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。

インターフェイスの詳細設定について

ここでは、インターフェイスの詳細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、デフォルトを上書きすることができます。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（サブインターフェイスの）シングルコンテキストモードを自動的に生成できます。.

（注） 親インターフェイスと同じ組み込みの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制御を行う場合があります。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 デバイスで特定のインスタンスでのトラフィックの中断を回避できます。

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では、Burned-In MAC Address を使用します。
- VLAN インターフェイス（Firepower 1010 および Secure Firewall 1210/1220）：ルーテッド ファイアウォール モード：すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。を参照してくださいMAC アドレスの手動設定 （6 ページ）。

  トランスペアレント ファイアウォール モード：各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。を参照してくださいMAC アドレスの手動設定 （6 ページ）。
- EtherChannel（Firepower モデル）：EtherChannel の場合、そのチャ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透過的になります。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。ポートチャネルインターフェイスは、プールにある一意の MAC アドレスを使用します。インターフェイス メンバーシップは MAC アドレスに影響しません。
- EtherChannel（ASA モデル）：ポートチャネルインターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポートチャネル MAC アドレスとして使用します。または、ポートチャ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お勧めします。ポートチャネル 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は同じ Burned-In MAC Address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ことが必要になる場合があります。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制御を行う場合があります。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。

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、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に一意のMACアドレスが割り当てられます。

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。

A2*xx.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であり、*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としてたとえば、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転されます（*xxyy*）。

A2**4D.00***zz.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。

A2**F1.03***zz.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可能な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、またはその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、VLAN を使用する場合は 1522 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 または Geneve 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 パケットは大きくなり、より大きな MTU が必要となります。そのため、ASA VTEP 送信元インターフェイスの MTU をネットワーク MTU + 54 バイト（VXLAN）、または + 306 バイト（Geneve）に設定する必要があります。

パス MTU ディスカバリ

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分の 18～22 バイトは含まれません。

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、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。一般的には、ASA 送信元インターフェイス 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 の場合、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。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 の場合、通常、パケットのフラグメント化は許可されません。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 サイズ以内におさめる必要があります。

TCP パケットの場合、通常、エンドポイントが MTU を使用して、TCP 最大セグメント サイズ（たとえば、MTU - 40 など）を判別します。途中で TCP ヘッダーが追加される場合（たとえば、サイト間 VPN トンネルなど）、トンネリング エンティティによって TCP MSS を調整する必要があります。TCP MSS について （5 ページ）を参照してください。

UDP または ICMP の場合、アプリケーションは、フラグメンテーションを避けるために、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します。

MTU とジャンボ フレーム

MTU が大きくなると、より大きなパケットを送信できます。大きなパケットはネットワークにとってより効率的です。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 インターフェイスの MTU と、トラフィック パス上のその他のデバイス インターフェイスの MTU を同じ値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 フレームへの対応：ジャンボ フレームが有効な場合、MTU を 9,000 バイト以上に設定できます。最大値はモデルによって異なります。

TCP MSS について

TCP 最大セグメント サイズ（MSS）とは、あらゆる TCP と 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。

」を参照してください。デフォルトで、最大 TCP MSS は 1,380 バイトに設定されます。この設定は、ASA が IPsec VPN カプセル化のパケットサイズを大きく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 を無効化する必要があります。

最大 TCP MSS を設定すると、接続のいずれかのエンドポイントが ASA で設定した値よりも大きな TCP MSS を要求した場合に、ASA は要求パケットの TCP MSS を ASA の最大値で上書きします。ホストやサーバが 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、パケットを変更することはありません。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。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 はさらに 120 バイトのヘッダーをパケットに追加しますが、それでも 1500 の MTU サイズに収まります。

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 接続用を含む to-the-box トラフィックには、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、。

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。一般に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間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。

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と同じ組み込みの 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制御を行う場合があります。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 gigabithethernet 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。

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

タイプに一意の MAC アドレスが割り当てられます。 シングル モードでは、この機能によって、VLAN サブインターフェイスに一意の 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（ASA 仮想、ISA 3000）に従って、ジャンボ フレームをイネーブルにします。

手順

ステップ 1 MTU を設定します。最小値と最大値は、プラットフォームによって異なります。

mtu *interface_name bytes*

例：

```
ciscoasa(config-if)# mtu inside ?

configure mode commands/options:
  <64-9198>  MTU bytes
ciscoasa(config)# mtu inside 9000
```

デフォルトは 1500 バイトです。

（注）
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一部のモデルでは、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（ASA 仮想、ISA 3000） を参照してください。

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**] バイト

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無効にできます。

minimum キーワードには、48 ～ 65535 の間で *bytes* の値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 未処理 TCP セグメントの最大数を設定します。

sysopt connection tcp-max-unprocessed-seg *unprocessed segments*

例：

```
ciscoasa(config)# sysopt connection tcp-max-unprocessed-seg 7
```

デフォルト値は、6 です。範囲は 6 ～ 24 です。

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）。

```
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）。

```
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した。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**
シングル コンテキスト モード用の一意の MAC アドレス生成	9.8(3), 9.8(4), 9.9(2)	シングル コンテキスト モードで VLAN サブインターフェイスの一意の MAC アドレス生成を有効にできるようになりました。通常、サブインターフェイスはメインインターフェイスと同じ MAC アドレスを共有します。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、この機能により一意の IPv6 リンクローカル アドレスが許可されます。 新規または変更されたコマンド：**mac-address auto**
Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。	9.17(1)	Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。他のモデルの SFP ポートの場合、**no speed nonegotiate** オプションは速度を 1000 Mbps に設定します。新しいコマンドは、自動ネゴシエーションと速度を個別に設定できることを意味します。 新規/変更されたコマンド：**negotiate-auto**

インターフェイスの詳細設定の履歴

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。