詳細設定

いくつかのデバイスの機能は、ASA 設定コマンドを使用して設定されます。Device Manager はコマンドベースの多くの機能を設定できますが、それらのすべてはサポートしません。Device Manager でサポートされていないこれらの ASA 機能の一部を使用する必要がある場合は、Smart CLI または FlexConfig を使用して手動で機能を設定できます。

次のトピックでは、このタイプの高度な設定について、より詳細に説明します。

Smart CLI と FlexConfig について

Threat Defense では、ASA 設定コマンドを使用して、すべての機能ではなく一部の機能を実装します。脅威に対する防御 設定コマンドの一意のセットはありません。

次の方法により CLI を使用して機能を設定できます。

- **Smart CLI**：（推奨の方法です。）Smart CLI テンプレートは、特定の機能の定義済みテンプレートです。機能に必要なすべてのコマンドが提供されているため、変数の値を選択するだけで済みます。システムにより選択が検証されるため、機能を正しく設定できる可能性が高まります。目的の機能の Smart CLI テンプレートが存在する場合は、この方法を使用する必要があります。

- **FlexConfig**：FlexConfig ポリシーは、FlexConfig オブジェクトのコレクションです。FlexConfig オブジェクトは Smart CLI テンプレートより自由な形式であり、システムに CLI 変数はなく、データ検証も行われません。有効な一連のコマンドを作成するには、ASA 設定コマンドを知り、ASA 設定ガイドに従う必要があります。

Smart CLI と FlexConfig のポイントは、Device Manager のポリシーと設定によって直接サポートされていない機能を設定できることです。

注意 Smart CLI と FlexConfig の利用は、ASA の強力なバックグラウンドを持つ上級者が自身のリスクで行う場合にかぎることをシスコは強く推奨します。禁止されていないコマンドはすべて、設定できます。Smart CLI と FlexConfig を使用して機能を有効にすると、その他の設定済みの機能で予期しない結果が生じる可能性があります。

設定した Smart CLI と FlexConfig のオブジェクトに関するサポートについては、Cisco Technical Assistance Center にお問い合わせください。Cisco Technical Assistance Center は、顧客に代わってカスタム設定を設計したり、作成したりしません。正常な動作や他の 脅威に対する防御 機能の相互運用性について、シスコは一切保証しません。Smart CLI と FlexConfig の機能は、いつでも廃止になる可能性があります。完全に保証された機能のサポートについては、Device Manager サポートを待つ必要があります。疑問がある場合、Smart CLI または FlexConfig は使用しないでください。

ここでは、これらの機能についてさらに詳しく説明します。

Smart CLI と FlexConfig の推奨される使用法

FlexConfig ポリシーには、推奨される使用法が主に 2 つあります。

- ASA から 脅威に対する防御 に移行中で、互換性はあるが、Device Manager が直接サポートしていない機能を使用しています（および使用を継続する必要があります）。この場合、ASA で **show running-config** コマンドを使用してその互換機能の設定を確認し、その機能を実装する FlexConfig オブジェクトを作成します。2 台のデバイスでの **show running-config** の出力を比較して確認します。
- 脅威に対する防御 を使用しているが、ある設定または機能を設定する必要があります。たとえば、Cisco Technical Assistance Center が、発生している特定の問題が特定の設定により解決されると伝えます。複雑な機能については、ラボ デバイスを使用して FlexConfig をテストし、期待する動作を得られることを確認します。

ASA設定を再作成する前に、まず標準的なポリシーで同等の機能を設定できるかどうかを判断します。たとえば、アクセス コントロール ポリシーには侵入検知および防御、HTTPおよびその他のタイプのプロトコル インスペクション、URL フィルタリング、アプリケーション フィルタリング、アクセス制御が含まれており、ASAはこれらの要素を別個の機能を使用して実装します。多くの機能はCLIコマンドを使用して設定されていないので、**show running-config** の出力にすべてのポリシーが表示されるわけではありません。

（注） 常に、ASA と 脅威に対する防御 との間の重複は 1 対 1 であるわけではないことに注意してください。ASAの設定を脅威に対する防御デバイス上で完全に再現しようとしないでください。設定する機能は、FlexConfig を使用して慎重にテストする必要があります。

Smart CLI および FlexConfig オブジェクトの CLI コマンド

脅威に対する防御 では一部の機能の設定に ASA コンフィギュレーション コマンドを使用します。ASA のすべての機能に 脅威に対する防御 との互換性があるわけではありませんが、脅威に対する防御 で使用はできるが Device Manager ポリシーでは設定できない機能があります。Smart CLI および FlexConfig オブジェクトを使用すると、これらの機能を設定するために必要な CLI を指定できます。

Smart CLI または FlexConfig を使用して機能を手動で設定することに決めた場合、適切な構文を認識し、これに従ってコマンドを実装する必要があります。FlexConfig は CLI コマンド構文を検証しません。正しいシンタックスと CLI コマンドの設定に関する詳細については、ASA ドキュメンテーションを参照してください。

- 『ASA CLI Configuration Guides』では機能を設定する方法について説明しています。ガイドはこちらからご覧ください。 http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html
- 『ASA Command References』ではコマンド名ごとにその他の情報が記載されています。リファレンスはこちらからご覧ください。 http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html

ここでは、コンフィギュレーション コマンドについて詳しく説明します。

ソフトウェアのアップグレードが FlexConfig ポリシーに与える影響

新しいバージョンの 脅威に対する防御 ソフトウェアにはそれぞれ、Device Manager の機能を設定するためのサポートが追加されています。これらの新機能は、FlexConfig を使用して以前に設定した機能と重複する場合があります。

アップグレードの後に、FlexConfig ポリシーおよびオブジェクトを調べる必要があります。Device Manager または Smart CLI 内の追加されたサポートのために禁止されたコマンドがある場合は、オブジェクトのアイコンとメッセージに問題が示されます。その場合は、設定をやりなおしてください。禁止されたコマンドのリストは、コマンドをどのように設定する必要があるのかを判断するために役立ちます。

FlexConfig ポリシーに添付されている FlexConfig オブジェクトに新しく禁止されたコマンドが含まれていても、システムは変更の展開を妨げません。ただし、FlexConfig ポリシーに示されているすべての問題を解決するまでは、新しい Smart CLI オブジェクトを作成できません。

FlexConfig ポリシーから問題のあるオブジェクトを単に削除できます。これは、デバイス設定にアクティブに展開しているオブジェクトにのみ制限が適用されるためです。そのため、オブジェクトを削除してから、それらを、対応する Smart CLI または統合された Device Manager 設定を作成する際にリファレンスとして使用できます。新しい設定に不満がない場合は、単にオブジェクトを削除できます。削除されたオブジェクトに、禁止されていない要素が含まれている場合は、それらを編集してサポートされていないコマンドを削除してから、オブジェクトを FlexConfig ポリシーに再添付できます。

ASA ソフトウェアのバージョンおよび現在の CLI 設定の特定

システムが ASA ソフトウェア コマンドを使用して一部の機能を設定するため、脅威に対する防御 デバイスで実行するソフトウェアで使用されている現在の ASA バージョンを特定する必要があります。このバージョン番号に従って、機能設定時の手順に使用する ASA CLI 設定ガイドを選択します。また、現在の CLI ベースの設定を確認し、実装する ASA 設定と比較する必要があります。

脅威に対する防御 設定とどの ASA 設定も大きく異なることに注意してください。脅威に対する防御 ポリシーの多くは CLI の外部で設定されるため、コマンドを調べても設定を確認することができません。ASA と 脅威に対する防御 設定が 1 対 1 で対応するように作成しようとしないでください。

この情報を表示するには、Device Manager の CLI コンソールを開くか、デバイスの管理インターフェイスに SSH 接続し、次のコマンドを発行します。

- **show version system** また、Cisco 適応型セキュリティ アプライアンス ソフトウェアのバージョン番号を検索します。
- **show running-config** 現在の CLI 設定を表示します。
- **show running-config all** 現在の CLI 設定にすべてのデフォルト コマンドを含めます。

禁止された CLI コマンド

Smart CLI と FlexConfig の目的は、Device Manager を使用して 脅威に対する防御 デバイスで設定できない ASA デバイスで利用可能な機能を設定することです。

したがって、Device Manager に同等の機能がある ASA 機能は設定することができません。次の表に、これらの禁止されたコマンド領域のいくつかを示します。このリストには、設定モードを開始する多数の親コマンドが含まれています。親の禁止には、子コマンドの禁止が含まれています。また、コマンドの **no** バージョンと、関連する **clear** コマンドも含まれます。

FlexConfig オブジェクトエディタでは、オブジェクトにこれらのコマンドを含めることができません。Smart CLI テンプレートは、設定可能なコマンドのみが含まれるため、このリストが適用されません。

禁止された CLI コマンド	説明
aaa	**[オブジェクト（Objects)]**>**[アイデンティティソース（Identity Sources）]** を使用します。
aaa-server	**[オブジェクト（Objects)]**>**[アイデンティティソース（Identity Sources）]** を使用します。

禁止された CLI コマンド	説明
access-list	部分的にブロックされます。 • **ethertype** アクセス リストを作成できます。 • **extended** および **standard** アクセスリストは作成できません。Smart CLI 拡張アクセス リストまたは標準アクセス リスト オブジェクトを使用してこれらの ACL を作成します。その後、それらは、サービス ポリシー トラフィック クラス用の拡張 ACL により、オブジェクト名によって ACL を参照する FlexConfig サポート コマンド（**match access-list** など）で使用できます。 • **advanced** アクセス リスト（システムが **access-group** コマンドで使用する）は作成できません。代わりに、**[ポリシー（Policies）] > [アクセスコントロール（Access Control）]** を使用してアクセス ルールを設定します。 • **webtype** アクセス リストは作成できません。
anyconnect-custom-data	**[デバイス（Device）] > [リモートアクセスVPN（Remote Access VPN）]** を使用して セキュアクライアント を設定します。
asdm	この機能は脅威に対する防御システムには適用されません。
as-path	Smart CLI AS パス オブジェクトを作成し、それらを Smart CLI BGP オブジェクトで使用して、自律システム パス フィルタを設定します。
attribute	—
auth-prompt	この機能は脅威に対する防御システムには適用されません。
boot	—
call-home	—
captive-portal	**[ポリシー（Policies）] > [アイデンティティ（Identity）]** を使用して、アクティブな認証に使用するキャプティブ ポータルを設定します。
clear	—
client-update	—
clock	**[デバイス（Device）] > [システム設定（System Settings）] > [NTP]** を使用してシステム時間を設定します。
cluster	—

