



高度なインターフェイス設定

この章では、インターフェイスのMACアドレスを設定する方法、最大伝送ユニット (MTU) を設定する方法、TCP 最大セグメントサイズ (TCP MSS) を設定する方法、および同じセキュリティ レベルの通信を許可する方法について説明します。最高のネットワーク パフォーマンスを実現するには、正しい MTU と最大 TCP セグメント サイズの設定が不可欠です。

- [高度なインターフェイス設定について \(1 ページ\)](#)
- [MAC アドレスの手動設定 \(7 ページ\)](#)
- [マルチ コンテキスト モードでの MAC アドレスの自動割り当て \(9 ページ\)](#)
- [MTU および TCP MSS の設定 \(10 ページ\)](#)
- [同一のセキュリティ レベル通信の許可 \(11 ページ\)](#)
- [インターフェイスの詳細設定の履歴 \(12 ページ\)](#)

高度なインターフェイス設定について

この項では、インターフェイスの高度な設定について説明します。

MAC アドレスについて

手動で MAC アドレスを割り当ててデフォルトをオーバーライドできます。マルチコンテキストモードでは、(コンテキストに割り当てられているすべてのインターフェイスの) 一意の MAC アドレスと。



- (注) 親インターフェイスの同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

デフォルトの MAC アドレス

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは、Burned-in MAC Address を使用します。
- 冗長インターフェイス：冗長インターフェイスでは、最初に追加された物理インターフェイスの MAC アドレスが使用されます。構成でメンバーインターフェイスの順序を変更すると、MAC アドレスがリストの先頭にあるインターフェイスの MAC アドレスと一致するように変更されます。冗長インターフェイスに MAC アドレスを割り当てると、メンバーインターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。
- EtherChannel (Firepower Models)：EtherChannel の場合は、そのチャンネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワークアプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないからです。ポートチャンネルインターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。
- EtherChannel (ASA モデル)：ポートチャンネルインターフェイスは、最も小さいチャンネルグループインターフェイスの MAC アドレスをポートチャンネル MAC アドレスとして使用します。または、ポートチャンネルインターフェイスの MAC アドレスを設定することもできます。グループチャンネルインターフェイスのメンバーシップが変更された場合に備えて、一意の MAC アドレスを設定することを推奨します。ポートチャンネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャンネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。
- サブインターフェイス：物理インターフェイスのすべてのサブインターフェイスが同じ組み込みの MAC アドレスを使用します。サブインターフェイスに一意の MAC アドレスを割り当てる必要がある場合があります。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセスコントロールを実行する場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。
- ASASM VLAN：ASASM では、すべての VLAN がバックプレーンから提供される同じ MAC アドレスを使用します。

自動 MAC アドレス

マルチ コンテキスト モードでは、自動生成によって一意の MAC アドレスがコンテキストに割り当てられているすべてのインターフェイスに割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成がイネーブルになっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます（有効になっている場合）。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

ASA は、次の形式を使用して MAC アドレスを生成します。

A2xx.yyzz.zzzz

xx.yy はユーザ定義プレフィックスまたはインターフェイス MAC アドレスの最後の 2 バイトに基づいて自動生成されたプレフィックス、zz.zzzz は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、ASA は 77 を 16 進数値 004D (yyxx) に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆にされます (xxyy)。

A24D.00zz.zzzz

プレフィックス 1009 (03F1) の場合、MAC アドレスは次のようになります。

A2F1.03zz.zzzz



(注) プレフィックスのない MAC アドレス形式は従来のバージョンです。従来の形式に関する詳細については、コマンドリファレンスの **mac-address auto** コマンドを参照してください。

MTU について

MTU は、ASA が特定のイーサネットインターフェイスで送信する最大フレームペイロードサイズを指定します。MTU の値は、イーサネットヘッダー、VLAN タギング、他のオーバーヘッドを含まないフレームサイズです。たとえば、MTU を 1500 に設定すると、予想されるフレームサイズは、ヘッダーを含めて 1518 バイトです。または、VLAN を使用している場合は、1522 バイトです。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

VXLAN については、イーサネット データグラム全体がカプセル化されるため、新しい IP パケットにより大きな MTU が必要です。ASA VTEP 送信元インターフェイスの MTU を 54 バイト以上のネットワーク MTU に設定する必要があります。

Path MTU Discovery

ASA は、Path MTU Discovery (RFC 1191 の定義に従う) をサポートします。つまり、2 台のホスト間のネットワークパス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

デフォルト MTU

ASA のデフォルト MTU は、1500 バイトです。この値には、イーサネット ヘッダー、VLAN タギングや他のオーバーヘッドのための 18~22 バイト以上は含まれません。

