トラフィックの復号の概要

これらのトピックではTLS/SSL（Transport Layer Security/Secure Sockets Layer）インスペクションの概要を示し、TLS/SSLインスペクション構成の前提条件と詳細な導入シナリオについて説明します。

（注） TLSとSSLは相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSLプロトコルは、よりセキュアなTLSプロトコルを選択することによりIETFによって廃止されました。そのため、*TLS/SSL* は通常、TLSのみを指すものとして解釈できます。

SSLプロトコルとTLSプロトコルの詳細については、「SSL vs. TLS - What's the Difference?」[英語] などのリソースを参照してください。

トラフィック復号の説明

インターネット上のほとんどのトラフィックは暗号化されており、ほとんどの場合、復号しないことを選択できます。暗号化されたトラフィックから一部の情報を収集することができ、必要に応じてネットワークからその情報をブロックすることもできます。

選択できるタイプは、次のとおりです。

- トラフィックを復号し、完全な一連の詳細検査の対象とします。
  - [高度なマルウェア防御（Advanced Malware Protection）]
  - セキュリティ インテリジェンス

- Threat Intelligence Director
- アプリケーション ディテクタ
- URL およびカテゴリのフィルタリング

- トラフィックを暗号化したままにしてアクセス制御をセットアップし、decryption policyに検索させ、ブロックできるようにします。
  - 古いプロトコルバージョン（セキュアソケットレイヤなど）
  - セキュアでない暗号スイート
  - リスクが高く、ビジネスとの関連性が低いアプリケーション
  - 信頼できない発行元識別名

アクセス コントロール ポリシー

アクセス コントロール ポリシーは、decryption policy を含む、サブポリシーとその他の設定を呼び出すメイン設定です。アクセスコントロールと decryption policy を関連付けると、システムでは、この decryption policy を使用して暗号化セッションを処理し、その後でそれらのセッションをアクセスコントロールルールで評価します。TLS/SSL インスペクションを設定していない場合、またはデバイスで SSL インスペクションをサポートしていない場合は、アクセス コントロール ルールですべての暗号化トラフィックが処理されます。

TLS/SSL インスペクションの設定で暗号化トラフィックの通過が許可されている場合、アクセスコントロールルールによっても暗号化トラフィックが処理されます。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、システムは暗号化ペイロードの侵入およびファイル インスペクションを無効にしています。これにより、侵入およびファイル インスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

復号するプロトコル中

復号するプロトコルは次のとおりです。

- 1.3 までの TLS バージョン（Snort 3 が有効な場合）
- DNS over HTTPS
- DNS over TLS（RFC 7858）
- FTPS、SMTPS、IMAPS、POP3S

注記

Decryption rulesには、パフォーマンスに影響を及ぼす可能性があるオーバーヘッドの処理が必要です。トラフィックの復号を決定する前に、トラフィックを復号する場合としない場合（11 ページ） を参照してください。

管理対象デバイスで Snort 3 が有効になっていれば、システムは TLS 1.3 トラフィックの復号をサポートします。decryption policyの詳細オプションで TLS 1.3 の復号を有効にすることができます。詳細については、復号ポリシー 詳細オプションを参照してください。

Firepower システムは相互認証をサポートしていません。つまり、クライアント証明書を Secure Firewall Management Center にアップロードして、[復号-再署名（Decrypt - Resign）] アクションまたは [復号-既知のキー（Decrypt - Known Key）] decryption rule アクションに使用することはできません。

FlexConfig を使用して TCP 最大セグメントサイズ（MSS）の値を設定すると、観測される MSS が設定よりも小さくなる可能性があります。詳細については、「About the TCP MSS」を参照してください。

関連トピック

TLS/SSL ハンドシェイク処理 （3 ページ）
Decryption ルールとポリシーの基本 （9 ページ）

TLS/SSL ハンドシェイク処理

このマニュアルでは、*TLS/SSL* ハンドシェイクという用語は SSL プロトコルとその後継プロトコルである TLS の両方の暗号化セッションを開始する、2 ウェイ ハンドシェイクを表します。

インライン展開では、システムは TLS/SSL ハンドシェイクを処理し、ClientHello メッセージを修正する可能性があり、セッションの TCP プロキシサーバーとして機能します。

以下の図はインライン展開を示しています。

（正常に TCP 3 ウェイハンドシェイクが完了した後）クライアントがサーバーとの TCP 接続を確立すると、管理対象デバイスは TCP セッションでの暗号化されたセッションの開始の試行をモニターします。TLS/SSL ハンドシェイクは、クライアントとサーバー間の特殊なパケットの交換を利用して、暗号化セッションを確立します。SSL と TLS プロトコルでは、これらの特殊なパケットはハンドシェイク メッセージと呼ばれます。ハンドシェイク メッセージは、クライアントとサーバの両方がサポートする暗号化属性を伝えます。