禁止された CLI コマンド	説明
command-alias	—
community-list	Smart CLI 拡張コミュニティ リストまたは標準コミュニティ リスト オブジェクトを作成し、それらを Smart CLI BGP オブジェクトで使用して、コミュニティ リスト フィルタを設定します。
compression	—
configure	—
crypto	[オブジェクト（Objects）]ページで、[証明書（Certificates）]、[IKEポリシー（IKE Policies）]、および [IPsecプロポーザル（IPSec Proposals）] を使用します。
ddns	**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DDNSサービス（DDNS Service）]** を使用してダイナミック DNS を設定します。
dhcp-client	—
dhcpd	**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DHCPサーバ（DHCP Server）]** を使用します。 ただし、**dhcpd option** コマンドは許可されます。
dhcprelay	代わりに、脅威防御 APIの dhcprelayservices リソースを使用します。
dns	**[オブジェクト（Objects）]** > **[DNSグループ（DNS Groups）]** を使用して DNS グループを設定し、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DNSサーバー（DNS Server）]** を使用してグループを割り当てます。
dns-group	**[オブジェクト（Objects）]** > **[DNSグループ（DNS Groups）]** を使用して DNS グループを設定し、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DNSサーバー（DNS Server）]** を使用してグループを割り当てます。
domain-name	**[オブジェクト（Objects）]** > **[DNSグループ（DNS Groups）]** を使用して DNS グループを設定し、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DNSサーバー（DNS Server）]** を使用してグループを割り当てます。
dynamic-access-policy-config **dynamic-access-policy-record**	—
enable	—

禁止された CLI コマンド	説明
event	—
failover	—
fips	—
firewall	Device Manager はルーテッド ファイアウォール モードのみをサポートしています。
hostname	**[デバイス（Device）] > [システム設定（System Settings）] > [ホスト名（Hostname）]** を使用します。
hpm	この機能は脅威に対する防御システムには適用されません。
http	**[デバイス（Device）] > [システム設定（System Settings）] > [管理アクセス（Management Access）]** で[データインターフェイス（Data Interfaces）] タブを使用します。
inline-set	—
interface（BVI、管理、イーサネット、GigabitEthernet、およびサブインターフェイス用）	部分的にブロックされます。 **[デバイス（Device）]>[インターフェイス（Interfaces）]** ページで物理インターフェイス、サブインターフェイス、およびブリッジ仮想インターフェイスを設定します。FlexConfig を使用して追加のオプションを設定できます。 ただし、次の **interface** モードコマンドは、これらのタイプのインターフェイスでは禁止されています。 **cts** **ip address** **ip address dhcp** **ipv6 address** **ipv6 enable** **ipv6 nd dad** **ipv6 nd suppress-ra** **mode** **nameif** **security-level** **shutdown** **zone-member**
vni、**redundant**、**tunnel** の **interface**	**[デバイス（Device）]>[インターフェイス（Interfaces）]** ページでインターフェイスを設定します。Device Manager は、これらのタイプのインターフェイスをサポートしていません。

禁止された CLI コマンド	説明
ip audit	この機能は脅威に対する防御システムには適用されません。代わりに、アクセス制御ルールを使用して侵入ポリシーを適用します。
ip-client	管理ゲートウェイとしてデータ インターフェイスを使用するようシステムを設定するには、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** を使用します。
ip local pool	**[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** を使用してアドレス プールを設定します。
ipsec	—
ipv6	Smart CLI IPv6 プレフィックス リスト オブジェクトを作成し、それらを Smart CLI BGP オブジェクトで使用して、IPv6 のプレフィックス リスト フィルタを設定します。
ipv6-vpn-addr-assign	**[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** を使用してアドレス プールを設定します。
isakmp	**[デバイス（Device）]** > **[サイト間VPN（Site-to-Site VPN）]** を使用します。
jumbo-frame	デフォルトの 1500 以上のインターフェイスの MTU を増やす場合、システムは自動的にジャンボ フレームのサポートを有効にします。
ldap	—
license-server	**[デバイス（Device）]** > **[スマートライセンス（Smart License）]** を使用します。
logging	**[オブジェクト（Objects）]** > **[Syslogサーバー（Syslog Servers）]** および **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[ロギング設定（Logging Settings）]** を使用します。 ただし、FlexConfig で **logging history** コマンドを設定できます。
management-access	—
migrate	**[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** および **[デバイス（Device）]** > **[サイト間VPN（Site-to-Site VPN）]** を使用して IKEv2 サポートを有効にします。

禁止された CLI コマンド	説明
mode	Device Manager はシングルコンテキストモードのみをサポートしています。
mount	—
mtu	**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** でインターフェイスごとに MTU を設定します。
nat	**[ポリシー（Policies）]** > **[NAT]** を使用します。
ngips	—
ntp	**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[NTP]** を使用します。
object-group network **object network**	**[オブジェクト（Objects）]**>**[ネットワーク（Network）]** を使用します。 FlexConfig でネットワーク オブジェクトまたはグループを作成することはできませんが、テンプレート内で変数としてオブジェクト マネージャで定義されているネットワーク オブジェクトおよびグループは使用できます。
object service |natorigsvc **object service |natmappedsvc**	**object service** コマンドは一般に使用できますが、|natorigsvc または |natmappedsvc という内部オブジェクトは編集できません。これらの名前の垂直バーは意図的であり、制限されているオブジェクト名の最初の文字です。
passwd **password**	—
password-policy	—
policy-list	スマート CLI ポリシー リスト オブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、ポリシー リストを設定します。
policy-map sub-commands	ポリシー マップでは次のコマンドを設定できません。 **priority** **police** **match tunnel-group**
prefix-list	Smart CLI IPv4 プレフィックス リスト オブジェクトを作成し、それらを Smart CLI OSPF または BGP オブジェクトで使用して、IPv4 のプレフィックス リスト フィルタを設定します。
priority-queue	—

禁止された CLI コマンド	説明
privilege	—
reload	リロードはスケジュールできません。システムは、システムを再起動するために **reload** コマンドを使用せず、**reboot** コマンドを使用します。
rest-api	この機能は脅威に対する防御システムには適用されません。REST API は常にインストールされ、有効になります。
route	**[デバイス（Device）]** > **[ルーティング（Routing）]** を使用してスタティック ルートを設定します。
route-map	スマート CLI ルート マップ オブジェクトを作成し、それらをスマート CLI OSPF オブジェクトまたはスマート CLI BGP オブジェクトで使用して、ルート マップを設定します。
router bgp	BGP には Smart CLI テンプレートを使用します。
router eigrp	EIGRP には Smart CLI テンプレートを使用します。
router ospf	OSPF には Smart CLI テンプレートを使用します。
scansafe	この機能は脅威に対する防御システムには適用されません。代わりに、アクセス制御ルールで URL フィルタリングを設定します。
setup	この機能は脅威に対する防御システムには適用されません。
sla	—
snmp-server	SNMP を設定するには、FTP API SNMP リソースを使用します。
ssh	**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** で [データインターフェイス（Data Interfaces）] タブを使用します。
ssl	**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[SSL設定（SSL Settings）]** を使用します。
telnet	Threat Defense は Telnet 接続をサポートしません。デバイス CLI にアクセスするには、Telnet の代わりに SSH を使用します。
time-range	—

禁止された CLI コマンド	説明
tunnel-group	**[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** および **[デバイス（Device）]** > **[サイト間VPN（Site-to-Site VPN）]** を使用します。
tunnel-group-map	**[デバイス（Device）]** > **[リモートアクセスVPN（Remote Access VPN）]** および **[デバイス（Device）]** > **[サイト間VPN（Site-to-Site VPN）]** を使用します。
user-identity	**[ポリシー（Policies）]** > **[アイデンティティ（Identity）]** を使用します。
username	CLI ユーザーを作成するには、デバイスに対して SSH またはコンソールセッションを開き、**configure user** コマンドを使用します。
vpdn	—
vpn	—
vpn-addr-assign	—
vpnclient	—
vpn-sessiondb	—
vpnsetup	—
webvpn	—
zone	—
zonelabs-integrity	この機能は脅威に対する防御システムには適用されません。

Smart CLI テンプレート

次の表では、機能に基づく Smart CLI テンプレートについて説明します。

（注） スマート CLI テンプレートを使用して OSPF と BGP を設定することもできます。ただし、これらのテンプレートは、[詳細設定（Advanced）] ページではなく **[デバイス（Device）]** > **[ルーティング（Routing）]** ページから使用できます。

機能	テンプレート	説明
オブジェクト：AS パス	AS パス	ルーティング プロトコル オブジェクトで使用する AS パス オブジェクトを作成します。

機能	テンプレート	説明
オブジェクト：アクセス リスト	拡張アクセス リスト 標準アクセス リスト	ルーティング オブジェクトで使用する拡張 ACL または標準 ACL を作成します。ACL を使用する許可コマンドを設定する FlexConfig オブジェクトからの名前によって、これらのオブジェクトを参照することもできます。
オブジェクト：コミュニティ リスト	拡張コミュニティ リスト 標準コミュニティ リスト	ルーティング オブジェクトで使用する拡張コミュニティ リストまたは標準コミュニティ リストを作成します。
オブジェクト：プレフィックス リスト	IPv4 プレフィックス リスト IPv6 プレフィックス リスト	ルーティング オブジェクトで使用する IPv4 または IPv6 プレフィックス リストを作成します。
オブジェクト：ポリシー リスト	ポリシー リスト	ルーティング オブジェクトで使用するポリシー リストを作成します。
オブジェクト：ルート マップ	ルート マップ	ルーティング オブジェクトで使用するルート マップを作成します。