VTEP 送信元インターフェイスの VXLAN を有効にし、MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。この場合、イーサネット データグラム全体がカプセル化されるため、新しいパケットにはより大きな MTU が必要です。一般的には、ASA ソースインターフェイス MTU をネットワーク MTU + 54 バイトに設定する必要があります。

MTU とフラグメンテーション

IPv4 では、出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは送信先（場合によっては中継先）で組立て直されますが、フラグメント化はパフォーマンス低下の原因となります。IPv6 では、通常、パケットはフラグメント化を許可されていません。したがってフラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

TCP パケットでは、通常、エンドポイントは MTU を使用して TCP の最大セグメント サイズ（たとえば、MTU - 40）を判別します。途中で追加の TCP ヘッダーが追加された場合（たとえば、サイト間 VPN トンネル）、TCP MSS はトンネリング エンティティで下方調整しないといけない場合があります。TCP MSS について (5 ページ) を参照してください。

UDP または ICMP では、フラグメンテーションを回避するために、アプリケーションは MTU を考慮する必要があります。



(注) ASA はメモリに空きがある限り、設定された MTU よりも大きいフレームを受信できます。

MTU とジャンボ フレーム

より大きな MTU は、より大きなパケットの送信が可能です。より大きなパケットは、ネットワークにとってより効率的な場合があります。次のガイドラインを参照してください。

- トラフィック パスの MTU の一致：すべての ASA インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボ フレームに対応する：ジャンボ フレームを有効にすると、MTU を最大 9198 バイトに設定できます。最大値は、Firepower 4100/9300 シャーシの ASA v で 9000、ASA で 9184 です。



(注) ASA 5585-X では、VLAN タギングを使用している場合、最大 MTU は 4 バイト小さくなります (9194)。

TCP MSS について

最大セグメントサイズ (TCP MSS) とは、あらゆる TCP および IP ヘッダーが追加される前の TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイ ハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

(を参照) ASA で TCP MSS を通過トラフィック用に設定できます。デフォルトでは、最大 TCP MSS は 1380 バイトに設定されます。この設定は、ASA が IPsec VPN カプセル化の packetsize を追加する必要がある場合に役立ちます。ただし、非 IPsec エンドポイントでは、ASA の最大 TCP MSS を無効にする必要があります。

最大 TCP MSS を設定している場合、接続のいずれかのエンドポイントが ASA に設定された値を超える TCP MSS を要求すると、ASA は要求パケット内の TCP MSS を ASA の最大サイズで書き換えます。ホストまたはサーバが TCP MSS を要求しない場合、ASA は RFC 793 のデフォルト値 536 バイト (IPv4) または 1220 バイト (IPv6) を想定しますが、パケットは変更しません。たとえば、MTU をデフォルトの 1500 バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。ASA の最大 TCP MSS が 1380 (デフォルト) の場合は、ASA は TCP 要求パケットの MSS 値を 1380 に変更します。その後、サーバは、1380 バイトのペイロードを含むパケットを送信します。ASA は、最大 120 バイトのヘッダーをパケットに追加しても、1500 バイトの MTU サイズに適応することができます。

TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、ASA は値を調整します。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN 接続用を含め、to-the-box トラフィックの場合、この設定は適用されません。ASA は MTU を使用して、TCP MSS を導き出します。MTU - 40 (IPv4) または MTU - 60 (IPv6) となります。

デフォルト TCP MSS

デフォルトでは、ASA の最大 TCP MSS は 1380 バイトです。このデフォルトは、ヘッダーが最大 120 バイトの IPv4 IPsec VPN 接続に対応しています。この値は、MTU のデフォルトの 1500 バイト内にも収まっています。

TCP MSS の推奨最大設定

デフォルトでは TCP MSS は、ASA が IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。ASA が IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして ASA を使用しない場合は、FlexConfig の Sysopt_Basic オブジェクトを使用して TCP MSS 設定を参照してください。次のガイドラインを参照してください。

- 通常のトラフィック：TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。通常、接続エンドポイントは MTU から TCP MSS を取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。

- IPv4 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。
- IPv6 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 140 に設定します。

インターフェイス間通信

同じセキュリティ レベルのインターフェイスで相互通信を許可する利点としては、次のものがあります。

- 101 より多い数の通信インターフェイスを設定できます。
各インターフェイスで異なるセキュリティ レベルを使用したときに、同一のセキュリティ レベルにインターフェイスを割り当てないと、各レベル（0～100）に1つのインターフェイスしか設定できません。
- ACL がなくても同じセキュリティ レベルのインターフェイスすべての中で自由にトラフィックが流れるようにできます。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

