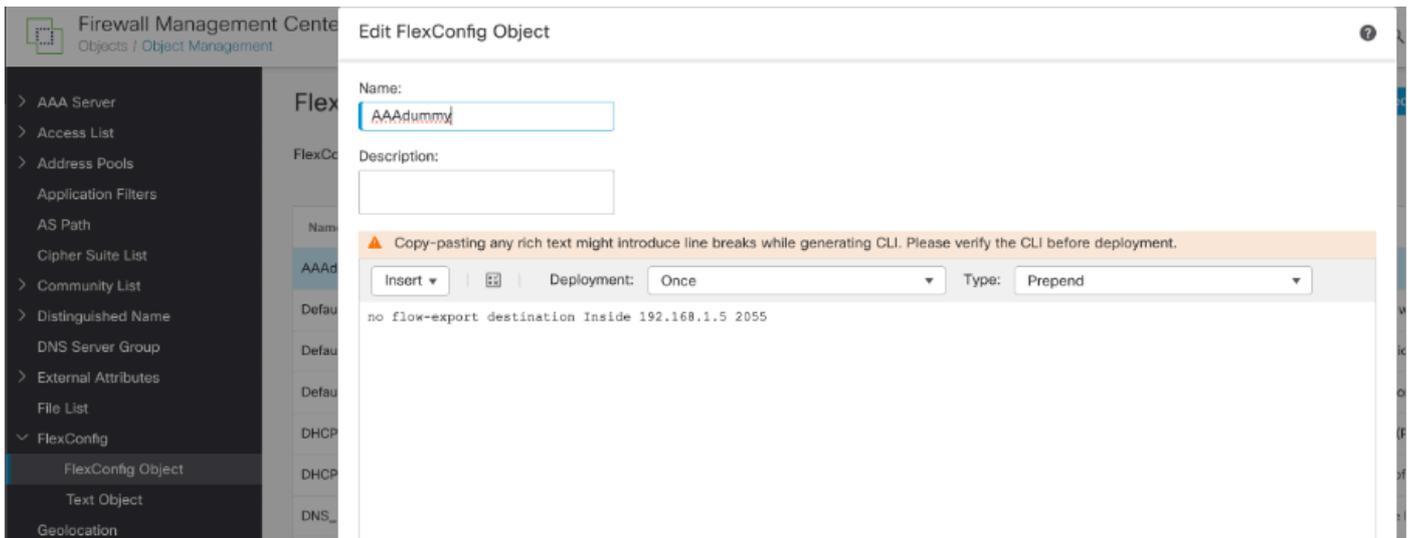
```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
 match access-list flow_export_acl
!
policy-map global_policy
 class flow_export_class
  flow-export event-type flow-create destination 192.168.1.5
  flow-export event-type flow-denied destination 192.168.1.5
  flow-export event-type flow-teardown destination 192.168.1.5
  flow-export event-type flow-update destination 192.168.1.5
```

一方、削除されない設定は次のとおりです。

```
flow-export destination Inside 192.168.1.5 2055
```

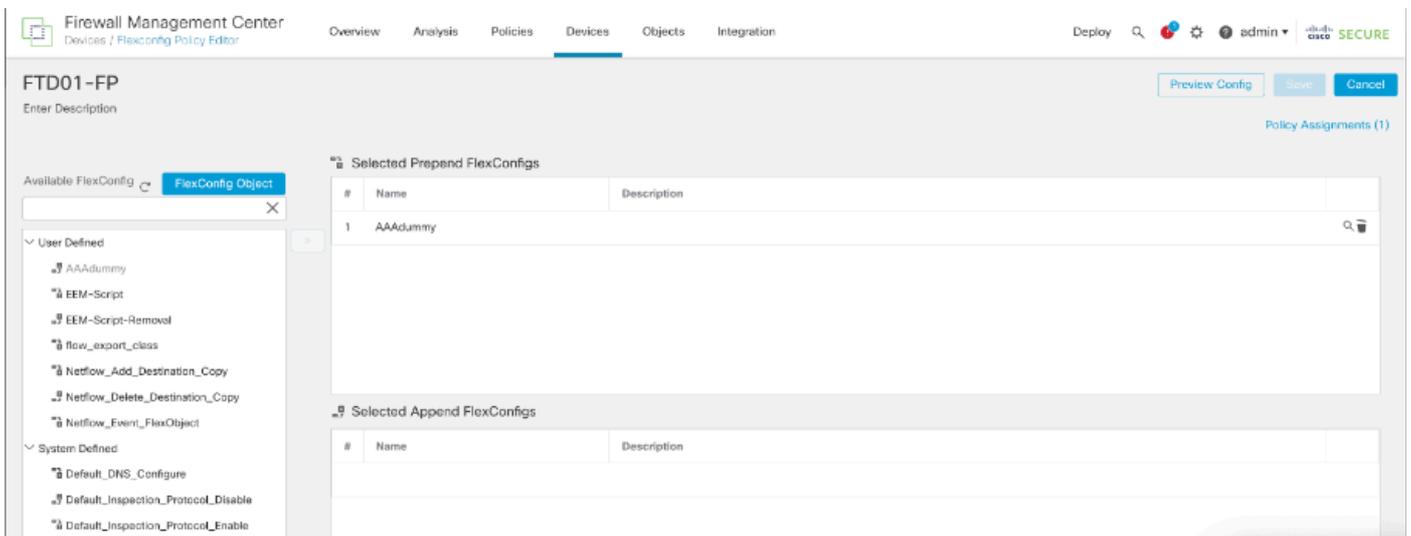
ステップ3：これを削除するには、「prepend」タイプのフレックスオブジェクトを作成し、設定を追加する必要があります。

```
no flow-export destination Inside 192.168.1.5 2055
```