Smart CLI および FlexConfig に関する注意事項と制限事項

Smart CLI または FlexConfig を介して機能を設定するときは、次の点に注意してください。

- FlexConfig オブジェクトで定義されているコマンドは、Smart CLI を含む Device Manager で定義された機能のすべてのコマンドの後に展開されます。したがって、デバイスに対してこれらのコマンドが発行される前に設定されているオブジェクト、インターフェイスなどに依存する場合があります。Smart CLI テンプレートで FlexConfig が展開された項目を使用する必要がある場合は、Smart CLI テンプレートを作成して展開する前に FlexConfig を作成して展開します。たとえば、OSPF Smart CLI テンプレートを使用して EIGRP ルートを再配布する場合は、最初に FlexConfig を使用して EIGRP を設定し、それから OSPF Smart CLI テンプレートを作成します。
- FlexConfig から設定した機能または機能の一部を削除するが、Smart CLI テンプレートがその機能を参照している場合は、最初に機能を使用する Smart CLI テンプレートでコマンドを削除する必要があります。その後、Smart CLI で設定された機能が参照しないように設定を展開します。FlexConfig から機能を削除して設定を再展開すると、最終的に完全削除できます。

Smart CLI オブジェクトの設定

Smart CLI オブジェクトは、Device Manager の他では構成することができない機能を定義します。Smart CLI オブジェクトは、機能の構成において一定レベルのガイダンスを提供します。指定された機能（テンプレート）について、すべての可能なコマンドが事前に読み込まれ、入力した変数が検証されます。したがって、機能を構成するためにCLIコマンドを使用しても、Smart CLI オブジェクトは FlexConfig オブジェクトほど自由な形式ではありません。

Smart CLI テンプレートは一定レベルのガイダンスを提供しますが、ネットワークで正しく動作するように値を選択するために ASA 構成ガイドとコマンド リファレンスを読み、コマンドの使用方法を理解する必要があります。理想的には、動作する ASA 構成はすでにあり、必要とされるのは Smart CLI オブジェクトでコマンドの同じシーケンスを構築することだけです。

Smart CLI オブジェクトは、機能エリアによってグループ化されます。

（注） 定義したすべての Smart CLI オブジェクトが展開されます。FlexConfig とは異なり、いくつかの Smart CLI オブジェクトを作成し、その中から選択して展開することはできません。構成する機能に対してのみ Smart CLI オブジェクトを作成します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で [スマートCLI（Smart CLI）] の下の該当する機能のエリアをクリックします。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

オブジェクトを削除するには、そのオブジェクトのごみ箱アイコン（）をクリックします。

ステップ 4 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 5 構成する機能の [CLIテンプレート（CLI Template）] を選択します。

システムはコマンドテンプレートを [テンプレート（Template）] ウィンドウに読み込みます。最初に必要なコマンドのみが表示されます。これらはテンプレートに必要な最小構成を表します。

ステップ 6 変数を入力し、必要に応じてテンプレートにコマンドを追加します。

理想的には、ASA または Threat Defense デバイス（Management Center によって管理されているもの）から既存の構成を使用して作業します。所有している構成では、単にネットワーク内

のこの特定のデバイスの場所に応じて IP アドレス、インターフェイス名などの変数を変更して、テンプレートをそれに適合させる必要があります。

テンプレートへの入力に関するいくつかのヒントを次に示します。

- 変数の値を選択するには、変数のいずれかをクリックして適切な値を入力するか、リストから選択します（値が列挙されている場合）。入力を必要とする変数をマウスオーバーすると、数値の範囲など、オプションの有効な値が表示されます。一部のケースでは推奨値が記載されています。

  たとえば、OSPF のテンプレートでは、必要なコマンドの **router ospf** *process-id* をマウスオーバーすると「Process ID (1-65535)」と表示され、*process-id* をクリックするとフィールドが強調表示されます。単に希望の数値を入力します。

- 変数のオプションを選択するときに、オプションを構成するために使用できる追加のコマンドがある場合、それらが自動的に公開され必要に応じて有効または無効になります。これらの追加のコマンドを確認します。

- テンプレート上の [表示（Show）] /[無効を非表示（Hide Disabled）] リンクを使用してビューを制御します。無効なコマンドは構成されませんが、それらを表示して構成する必要があります。完全なテンプレートを表示するには、テンプレート上の[無効を表示（Show Disabled）] リンクをクリックします。構成されるコマンドのみを表示するには、テーブルの上の [無効を非表示（Hide Disabled）] リンクをクリックします。

- オブジェクトを最後に保存して以降のすべての編集をクリアするには、テンプレートの上の [リセット（Reset）] リンクをクリックします。

- オプションのコマンドを有効にするには、行番号の左側にある [+] のボタンをクリックします。

- オプションのコマンドを無効にするには、行番号の左側にある [-] のボタンをクリックします。行を編集した場合、編集内容は削除されません。

- コマンドを複製するには、[オプション...（Options...）] ボタンをクリックして [複製（Duplicate）] を選択します。コマンドを複数回入力することが有効な場合にのみ、コマンドを複製できます。

- 複製したコマンドを削除するには、[オプション...（Options...）] ボタンをクリックして [削除（Delete）] を選択します。ベース テンプレートの一部であるコマンドは削除できません。

ステップ 7 [OK] をクリックします。

FlexConfig ポリシーの設定

FlexConfig ポリシーは単にデバイスの構成に展開する FlexConfig オブジェクトのリストです。ポリシーに含まれるこれらのオブジェクトのみが展開され、他はすべてが単に定義されるだけで使用されません。

FlexConfig オブジェクトで定義されているコマンドは、Smart CLI を含む Device Manager で定義された機能のすべてのコマンドの後に展開されます。したがって、デバイスに対してこれらのコマンドが発行される前に設定されているオブジェクト、インターフェイスなどに依存する場合があります。Smart CLI テンプレートで FlexConfig が展開された項目を使用する必要がある場合は、Smart CLI テンプレートを作成して展開する前に FlexConfig を作成して展開します。たとえば、OSPF Smart CLI テンプレートを使用して EIGRP ルートを再配布する場合は、最初に FlexConfig を使用して EIGRP を設定し、それから OSPF Smart CLI テンプレートを作成します。

（注） 機能の Smart CLI テンプレートがある場合、FlexConfig を使用してそれを構成できません。Smart CLI オブジェクトを使用する必要があります。

始める前に

FlexConfig オブジェクトを作成します。次のトピックを参照してください。

- FlexConfig オブジェクトの設定 （16 ページ）
- FlexConfig オブジェクトの変数の作成 （19 ページ）
- 秘密キー オブジェクトの設定 （28 ページ）

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigポリシー（FlexConfig Policy）]** をクリックします。

ステップ 3 [グループリスト（Group List）] 内のオブジェクトのリストを管理します。

- オブジェクトを追加するには、[+] ボタンをクリックします。オブジェクトがまだ存在しない場合は、[新規FlexConfigオブジェクトを作成（Create New FlexConfig Object）] をクリックして定義します。
- オブジェクトを削除するには、オブジェクトエントリの右側にある [X] ボタンをクリックします。

（注） 各オブジェクトは完全に自己完結型で、他の FlexConfig オブジェクトで定義されている構成に依存しないことをお勧めします。これにより、他のオブジェクトに影響を与えずにオブジェクトを追加または削除できます。

ステップ 4 [プレビュー（Preview）] ペインで提案されたコマンドを評価します。

[展開（Expand）] ボタン（その後 [折りたたむ（Collapse）]）をクリックすると画面を拡大できます。これにより長いコマンドがより見やすくなります。

プレビューは、変数を評価し、発行される正確なコマンドを生成します。これらのコマンドが正しく有効なことを確認します。コマンドがエラーを生じたり、デバイスが使用できなくなる不適切な構成でないことを確保する責任があります。

注意 システムはコマンドを検証しません。無効なコマンドや、破壊の可能性があるコマンドも展開が可能です。変更を展開する前に慎重にプレビューを確認します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

FlexConfig ポリシーを編集した後は、次の展開の結果を慎重に調べてください。エラーがある場合は、オブジェクトの CLI を修正します。FlexConfig ポリシーのトラブルシューティング（29 ページ） を参照してください。

FlexConfig オブジェクトの設定

FlexConfig オブジェクトには、別の方法では Device Manager を使用して設定できない特定の機能を設定するために必要な ASA コマンドが含まれます。コマンドのシーケンスは、入力ミスなく正しく入力する必要があります。システムは、FlexConfig オブジェクトの内容を検証しません。

設定する一般的な機能ごとに別のオブジェクトを作成することをお勧めします。たとえば、バナーを定義し、RIP ルーティング プロトコルも設定する場合は、2 つの独立したオブジェクトを使用します。機能を別のオブジェクトに分離すると、展開するオブジェクトの選択が容易になり、またトラブルシューティングも容易になります。

（注） **enable** および **configure terminal** コマンドは含めないでください。システムは、自動的にコンフィギュレーション コマンドに適切なモードに入ります。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 4 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 5 [変数（Variables）] セクションで、オブジェクト本文内で使用する変数を作成します。

作成する必要がある唯一の変数は Device Manager 内で定義されているオブジェクトを指すもので、具体的にはネットワーク、ポート、および秘密キーの変数の型、または名前付きインターフェイスを指すインターフェイス変数です。他の変数の型では、単にオブジェクト本文に値を入力できます。

変数の作成と使用の詳細については、FlexConfig オブジェクトの変数の作成 （19 ページ）を参照してください。

ステップ 6 [テンプレート（Template）] セクションに、機能を設定するために必要な ASA コマンドを入力します。

機能を設定するために正しい順序でコマンドを入力する必要があります。ASA CLI 構成ガイドを使用して、コマンドを入力する方法を学習します。理想的には、ASA または参照として使用できる別の 脅威に対する防御 デバイスから事前テスト済みの構成ファイルを取得します。

変数を参照および処理するために Mustache 表記を使用することもできます。詳細については、FlexConfig 変数の参照と値の取得 （20 ページ）を参照してください。