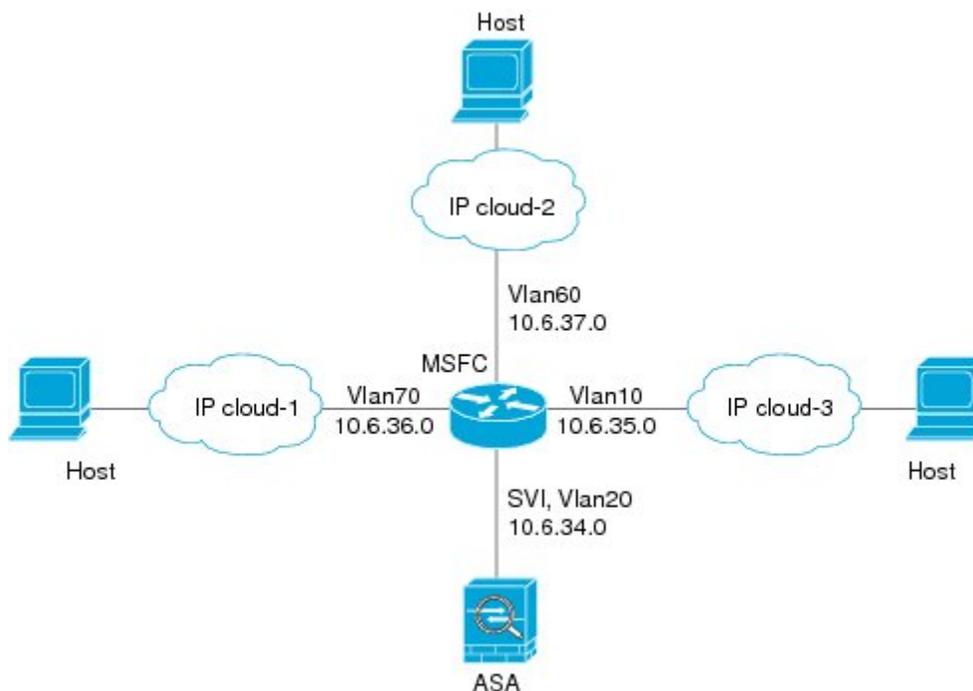
インターフェイス内通信（ルーテッド ファイアウォール モード）

インターフェイス内通信は、インターフェイスに入ってくる VPN トラフィックに対して使用できますが、その場合は同じインターフェイスのルートから外されます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブアンドスポーク VPN ネットワークがあり、ASA がハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックは ASA に入ってから他のスポークに再度ルーティングされる必要があります。



- (注) この機能で許可されたすべてのトラフィックは、引き続きファイアウォール規則に従います。リターン トラフィックが ASA を通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

ASASM の場合、この機能をイネーブルにするには、まず、パケットがスイッチ経由で宛先ホストに直接送信されるのではなく、ASA の MAC アドレスに送信されるように、MSFC を正しく設定する必要があります。次の図に、同一インターフェイス上のホストが通信する必要があるネットワークを示します。



次の設定例では、次の図に示すネットワークのポリシールーティングをイネーブルにするために使用される Cisco IOS **route-map** コマンドを示します。

```
route-map intra-inter3 permit 0
  match ip address 103
  set interface Vlan20
  set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
  match ip address 102
  set interface Vlan20
  set ip next-hop 10.6.34.7
!
route-map intra-inter1 permit 10
  match ip address 101
  set interface Vlan20
  set ip next-hop 10.6.34.7
```

MAC アドレスの手動設定

MAC アドレスを手動で割り当てる必要がある場合は、この手順を使用して実行できます。

親インターフェイスの同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカ

ルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context name** コマンドを入力します。

手順

ステップ 1 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。

interface id

例 :

```
ciscoasa(config)# interface gigabithernet 0/0
```

ステップ 2 プライベート MAC アドレスをこのインターフェイスに割り当てます。

mac-address mac_address [standby mac_address]

例 :

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

mac_address は、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。MAC アドレスはマルチキャストビットセットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

フェールオーバーで使用する場合は、**スタンバイ** MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

マルチ コンテキスト モードでの MAC アドレスの自動割り当て

この項では、MAC アドレスの自動生成の設定方法について説明します。マルチ コンテキスト モードの場合、この機能によって、コンテキストに割り当てられたすべてのインターフェイス タイプに一意的な MAC アドレスが割り当てられます。

始める前に

- インターフェイスの **nameif** コマンドを設定すると、ただちに新規 MAC アドレスが生成されます。インターフェイスを設定した後でこの機能をイネーブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。
- 生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

プライベート MAC アドレスを各インターフェイスに自動的に割り当てます。

mac-address auto [prefix prefix]