フレックス構成の移行先の削除

ステップ4：フレックスポリシーで、ステップ3で新しく作成したプリペンドオブジェクトを呼び出し、ポリシーを展開します。



これをflex config policyの下に追加します。

ステップ5：フレックスポリシーから先頭に追加されたオブジェクトを削除し、再度展開します。

Firewall Management Center
Devices / FlexConfig Policy Editor

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

FTD01-FP Enter Description [Preview Config] [Save] [Cancel] Policy Assignments (1)

Available FlexConfig FlexConfig Object

User Defined

- AAAadummy
- EEM-Script
- EEM-Script-Removal
- flow_export_class
- Netflow_Add_Destination_Copy
- Netflow_Delete_Destination_Copy
- Netflow_Event_FlexObject

System Defined

- Default_DNS_Configure
- Default_Inspection_Protocol_Disable
- Default_Inspection_Protocol_Enable

Selected Prepend FlexConfigs

#	Name	Description
---	------	-------------

Selected Append FlexConfigs

#	Name	Description
---	------	-------------

Selected Append FlexConfigs

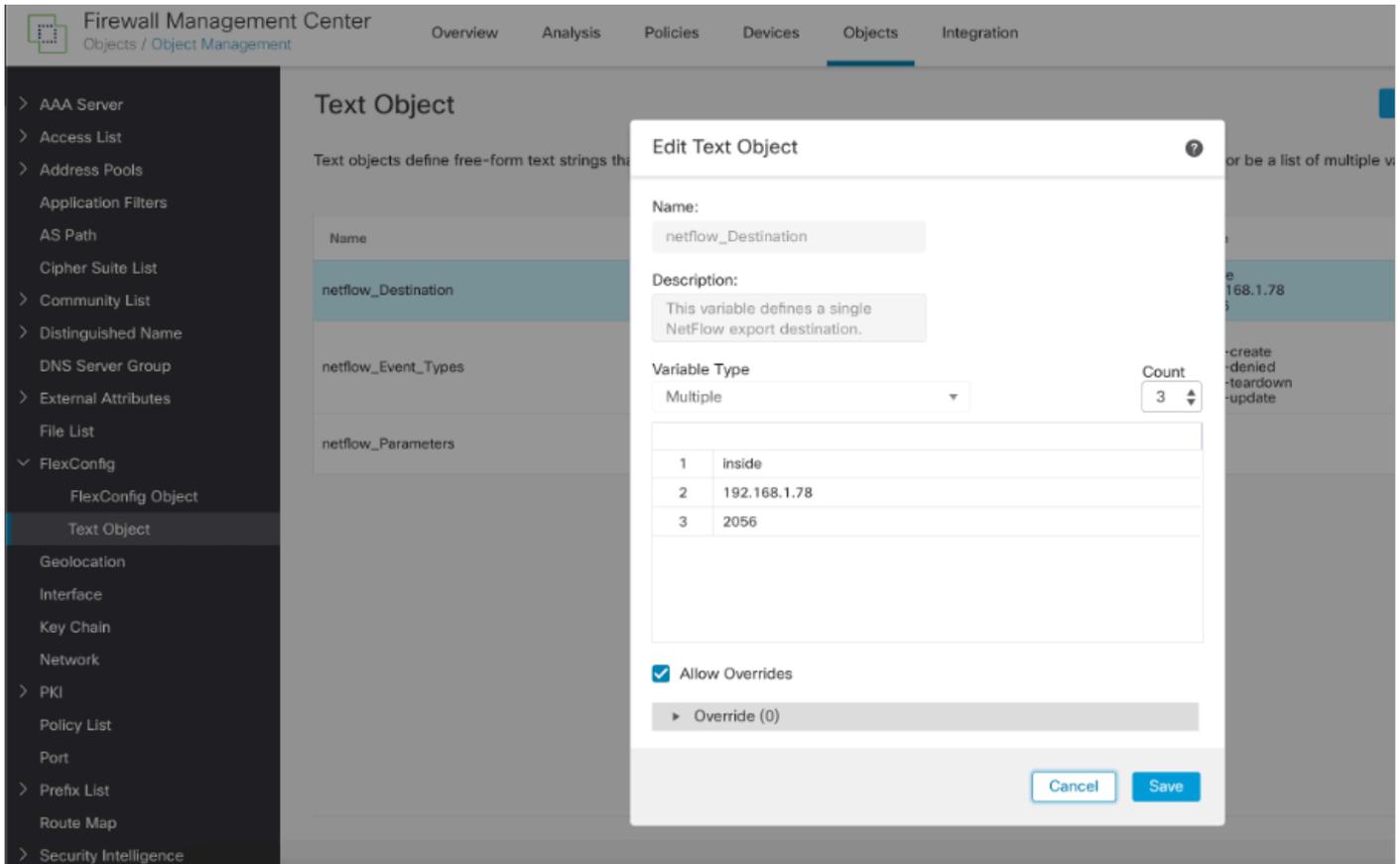
プリペンドオブジェクトを削除する

フローエクスポート関連の設定がすべて削除されました。

既存のNetFlow設定の変更

ステップ1: Netflowの宛先に作成されたテキストオブジェクトを編集します。必要なパラメータIP、インターフェイス名、またはポートを変更します。

例：IPアドレスとポートを(192.168.1.5, 2055)から(192.168.1.78, 2056)に変更しました。



Netflow送信先テキストオブジェクト

手順2：ポリシーを展開します。変更は期待どおりに反映されますが、古いNetFlow宛先設定と一緒に次のように反映されます。

```
access-list flow_export_acl extended permit ip any any
!
class-map flow_export_class
 match access-list flow_export_acl
!
policy-map global_policy
 class flow_export_class
  flow-export event-type flow-create destination 192.168.1.78
  flow-export event-type flow-denied destination 192.168.1.78
  flow-export event-type flow-teardown destination 192.168.1.78
  flow-export event-type flow-update destination 192.168.1.78
!
flow-export destination Inside 192.168.1.78 2056
flow-export destination Inside 192.168.1.5 2055
```

ステップ3：これを削除するには、「prepend」タイプのフレックスオブジェクトを作成し、設定を追加する必要があります。

no flow-export destination Inside 192.168.1.5 2055

Firewall Management Center
Objects / Object Management

FlexConfig Object

Name: AAAdummy

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert | Deployment: Once | Type: Prepend

no flow-export destination Inside 192.168.1.5 2055

Name	Dimension	Default Value	Property (Type:Name)	Override	Description
No records to display					

Cancel

NetFlow宛先の削除

ステップ4 : フレックスポリシーで、ステップ3で新しく作成したプリペンドオブジェクトを呼び出し、ポリシーを展開します。

Firewall Management Center
Devices / Flexconfig Policy Editor

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

FTD01-FP Preview Config Save Cancel