オブジェクト本文を作成するためのいくつかのヒントを次に示します。

- 行を追加するには、行の末尾にカーソルを置いて、Enter キーを押します。
- 変数を使用するには、二重括弧に間に変数名を入力します：{{変数名}}。オブジェクトを参照する変数では、取得する値の属性を含める必要があります：{{変数名.属性}}。使用可能な属性は、オブジェクト タイプによって異なります。詳細については、変数参照：{{variable}} または {{{variable}}} （20 ページ）を参照してください。
- Smart CLI オブジェクトを使用するには、オブジェクト名を入力します。Smart CLI に設定されているルーティング プロセスを参照する必要がある場合は、プロセス ID を入力します。FlexConfig オブジェクト内の Smart CLI オブジェクトの参照 （26 ページ）を参照してください。
- テンプレート本体の上の [展開する/折りたたむ（Expand/Collapse）] リンクをクリックして、本体を大きくまたは小さくします。
- [リセット（Reset）] リンクをクリックして、オブジェクトを最後に保存した後に行ったすべての変更を消去します。

ステップ 7 [ネゲートテンプレート（Negate Template）] セクションに、オブジェクト本体で設定したコマンドを削除または入れ替えるために必要なコマンドを入力します。

ネゲート セクションは非常に重要であり、2 つの目的を果たします。

- 展開を簡単にします。本体でコマンドを再展開する前に、最初に設定を消去したり元に戻すためにこれらのコマンドを使用します。これにより正常に展開されます。
- FlexConfig ポリシーからオブジェクトを削除することによって機能を削除する場合、システムはデバイスからコマンドを削除するためにこれらのコマンドを使用します。

オブジェクト本体内でCLIをネゲートまたは入れ替えるために必要なコマンドを指定しない場合、展開ではデバイス全体の構成をクリアし、オブジェクト内のコマンドだけではなく、すべてのポリシーを再展開する必要があります。これにより展開にかかる時間が長くなり、またトラフィックが中断されます。オブジェクト本体で定義されている構成を元に戻すために必要なこれらのコマンドがすべてあり、これだけであることを確認します。negate コマンドは通常、テンプレートで**no**形式または**clear**形式のコマンドになりますが、有効だった機能を実際にオフする場合、「negate」コマンドは実際には機能を有効にする正形式のコマンドになります。

ASA 構成ガイドとコマンド リファレンスを使用して、適切なコマンドを判断します。場合によっては、単一のコマンドで設定を元に戻すことができます。たとえば、RIP を構成するオブジェクトでは、単純な **no router rip** コマンドで、サブコマンドを含めた **router rip** 構成全体を削除します。

同様に、複数行のバナーを作成するために **banner login** コマンドをいくつかを入力した場合、単一の **no banner login** コマンドでログインバナー全体が無効になります。

テンプレートで複数のネストされたオブジェクトを作成する場合、ネゲートテンプレートでは逆の順番でオブジェクトを削除する必要があります（つまり、オブジェクトを削除する前にオブジェクトへの参照を最初に削除します）。たとえば、まず ACL を作成して、トラフィック クラスで ACL を参照し、ポリシー マップでトラフィック クラスを参照し、最後にサービス ポリシーを使用してポリシー マップを有効にする場合、ネゲート テンプレートではまずサービス ポリシーを削除してからポリシー マップ、トラフィック クラス、最後に ACL の順で削除して、設定を元に戻す必要があります。

ステップ 8 [OK] をクリックします。

次のタスク

単に FlexConfig オブジェクトを作成するだけでは、それを展開するのには十分ではありません。オブジェクトを FlexConfig ポリシーに追加する必要があります。FlexConfig ポリシー内のこれらのオブジェクトのみ展開されます。これにより FlexConfig オブジェクトの改善が可能になり、すべてが自動的に展開されるのではなくいくつかは特別な用途のために利用可能になります。FlexConfig ポリシーの設定 （15 ページ） を参照してください。

FlexConfig オブジェクトの変数の作成

FlexConfig オブジェクト内部で使用する変数は、オブジェクト自体の内部で定義されます。変数の個別のリストはありません。したがって、変数を定義して個別の FlexConfig オブジェクト内で使用することはできません。

変数はこれらの主な利点を提供します。

- Device Manager を使用して定義されているオブジェクトを指し示すことを可能にします。これには、ネットワーク、ポート、および秘密鍵オブジェクトが含まれます。
- これらは変更する可能性がある値をオブジェクト本体から分離します。したがって、値を変更する場合は単に変数を編集します。オブジェクト本体を編集する必要はありません。これは、いくつかのコマンドライン内のオブジェクトを参照する必要がある場合に特に便利です。

この手順では、FlexConfig オブジェクトに変数を追加するプロセスについて説明します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** ページから FlexConfig オブジェクトを編集または作成します。

「FlexConfig オブジェクトの設定 （16 ページ）」を参照してください。

ステップ 2 [変数（Variables）] セクションで次のいずれかを実行します。

- 変数を追加するには、[+] ボタンをクリックします（またはまだ定義されていない場合は [変数の追加（Add Variable）] をクリックします）。
- 変数を編集するには、その変数の編集アイコン（）をクリックします。

変数を削除するには、その変数のごみ箱アイコン（）をクリックします。その変数への参照をテンプレート本体から削除していることを確認します。

ステップ 3 変数の名前を入力し、任意で説明を入力します。

ステップ 4 変数のデータの [タイプ（Type）] を選択し、値を入力または選択します。

次のタイプの変数を作成できます。変数を使用するコマンドのデータ要件に適合するタイプを選択します。

- [文字列（String）]：テキスト文字列です。 たとえば、ホスト名、ユーザ名など。
- [数値（Numeric）]：整数値です。 コンマ、小数、（マイナスなどの）記号または 16 進数表記を含めないでください。非整数の場合は文字列変数を使用します。
- [ブール値（Boolean）]：論理的 true/false です。 True または False を選択します。

- [ネットワーク（Network）]：[オブジェクト（Objects）] ページで定義されているネットワーク オブジェクトやグループです。ネットワーク オブジェクトまたはグループを選択します。
- [ポート（Port）]：[オブジェクト（Objects）] ページで定義されている TCP または UDP ポート オブジェクトです。ポート オブジェクトを選択します。グループやその他のプロトコル用のオブジェクトは選択できません。
- [インターフェイス（Interface）]：[デバイス（Device）]>[インターフェイス（Interfaces）] のページで定義されている名前付きインターフェイスです。インターフェイスを選択します。名前を持たないインターフェイスは選択できません。
- [IP]：ネットマスクまたはプレフィックス長がない単一の IPv4 または IPv6 IP アドレスです。
- [秘密（Secret）]：FlexConfig に定義された秘密キー オブジェクトです。オブジェクトを選択します。秘密キー オブジェクトの作成の詳細については、秘密キー オブジェクトの設定 （28 ページ）を参照してください。

ステップ 5 [変数（Variable）] ダイアログ ボックスで [追加（Add）] または [保存（Save）] をクリックします。

これで FlexConfig オブジェクトの本体内の変数を使用できます。変数を参照する方法は、変数のタイプによって異なります。これらの変数の使用方法の詳細については、次のトピックを参照してください。

- 変数参照：{{variable}} または {{{variable}}} （20 ページ）
- セクション {{#key}} {{/key}} と逆セクション {{^key}} {{/key}} （24 ページ）

ステップ 6 [FlexConfigオブジェクト（FlexConfig Object）] ダイアログボックスで [OK] をクリックします。

FlexConfig 変数の参照と値の取得

FlexConfig はテンプレート言語として Mustache を使用しますが、サポートは、次のセクションで説明する機能に限定されます。これらの機能を使用して、変数を参照し、その値を取得して、処理します。

変数参照：{{variable}} または {{{variable}}}

FlexConfig オブジェクト内で定義した変数を参照するには、次の表記を使用します。

{{*variable_name*}}

または

{{{*variable_name*}}}

詳細設定

次の種類の変数を含む、単一値の変数の場合はこれで十分です：[数値（Numeric）]、[文字列（String）]、[ブール値（Boolean）]、[IP]。変数に & などの特殊文字が含まれている場合、三重カッコを使用します。または、すべての変数で常に三重カッコを使用することもできます。

ただし、構成データベース内のオブジェクトとしてモデル化される要素を指し示す変数の場合は、ドット表記を使用し、取得するオブジェクト属性の名前を含める必要があります。関連するオブジェクト タイプの API エクスプローラでのモデルを調べることによって、これらの属性名を確認できます。次の種類の変数を使用するには次の標記を使用する必要があります：[秘密（Secret）]、[ネットワーク（Network）]、[ポート（Port）]、[インターフェイス（Interface）]。

{{*variable_name.attribute*}}

たとえば、net-object1（ネットワーク グループではなく、ネットワーク オブジェクトを示す）という名前のネットワーク変数のアドレスを取得するには、次を使用します。

{{net-object1.value}}

オブジェクト内のオブジェクトから属性値を取得しようとする場合は、一連のドット区切りの属性を使用して、目的の値にドリルダウンする必要があります。たとえば、インターフェイスの IP アドレスは、ipv4 と ipv6 という名前のサブオブジェクトとして、インターフェイス オブジェクトにモデル化されます。したがって、int-inside という名前の（内部インターフェイスを示す）インターフェイス変数の IPv4 アドレスとサブネット マスクを取得するには、次を使用します。

{{int-inside.ipv4.ipAddress.ipAddress}} {{int-inside.ipv4.ipAddress.netmask}}

（注） API エクスプローラを開くには、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。

次の表に、変数の型とそれらを参照する方法、オブジェクトの場合は、API モデルの名前と使用する可能性が高い参照を示します。

変数の型	参照モデル	説明
ブール値 （単純変数）	**変数**： {{*variable_name*}} **セクション**： {{#*variable_name*}} commands {{/*variable_name*}} **反転セクション**： {{^*variable_name*}} commands {{/*variable_name*}}	論理的 true/false。ブール変数の主な目的は、セクションまたは反転セクションです。たとえば、定期的にまたは特別な事情の下でのみ機能を有効にする必要がある場合、ブール変数の値を編集してコマンドのセクションをオンまたはオフにできます。 いくつかのオブジェクトにも、セクションのオプションの処理を提供するために使用できるそれらのモデルのブール型の属性があります。