プレフィックスを入力しない場合は、ASA によって、インターフェイス MAC アドレスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

手動でプレフィックスを入力する場合は、*prefix* に 0 ～ 65535 の 10 進数値を指定します。このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。

例：

```
ciscoasa(config)# mac-address auto prefix 19
```

MTUおよびTCP MSSの設定

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context name** コマンドを入力します。
- MTU を 1500 より多く増やすには、[ジャンボ フレーム サポートの有効化](#)に従って、ジャンボフレームをイネーブルにします。ジャンボフレームはデフォルトでASASMでサポートされるため、この機能をイネーブルにする必要はありません。

手順

ステップ1 MTU を 300 ~ 9198 (ASA の場合は 9000、Firepower 4100/9300 シャーシ の場合は 9184) バイトの範囲で設定します

mtu interface_name bytes

例 :

```
ciscoasa(config)# mtu inside 9000
```

デフォルトは 1500 バイトです。

- (注) 冗長インターフェイスまたはポートチャネル インターフェイスに MTU を設定すると、ASA は、この設定をすべてのメンバー インターフェイスに適用します。

ジャンボ フレームをサポートする多くのモデルでは、インターフェイスに 1500 よりも大きな値を入力する場合、ジャンボフレームのサポートをイネーブルにする必要があります。「[ジャンボ フレーム サポートの有効化](#)」を参照してください。

- (注) VLAN タギングを使用する場合、ASA 5585-X の最大値は 4 バイト少なくなります。したがって、になります。ASA ではMTUの値を9195 ~ 9198に設定できますが、実際のペイロードのサイズは9194になります。

ステップ2 最大 TCP セグメント サイズをバイト単位で設定します (48 ~ 任意の最大値)。

sysopt connection tcpmss [minimum] bytes

例 :

```
ciscoasa(config)# sysopt connection tcpmss 8500
ciscoasa(config)# sysopt connection tcpmss minimum 1290
```

デフォルト値は1380バイトです。この機能は、0バイトに設定することによってディセーブルにできます。

minimal キーワードには、48 ～ 65535 の間のバイト数未満にならないように最大セグメントサイズを設定します。**minimum** 機能は、デフォルトでディセーブルです (0 に設定)。

ステップ 3 [ASA Cluster] 設定については、[マスターユニットでのインターフェイスの設定](#)を参照してください。

例

下記の例では、ジャンボフレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、非 VPN トラフィックの TCP MSS をディセーブルにします (TCP MSS を 0 に設定、すなわち無制限とすることによって行います)。

```
jumbo frame-reservation
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 0
```

下記の例では、ジャンボフレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、VPN トラフィックの TCP MSS を 9078 に変更します (MTU から 120 を差し引きます)。

```
jumbo frame-reservation
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 9078
```

同一のセキュリティ レベル通信の許可

デフォルトでは、同じセキュリティレベルのインターフェイスは相互に通信することができません。また、パケットは同じインターフェイスを出入りすることができません。この項では、複数のインターフェイスが同じセキュリティレベルの場合にインターフェイス間通信をイネーブルにする方法と、インターフェイス内通信をイネーブルにする方法について説明します。

手順

ステップ 1 相互通信を可能にするために同じセキュリティレベルのインターフェイスをイネーブルにします。

same-security-traffic permit inter-interface

ステップ 2 同じインターフェイスに接続されたホスト間の通信をイネーブルにします。

same-security-traffic permit intra-interface

インターフェイスの詳細設定の履歴

表 1: インターフェイスの詳細設定の履歴

機能名	リリース	機能情報
最大 MTU が 9198 バイトになりました	9.1(6)、9.2(1)	ASA で使用できる最大の MTU は 9198 バイトです (CLI のヘルプでご使用のモデルの正確な最大値を確認してください)。この値にはレイヤ 2 ヘッダーは含まれません。以前は、ASA で 65535 バイトの最大 MTU を指定できましたが、これは不正確であり、問題が発生する可能性があります。9198 よりも大きいサイズに MTU を設定している場合は、アップグレード時に MTU のサイズが自動的に削減されます。場合によっては、この MTU の変更により MTU の不一致が発生する可能性があります。接続している機器が新しい MTU 値を使用するように設定されていることを確認してください。 次のコマンドが変更されました。 mtu
Firepower 4100/9300 シャーシの ASA の MTU サイズ増加	9.6(2)	Firepower 4100 および 9300 で、最大 MTU を 9184 バイトに設定できます。これまでは 9000 バイトが最大でした。この MTU は FXOS 2.0.1.68 以降でサポートされます。 次のコマンドが変更されました。 mtu