Enter Description Policy Assignments (1)

Available FlexConfig FlexConfig Object

▼ User Defined

- AAAadummy
- EEM-Script
- EEM-Script-Removal
- flow_export_class
- Netflow_Add_Destination_Copy
- Netflow_Delete_Destination_Copy
- Netflow_Event_FlexObject

▼ System Defined

- Default_DNS_Configure
- Default_Inspection_Protocol_Disable
- Default_Inspection_Protocol_Enable
- DHCPv6_Prefix_Delegation_Configure
- DHCPv6_Prefix_Delegation_UnConfigure
- DNS_Configure
- DNS_UnConfigure

Selected Prepend FlexConfigs

#	Name	Description
1	AAAadummy	

Selected Append FlexConfigs

#	Name	Description
1	Netflow_Add_Destination_Copy	Create and configure a NetFlow export destination.
2	Netflow_Event_FlexObject	Create and configure a NetFlow export destination.

Flex Configの先頭に追加

ステップ5：フレックスポリシーから先頭に追加されたオブジェクトを削除し、再度展開します。

Firewall Management Center
Devices / Flexconfig Policy Editor

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

FTD01-FP Preview Config Save Cancel

Enter Description Policy Assignments (1)

Available FlexConfig FlexConfig Object

▼ User Defined

- AAAadummy
- EEM-Script
- EEM-Script-Removal
- flow_export_class
- Netflow_Add_Destination_Copy
- Netflow_Delete_Destination_Copy
- Netflow_Event_FlexObject

▼ System Defined

- Default_DNS_Configure
- Default_Inspection_Protocol_Disable
- Default_Inspection_Protocol_Enable
- DHCPv6_Prefix_Delegation_Configure
- DHCPv6_Prefix_Delegation_UnConfigure
- DNS_Configure
- DNS_UnConfigure

Selected Prepend FlexConfigs

#	Name	Description
---	------	-------------

Selected Append FlexConfigs

#	Name	Description
1	Netflow_Add_Destination_Copy	Create and configure a NetFlow export destination.
2	Netflow_Event_FlexObject	Create and configure a NetFlow export destination.

先頭のFlexConfigの削除

NetFlow関連の構成が正常に変更されました。

```
access-list flow_export_acl extended permit ip any any
!
flow-export destination Inside 192.168.1.78 2056
!
class-map flow_export_class
 match access-list flow_export_acl
!
policy-map global_policy
 class flow_export_class
  flow-export event-type flow-create destination 192.168.1.78
  flow-export event-type flow-denied destination 192.168.1.78
  flow-export event-type flow-teardown destination 192.168.1.78
  flow-export event-type flow-update destination 192.168.1.78
```

関連資料

<https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configure-netflow-secure-event-logging-o.html>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。