変数の型	参照モデル	説明

インターフェイス
（オブジェクト変数：API モデルはインターフェイスです）
	変数：
	{{*variable_name*.*attribute*}}
	セクション：
	`{{#variable_name.attribute}}`
	`commands`
	`{{/variable_name.attribute}}`
	反転セクション：
	`{{^variable_name.attribute}}`
	`commands`
	`{{/variable_name.attribute}}`
		[デバイス（Device）] > [インターフェイス（Interfaces）] のページで定義されている名前付きインターフェイス。無名のインターフェイスを指定することはできません。
		インターフェイス モデルで使用できるさまざまな属性があります。またインターフェイス モデルには、サブオブジェクト、たとえば IP アドレスが含まれます。
		次に、役に立つ主な属性をいくつか示します。
		• *variable_name*.**name** はインターフェイスの論理名を返します。
		• *variable_name*.**hardwareName** は GigabitEthernet1/8 などのインターフェイスポート名を返します。
		• *variable_name*.**managementOnly** はブール値です。TRUE は、インターフェイスが管理限定として定義されていることを意味します。FALSE は、インターフェイスがデバイスを通過するトラフィックに使用されることを意味します。このオプションは、セクション キーとして使用できます。
		• *variable_name*.**ipv4.ipAddress.ipAddress** はインターフェイスの IPv4 アドレスを返します。
		• *variable_name*.**ipv4.ipAddress.netmask** はインターフェイスの IPv4 アドレスのサブネットマスクを返します。

IP （単純変数）	**変数**： {{*variable_name*}}	ネットマスクまたはプレフィックス長がない単一の IPv4 または IPv6 IP アドレス。

変数の型	参照モデル	説明
ネットワーク （オブジェクト変数：API モデルは NetworkObject です）	**変数（ネットワークオブジェクト）**： {{*variable_name.attribute*}} **セクション（グループオブジェクト）**： {{#*variable_name*.**networkObjects**}} commands referring to one of {{**value**}} {{**name**}} {{/*variable_name*.**networkObjects**}}	[オブジェクト（Objects）]ページで定義されているネットワーク オブジェクトやグループです。セクションを使用してネットワーク グループを処理できます。 次に、役に立つ主な属性を示します。 • {{*variable_name*.**name**}} はネットワークオブジェクトまたはグループの名前を返します。 • {{*variable_name*.**value**}} はネットワークオブジェクト（ネットワークグループではありません）の IP アドレスの内容を返します。ネットワーク オブジェクトの持つ内容のタイプが指定されたコマンドに対して正しいことを確認します。たとえば、サブネット アドレスではなくホスト アドレスです。 • {{*variable_name*.**groups**}} はネットワークグループに含まれるネットワークオブジェクトのリストを返します。これはネットワーク グループを指す変数でのみ使用します。またグループの内容を繰り返し処理するセクション タグに使用します。{{**value**}} または {{**name**}} のいずれかを使用して、次に各ネットワークオブジェクトの内容を取得します。
数値 （単純変数）	**変数**： {{*variable_name*}}	整数値。コンマ、小数、（マイナスなどの）記号または 16 進数表記を含めないでください。非整数の場合は文字列変数を使用します。
ポート （オブジェクト変数：API モデルは、PortObject、tcpports または udpports です）	**変数**： {{*variable_name.attribute*}}	[オブジェクト（Objects）] ページで定義されている TCP または UDP ポート オブジェクトです。これは、ポート グループではなく、ポート オブジェクトである必要があります。 次に、役に立つ主な属性を示します。 • {{*variable_name*.**port**}} はポート番号を返します。プロトコルは含まれません。 • {{*variable_name*.**name**}} はポートオブジェクトの名前を返します。
秘密（Secret） （オブジェクト変数：API モデルは Secret です）	**変数**： {{*variable_name*.**password**}} または {{{*variable_name*.**password**}}}	FlexConfig に定義された秘密キー オブジェクトです。 参照する必要があるのは、暗号化された文字列を返す **password** 属性のみです。 パスワードに & などの特殊文字が含まれている場合、三重カッコを使用します。

変数の型	参照モデル	説明
文字列 （単純変数）	**変数**： {{*variable_name*}}	テキスト文字列です。たとえば、ホスト名、ユーザー名など。

セクション{{#key}}{{/key}}と逆セクション{{^key}}{{/key}}

セクションまたは逆セクションは、セクションの開始タグと終了タグの間のコマンドのブロックで、処理条件としてキーを使用します。セクションの処理方法は、それが通常か逆セクションかによって異なります。

- 通常のセクション（または単にセクション）は、キーがTRUEであるか、または空でないコンテンツを含む場合に処理されます。キーがFALSEであるか、またはオブジェクトにコンテンツがない場合、セクション内のコマンドは設定されません。セクションはバイパスされます。

  次に、通常のセクションの構文を示します。

```
{{#key}}
one or more commands
{{/key}}
```

- 逆セクションは、セクションの反対です。キーがFALSEであるか、またはオブジェクトに内容がない場合に処理されます。キーがTRUEであるか、またはオブジェクトにコンテンツがある場合、逆セクションはバイパスされます。

  次に、逆セクションの構文を示します。唯一の違いは、キャレットがハッシュタグを置き換えることです。

```
{{^key}}
one or more commands
{{/key}}
```

次のトピックで、セクションおよび逆セクションの主な用途について説明します。

複数値の変数を処理する方法

複数値の変数の処理の主な例は、ネットワークグループを指すネットワーク変数です。グループに複数のオブジェクトが含まれている（**objects**属性の下）ので、ネットワークグループ内の値を繰り返し実行し、異なる値を使用して複数回同じコマンドを設定できます。

オブジェクトグループによってオブジェクトの属性に含まれるネットワークオブジェクトが定義されますが、ネットワークオブジェクトの内容はオブジェクトに含まれていません。代わりに、**networkObjects**属性を使用してネットワークオブジェクトの内容を取得します。

たとえば、ホスト192.168.30.0、192.168.20.0、192.168.10.0を含むnet-groupという名前のネットワーク グループがある場合は、次の方法を使用して、RIPルーティング用の各アドレスにネットワーク コマンドを設定できます。ネットワークオブジェクトの**value**属性のみを使用す

ることに注意してください。セクションの開始時に **net-group.networkObjects** を使用すると、属性値がメンバオブジェクトから取得されるためです。（FlexConfigオブジェクト内の「value」属性に個別の変数を作成しないでください）。

```
router rip
{{#net-group.networkObjects}}
 network {{value}}
{{/net-group.networkObjects}}
```

システムはセクションの構造を次のように変換します。

```
router rip
   network 192.168.10.0
   network 192.168.20.0
   network 192.168.30.0
```

ブール値または空のオブジェクトに基づいて省略可能な処理を実行する方法

（注） このトピックの例は、説明のみを目的としたものです。たとえば、FlexConfig を使用してバージョン 6.7 以降の SNMP を設定することはできません。代わりに Threat Defense API SNMP リソースを使用する必要があります。

セクションの開始タグ内の変数のコンテンツがTRUEの場合、またはオブジェクトが空でない場合、セクションは処理されます。ブール値が FALSE または空（空のオブジェクトなど）のセクションは省略されます。

ここでの主な用途はブール値用です。たとえば、ブール変数を作成し、変数の対象であるセクション内にコマンドを置きます。その後、FlexConfig オブジェクト内のコマンドのセクションを有効または無効にする必要がある場合、ブール変数の値を変更する必要があるだけで、これらの行をコードから削除する必要はありません。これにより、簡単に、機能を有効または無効にできます。

たとえば、SNMP を有効にする FlexConfig を使用する場合、SNMP トラップをオフにできます。enable-traps という名前のブール変数を作成し、最初はTRUEに設定します。次に、トラップをオフにする場合、変数を編集して FALSE に変更し、オブジェクトを保存して、設定を再展開するだけです。コマンド シーケンスは次のようになります。

```
snmp-server enable
snmp-server host inside 192.168.1.5
snmp-server community clearTextString
{{#enable-traps}}
snmp-server enable traps all
{{/enable-traps}}
```

オブジェクト内のブール値に基づいてこのタイプの処理を行うこともできます。たとえば、そこでいくつかの特性を設定する前に、インターフェイスが管理専用かどうかをチェックできます。次の例で、int-inside は inside という名前のインターフェイスを指すインターフェイス変数です。インターフェイスが管理専用に設定されていない場合にのみ、FlexConfig はそのイン

ターフェイスで EIGRP 関連のインターフェイス オプションを設定します。ブール値が FALSE の場合にのみコマンドが設定されるように、逆セクションを使用します。

```
router eigrp 2
 network 192.168.1.0 255.255.255.0
{{^int-inside.managementOnly}}
interface {{int-inside.hardwareName}}
 hello interval eigrp 2 60
 delay 200
{{/int-inside.managementOnly}}
```

FlexConfig オブジェクト内の Smart CLI オブジェクトの参照

FlexConfig オブジェクトを作成する場合、変数を使用して、Device Manager 内で設定可能なオブジェクトを示すことができます。たとえば、インターフェイス要素やネットワーク オブジェクトを示す変数を作成できます。

ただし、同じ方法で Smart CLI オブジェクトを示すことはできません。

代わりに、FlexConfig ポリシーで使用する必要がある Smart CLI オブジェクトを作成する場合は、適切な場所で Smart CLI オブジェクトの名前を単純に入力します。

たとえば、プロトコル インスペクションを設定する場合、トラフィック クラスとして、拡張アクセス リストを使用することがあります。これは、拡張アクセスリストの Smart CLI オブジェクトが存在するため、Smart CLI オブジェクトを使用して ACL を作成する必要があるためです。FlexConfig オブジェクトで **access-list** コマンドを使用することはできません。

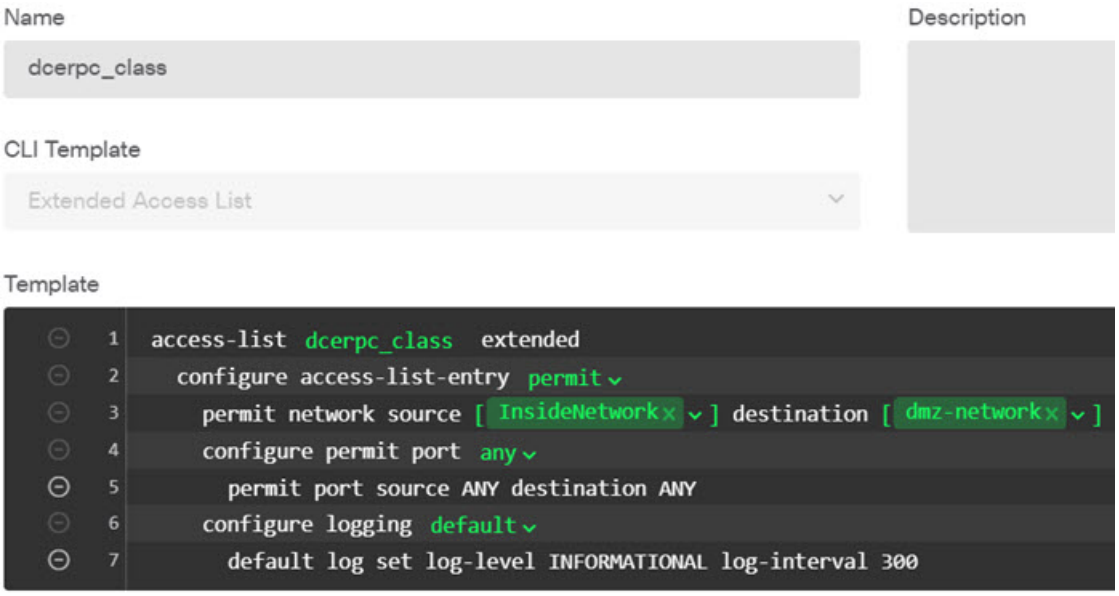
たとえば、192.168.1.0/24 および 192.168.2.0/24 ネットワーク間でグローバルに DCERPC インスペクションを有効化する場合は、次の手順を実行します。

手順

ステップ 1 2つのネットワークに個別のネットワーク オブジェクトを作成します。たとえば、InsideNetwork と dmz-network。

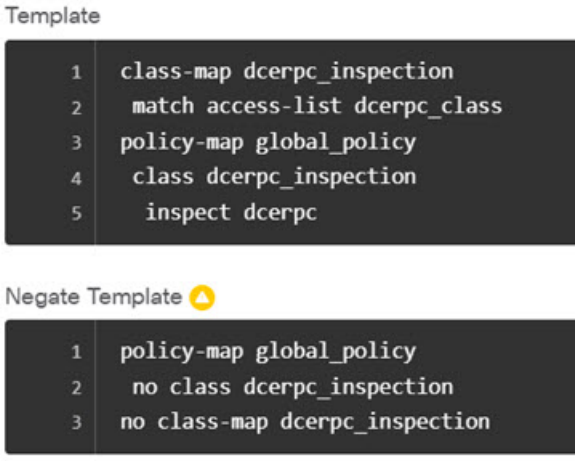
ステップ 2 これらのオブジェクトを Smart CLI 拡張アクセス リスト オブジェクトで使用します。

詳細設定



ステップ 3 名前で Smart CLI オブジェクトを示す FlexConfig オブジェクトを作成します。

たとえば、オブジェクトの名前が「dcerpc_class」の場合、FlexConfig オブジェクトは次のようになります。ネゲートテンプレートでは、Smart CLI オブジェクトから作成したアクセスリストは無効にできない点に注意してください。そのオブジェクトは、実際には FlexConfig から作成されたオブジェクトではないためです。



ステップ 4 オブジェクトを FlexConfig ポリシーに追加します。

秘密キー オブジェクトの設定

秘密キー オブジェクトのポイントは、パスワードや機密性の高い文字列を隠すことです。FlexConfig オブジェクトまたは Smart CLI テンプレートで使用される文字列を誰かに見られるリスクを避けたい場合は、文字列の秘密キー オブジェクトを作成します。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、コンテンツ テーブルから [秘密キー（Secret Keys）] を選択します。

ステップ 2 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 3 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 4 [パスワード（Password）] と [パスワードの確認（Confirm Password）] フィールドの両方にパスワードまたはその他秘密の文字列を入力します。

入力すると、システムがテキストを隠します。

ステップ 5 [OK] をクリックします。

次のタスク

- 新しいオブジェクトの場合は、FlexConfig でそれを使用するために、FlexConfig オブジェクトを編集し、秘密キーの型の変数を作成してオブジェクトを選択します。その後、オブジェクト本体内で変数を参照します。詳細については、FlexConfig オブジェクトの変数の作成 （19 ページ）を参照してください。
- FlexConfig ポリシーの一部である FlexConfig オブジェクトで使用されている既存のオブジェクトを編集する場合は、新しい文字列でデバイスを更新するために構成を展開する必要があります。
- Smart CLI テンプレートでは、コマンドに秘密キーが必要な場合、関連するプロパティを編集するときにこれらのオブジェクトの一覧が表示されます。目的にあわせて適切なキーを選択します。

FlexConfig ポリシーのトラブルシューティング

FlexConfig ポリシーを編集した後は、次の展開の結果を慎重に調べてください。[保留中の変更（Pending Changes）] ダイアログボックスに「最後の展開は失敗しました（Last Deployment Failed）」というメッセージが表示された場合は、[詳細の表示（See Details）] リンクをクリックします。リンクから監査ログが表示されます。このログで失敗した展開ジョブを確認できます。特定のエラー メッセージを検索するには、ジョブを開きます。

展開が FlexConfig の問題のため失敗した場合、詳細には不正なコマンドを含む FlexConfig オブジェクトについて記述され、失敗したコマンドが表示されます。この情報を使用して、オブジェクトを修正し、もう一度展開を試みてください。オブジェクト名はリンクであり、クリックしてオブジェクトの編集のダイアログを開きます。

たとえば、最大 TCP セグメント サイズ（TCP MSS）を設定できます。この設定は、**sysopt connection tcpmss** コマンドを使用して制御できます。Device Manager により設定する場合、このオプションに対する Threat Defense のデフォルトは 0 で、ASA のデフォルトは 1380 です。

MTU のデフォルトの 1500 を使用するインターフェイスで IPv4 VPN を実行している場合、ASA のデフォルトは処理を最適化するように設計されています。システムでは、VPN のヘッダーに 120 バイトが必要です。IPv6 の場合、システムでは 140 バイト必要です。Threat Defense のデフォルトの 0 では、エンドポイントによる MSS のネゴシエートが許可されるだけで、これは通常のトラフィック、特にデバイス上のインターフェイス間で、1500 以上の MTU を含む、異なる MTU を使用する場合には理想的な設定です。TCP の MSS はグローバル設定であり、インターフェイスごとに設定されないので、トラフィックのかなりの割合が VPN を介すものであり、過剰に断片化している場合のみ変更します。その場合は、TCP の MSS を MTU マイナス 120（IPv4 用）または 140（IPv6 用）に設定し、すべてのインターフェイスに同じ MTU を使用します。MSS を明示的に設定した場合でも、TLS/SSL 復号やサーバー検出などのコンポーネントが特定の MSS を必要とする場合、その MSS はインターフェイス MTU に基づいて設定され、MSS 設定は無視されます。

この図では、TCP の MSS を 3 バイトに設定するとします。コマンドは最小値として 48 バイトを取るので、次のような展開エラーが発生します。

エラーは、これらの要素で構成されます。

1. エラーが発生した FlexConfig オブジェクトの名前が含まれている展開エラー メッセージ。オブジェクト名は編集ダイアログ ボックスにリンクされているので、オブジェクトを開いてすぐにエラーを修正できます。これはメッセージの最初の文です。
2. 「ERROR:」から始まるテキストがデバイスから返されるメッセージです。これは SSH クライアントの書式なしで、誤ったコマンドで入力した場合の、ASA の正確な応答内容です。この例では、エラー メッセージは「エラー：[3] は RFC 791 で 許可されている MSS

の最小値 48 よりも小さいです。（ERROR: [3] is smaller than the minimum allowed MSS of 48 by RFC 791.）」です。「Config Error」で始まるテキストが、エラー メッセージを生成した特定の行を示しています。

3. 黒のテキストは、エラーを引き起こした FlexConfig オブジェクトからの実際の行です。この行を修正する必要があります。この例では、MTU 1500 インターフェイス（共通の状態）上の IPv4 VPN トラフィックに対応しようとする場合、3 を 1380 に変更します。

   この例を修正する場合、CLI コンソールを開いたままにし、**show running-config all sysopt** を使用して、**sysopt** コマンドのすべての設定を確認できます。ほとんどの **sysopt** コマンドには大部分の用途に適したデフォルトの設定があり、実行コンフィギュレーションには表示されません。**all** キーワードでは、出力にこれらのデフォルト設定が含まれます。

FlexConfig の例

ここでは、FlexConfig を使用して機能を設定するいくつかの例を示します。

グローバル デフォルト インスペクションを有効/無効にする方法

一部のプロトコルでは、IP アドレッシング情報がユーザ データ パケットに埋め込まれるか、動的に割り当てられたポートにセカンダリ チャネルが開かれます。そのようなプロトコルの場合、システムはディープ パケット インスペクションを実行し、NAT を適用して、セカンダリ チャネルを許可できるようにする必要があります。いくつかの一般的なインスペクション エンジンはデフォルトで有効になっていますが、ネットワークによっては、他のインスペクション エンジンを有効化したり、デフォルトのインスペクションを無効化したりする必要があります。

現在有効になっているインスペクションの一覧を表示するには、CLI コンソールまたは SSH セッションで **show running-config policy-map** コマンドを使用します。以下の出力は、インスペクションの設定に変更が加えられていないシステムで表示される内容です。この出力では、出力の最後にある **inspect** コマンドの一覧に有効になっているプロトコルインスペクションが表示されています。先行するコマンドにより、inspection_default トラフィック クラスでこれらのインスペクションが有効になります（通常のプロトコル、該当する場合はインスペクション済みプロトコルのポート番号）。このクラスは global_policy ポリシー マップの一部で、service-policy コマンド（出力には未表示）を使用して、すべてのインターフェイスに対するインスペクションに適用されます。たとえば、ICMP インスペクションは、デバイスを通過するすべての ICMP トラフィックに対して行われます。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
```

詳細設定

```
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
!
```

（注） 各インスペクションの詳細については、https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html で入手可能な『*Cisco ASA Series Firewall Configuration Guide*』を参照してください。

次の手順では、このグローバルに適用されるデフォルト インスペクション クラスのインスペクションを有効化または無効化する方法を示します。説明のための例：

- PPTP（Point-to-Point Tunneling Protocol）を有効にします。このプロトコルは、エンドポイント間のポイントツーポイント接続のトンネリングに使用されます。
- SIP（Session Initiation Protocol）を無効にします。通常は、インスペクションによってネットワークに問題が発生している場合にのみSIPを無効化します。SIPを無効化する場合は、アクセス コントロール ポリシーで SIP トラフィック（UDP/TCP 5060）と動的に割り当てられるポートが許可されていること、SIP接続にNATのサポートが必要ないことを確認します。アクセス コントロール ポリシーと NAT ポリシーを、FlexConfig ではなく、標準のページを使用して適宜調整します。

始める前に

適切な計画を立てることでFlexConfigを効率的に使用できます。この例では、同じトラフィック クラスに変更を加えていますが、2つの異なる関連性のないインスペクションを変更しています。ただし、それらのポリシーを変更する必要がある場合（可能性は高い）は、個別に変更します。

そのため、この例のインスペクションごとに個別のFlexConfigオブジェクトを作成することをお勧めします。そうすることで、他のインスペクションを変更することなく、1 つのインスペクションの設定を簡単に変更でき、FlexConfig オブジェクトを編集する必要もありません。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

ステップ 3 PPTP インスペクションを有効にするオブジェクトを作成します。

a) 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

b) オブジェクトの名前を入力します。例、**Enable_PPTP_Global_Inspection**。

c) [テンプレート（Template）] エディタで、インデントを含む次の行を入力します。

```
policy-map global_policy
 class inspection_default
  inspect pptp
```

d) [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

適切なサブモードでコマンドを有効にするために、ネゲートテンプレートに、親コマンドと同様にこれらのコマンドも含める必要があります。

FlexConfig ポリシーからこのオブジェクトを削除した場合（正常に導入された後）、および導入が失敗した場合でも（設定を前の状態にリセットするため）、ネゲートテンプレートが適用されます。

したがって、この例では、ネゲート テンプレートは次のようになります。

```
policy-map global_policy
 class inspection_default
  no inspect pptp
```

オブジェクトは次のようになります。

詳細設定

（注） Iinspection_default クラスには有効になっているその他のインスペクション コマンドがあるため、クラス全体を無効にはしたくありません。同様に、global_policy ポリシーマップにはその他のインスペクションが含まれているため、ポリシーマップも無効にはしたくありません。

e) [OK] をクリックしてオブジェクトを保存します。

ステップ 4 SIP 検査を無効にするオブジェクトを作成します。

a) 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

b) オブジェクトの名前を入力します。例、**Disable_SIP_Global_Inspection**。

c) [テンプレート（Template）] エディタで、インデントを含む次の行を入力します。

```
policy-map global_policy
 class inspection_default
  no inspect sip
```

d) [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

「no」コマンドを無効化するための「negate」コマンドは、機能を有効化するコマンドです。そのため、「ネゲート」テンプレートは機能を無効化するためだけのコマンドではな

く、「ポジティブ」テンプレートでの操作を元に戻すためのコマンドです。ネゲートテンプレートの要点は、変更を元に戻す点にあります。

したがって、この例では、ネゲート テンプレートは次のようになります。

```
policy-map global_policy
 class inspection_default
  inspect sip
```

オブジェクトは次のようになります。

e) [OK] をクリックしてオブジェクトを保存します。

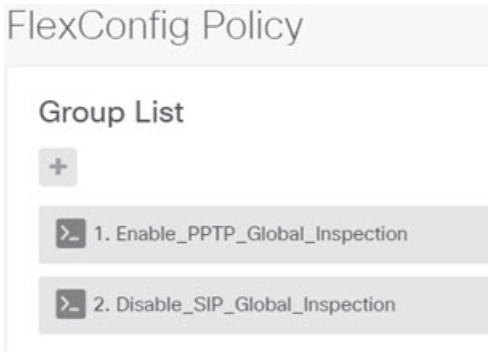
ステップ 5 オブジェクトを FlexConfig ポリシーに追加します。

オブジェクトを作成するだけでは不十分です。オブジェクトは、FlexConfig ポリシーに追加（および変更を保存）した場合にのみ展開されます。これにより、未終了の作業で展開が失敗するリスクを犯すことなく、オブジェクトを試す（および部分的に完了した状態で残す）ことができます。その後、オブジェクトを追加および削除することで、機能を簡単にオン/オフできます。オブジェクトを毎回再作成する必要はありません。

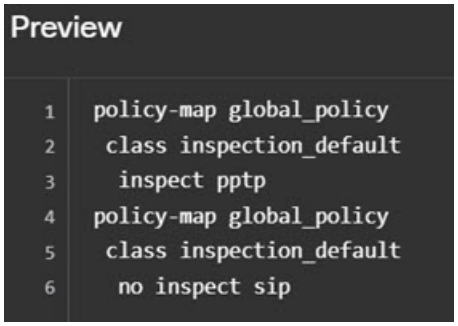
a) 目次で [FlexConfigポリシー（FlexConfig Policy）] をクリックします。
b) [グループリスト（Group List）] で [+] をクリックします。

c) Enable_PPTP_Global_Inspection オブジェクトと Disable_SIP_Global_Inspection オブジェクトを選択して、[OK] をクリックします。

グループ リストは次のようになります。



プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。



d) [保存（Save）] をクリックします。

これでポリシーを展開できます。

ステップ 6 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ 7 CLI コンソールまたは SSH セッションで、**show running-config policy-map** コマンドを使用し、実行コンフィギュレーションが正しく変更されているか確認します。

次の出力では、**inspect pptp** が inspection_default クラスの最後に追加されていて、**inspect sip** はクラスに含まれていないことに注意してください。これにより、FlexConfig オブジェクトで定義された変更が正常に導入されたことが確認されます

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
!
```

FlexConfig の変更を元に戻す方法

FlexConfig オブジェクトに正しいネゲートテンプレートを入力すると、そのオブジェクトを使用して行った変更の削除が容易になります。FlexConfig ポリシーから単純にオブジェクトを削除すると、次の展開時に、システムがネゲートテンプレートを使用して変更を元に戻します。

変更を元に戻すために新しいオブジェクトを作成する必要はありません。

次の例は、グローバルな SIP 検査を再度有効にする方法を示しています。この例では、SIP 検査を無効化しているグローバルデフォルトインスペクションを有効/無効にする方法（30ページ）で説明した変更を元に戻しています。

始める前に

FlexConfig オブジェクトにネゲートテンプレートが正しく設定されていることを確認します。正しくない場合は、オブジェクトを編集してネゲート テンプレートを修正します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigポリシー（FlexConfig Policy）]** をクリックします。

ステップ 3 FlexConfig ポリシーの **Disable_SIP_Global_Inspection** オブジェクトのエントリの右側にある [X] をクリックして、ポリシーから削除します。

オブジェクトのコマンドは、プレビューから削除されます。negate コマンドはプレビューには追加されず、バックグラウンドで実行されます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ 6 CLI コンソールまたは SSH セッションで、**show running-config policy-map** コマンドを使用し、実行コンフィギュレーションが正しく変更されているか確認します。

次の出力では、**inspect sip** が inspection_default クラスの一番下に追加されていることに注意してください。これにより、FlexConfig オブジェクトで定義された変更が正常に導入されたことが確認されます（このクラスでは順序は重要ではないため、**inspect sip** が最後にあり、元の場所になくても問題ありません）。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
  inspect sip
```

!

一意のトラフィック クラスのインスペクションを有効にする方法

この例では、特定のインターフェイスの 2 つのエンドポイント間でトラフィックの PPTP インスペクションを有効にします。これは、エンドポイント間にポイントツーポイント トンネルが設定されているエンドポイントのインスペクションだけをターゲットにします。

2 つのエンドポイント間で PPTP インスペクションを有効にするために必要な CLI には、以下の内容が含まれます。

1. 送信元と宛先がエンドポイントのホストの IP アドレスに設定されている ACL。
2. この ACL を参照するトラフィック クラス。
3. トラフィック クラスを含み、そのトラフィック クラスでの PPTP インスペクションを有効にするポリシー マップ。
4. 目的のインターフェイスにポリシー マップを適用するサービス ポリシー。これは、実際にポリシーをアクティブにして、インスペクションを有効にする手順です。

（注） インスペクション関連のサービス ポリシーの詳細については、https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html で入手可能な『*Cisco ASA Series Firewall Configuration Guide*』を参照してください。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 詳細設定の目次で **[FlexConfig]** > **[FlexConfigオブジェクト（FlexConfig Objects）]** をクリックします。

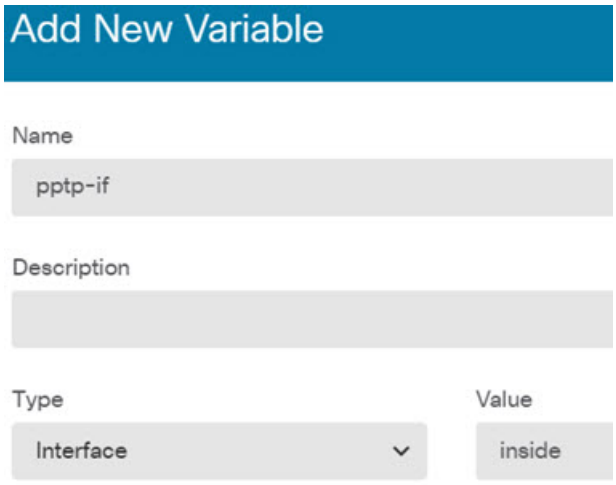
ステップ 3 新しいオブジェクトを作成するには、[+] ボタンをクリックします。

ステップ 4 オブジェクトの名前を入力します。例、[Enable_PPTP_Inspection_on_Interface]。

ステップ 5 内部インターフェイスの変数を追加します。

a) [変数（Variables）] リストの上にある [+] をクリックします。
b) 変数の名前、[pptp-if] などを入力します。
c) [種類（Type）] で [インターフェイス（Interface）] を選択します。
d) [値（Value）] で [内部（inside）] インターフェイスを選択します。

ダイアログボックスは次のようになります。



e) [追加（Add）] をクリックします。

ステップ 6 [テンプレート（Template）] エディタで、インデントを含む次の行を入力します。

```
access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
class-map MATCH_CMAP
 match access-list MATCH_ACL
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
service-policy PPTP_POLICY interface {{pptp-if.name}}
```

変数を使用するには、二重ブレースの間に変数名を入力する点に注意してください。また、インターフェイスを定義するオブジェクトには多数の属性が設定されているため、取得する属性を選択するにはドット表記法を使用する必要があります。インターフェイス名は「name」属性に保持されるため、[{{pptp-if.name}}] を入力すると、変数に割り当てられているインターフェイスの name 属性の値が取得されます。PPTP インスペクションのインターフェイスを変更する必要がある場合は、変数定義で単純に別のインターフェイスを選択する必要があります。

ステップ 7 [ネゲートテンプレート（Negate Template）] エディタで、この設定を元に戻すために必要な行を入力します。

この例では、クラス マップ、ポリシー マップ、およびサービス ポリシーは、PPTP インスペクションを適用するためにのみ存在していると仮定しています。したがって、ネゲートテンプレートでこれらをすべて削除します。

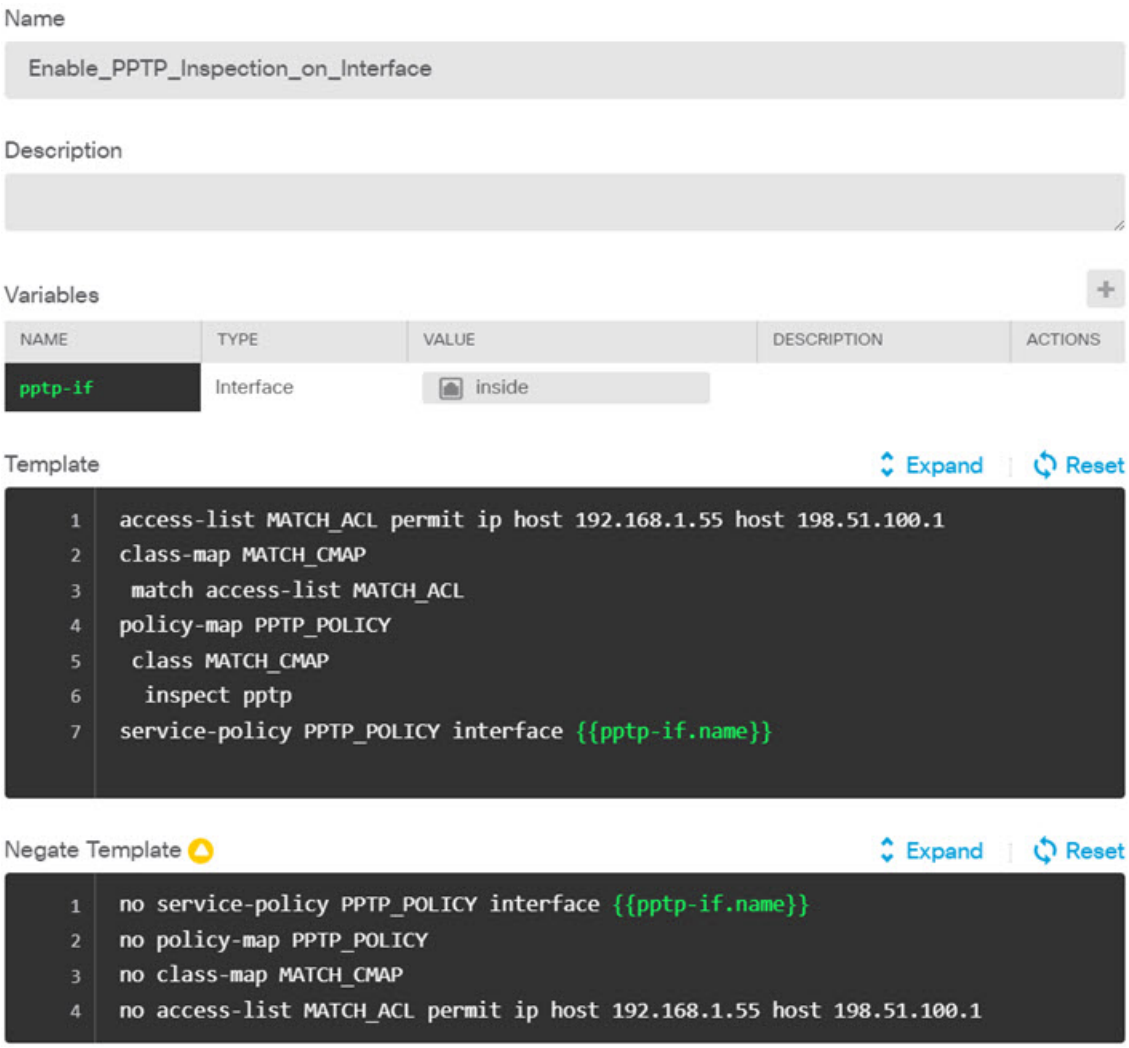
ただし、インターフェイスの既存のサービス ポリシーに PPTP インスペクションを実際に追加する場合は、ポリシー マップやサービス ポリシーを無効にはしません。ポリシー マップからクラスを無効にするか、またはポリシーマップ内のクラス内でインスペクションを単純にオフにします。ネゲート テンプレートで予期せぬ結果が生じないようにするには、その他の FlexConfig オブジェクトに実装している内容について明確に把握する必要があります。

ネストされた項目を削除する場合は、作成順とは逆の順番で削除する必要があります。したがって、最初にサービス ポリシーを削除して、最後にアクセス リストを削除します。そうし

ないと、使用中のオブジェクトを削除しようとして、システムからエラーが返され、削除できなくなります。

```
no service-policy PPTP_POLICY interface {{pptp-if.name}}
no policy-map PPTP_POLICY
no class-map MATCH_CMAP
no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```

オブジェクトは次のようになります。



ステップ 8 [OK] をクリックしてオブジェクトを保存します。

ステップ 9 オブジェクトを FlexConfig ポリシーに追加します。

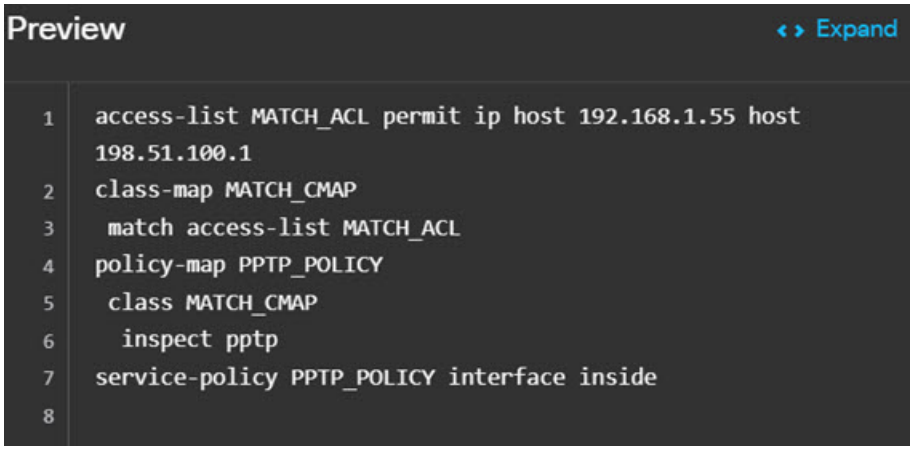
a) 目次で [FlexConfigポリシー（FlexConfig Policy）] をクリックします。

b) [グループリスト（Group List）] で [+] をクリックします。

c) [Enable_PPTP_Inspection_on_Interface] オブジェクトを選択し、[OK] をクリックします。

グループ リストは次のようになります。

プレビューはテンプレートのコマンドで更新されます。次の図に示されているように、予想していたコマンドが表示されていることを確認します。プレビューでは、インターフェイス変数は名前「inside」に解決されることに注意してください。変数には特に注意してください。プレビューで正しく解決されていない場合、変数は正確に展開されません。プレビューで変数が正しく変換されるまで、FlexConfig オブジェクトを編集します。



d) [保存（Save）] をクリックします。

これでポリシーを展開できます。

ステップ 10 変更を保存します。

a) Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

b) [今すぐ展開（Deploy Now）] ボタンをクリックします。

展開が完了するまで待機するか、[OK] をクリックして、後でタスク リストまたは展開履歴を確認します。

ステップ 11 CLI コンソールまたは SSH セッションで **show running-config** コマンドのバリエーションを使用して、実行コンフィギュレーションに正しい変更が含まれていることを確認します。

show running-config を入力して CLI の設定全体を検査したり、以下のコマンドを使用して、この設定の各部分を確認したりすることができます。

- **show running-config access-list MATCH_ACL** （ACL の確認用）。

- **show running-config class**（クラスマップの確認用）。すべてのクラス マップが表示されます。
- **show running-config policy-map PPTP_POLICY**（クラスおよびポリシーマップ設定の確認用）。
- **show running-config service-policy**（インターフェイスに適用されているポリシーマップの確認用）。すべてのサービス ポリシーが表示されます。

次の出力には、この一連のコマンドが表示されており、設定が正しく適用されていることを確認できます。

```
> show running-config access-list MATCH_ACL
access-list MATCH_ACL extended permit ip host 192.168.1.55 host 198.51.100.1

> show running-config class
!
class-map MATCH_CMAP
 match access-list MATCH_ACL
class-map inspection_default
 match default-inspection-traffic
!

> show running-config policy-map PPTP_POLICY
!
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
!
> show running-config service-policy
service-policy global_policy global
service-policy PPTP_POLICY interface inside
```

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