- ClientHello：クライアントは各暗号化属性に複数のサポートされる値を指定します。
- ServerHello：サーバーは各暗号化属性に 1 つのサポートされる値を指定し、ServerHello 応答がシステムがセキュリティで保護されたセッション中に使用する暗号化方式を決定します。

TLS/SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッションデータをキャッシュに保存し、それによりフルハンドシェイクを必要とせずにセッションを再開できます。管

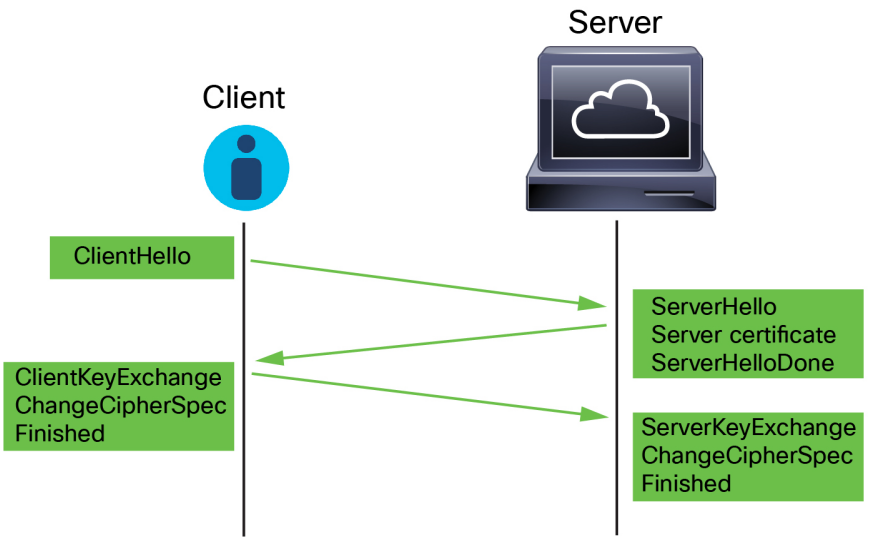
理対象デバイスもサーバー証明書データをキャッシュに保存し、それにより同じ証明書を使用する後続のセッションでのより速いハンドシェイクの処理が可能になります。

ClientHello メッセージ処理

セキュアな接続が確立できる場合、クライアントはパケットの宛先として機能するサーバに ClientHello メッセージを送信します。クライアントは TLS/SSL ハンドシェイクを開始するメッセージを送信するか、または宛先サーバーからの ServerHello メッセージへの応答に含めます。

概要

次の図は例を示しています。RFC 8446, sec. 4 も参照してください。cloudflare.com で「What Happens in a TLS Handshake?」 などのリソースを参照することもできます。



このプロセスは次のように要約できます。

1. ClientHello がプロセスを開始します。

   ClientHello メッセージには、サーバーの完全修飾ドメイン名を持つ Server Name Indication（SNI）が含まれています。

2. 管理対象デバイスが ClientHello メッセージを処理し、宛先サーバに送信した後、サーバはクライアントがメッセージで指定した復号属性をサポートするかどうかを決定します。その属性をサポートしない場合、サーバはクライアントにハンドシェイクの失敗のアラートを送信します。その属性をサポートする場合、サーバは ServerHello メッセージを送信します。同意済みキー交換方式で認証に証明書が使用される場合、サーバー証明書メッセージのすぐ後に ServerHello メッセージが送信されます。

   サーバー証明書には、完全修飾ドメイン名と IP アドレスを持つサブジェクトの代替名（SAN）が含まれています。SAN の詳細については、識別名を参照してください。

3. 管理対象デバイスはこれらのメッセージを受信すると、システムに設定されている decryption rules との照合を試みます。これらのメッセージには、ClientHello メッセージまたはセッショ

ン データ キャッシュにはなかった情報が含まれます。具体的には、decryption rulesの識別名、証明書ステータス、暗号スイート、およびバージョン条件で、これらのメッセージと照合される可能性があります。

プロセス全体が暗号化されます。

データ交換

TLS/SSL復号を設定した場合、管理対象デバイスがClientHelloメッセージを受信すると、システムはそのメッセージを**[復号-再署名（Decrypt - Resign）]**、または**[復号-既知のキー（Decrypt - Known Key）]**アクションを含むdecryption rulesと照合しようとします。照合はClientHelloメッセージからのデータとキャッシュされたサーバ証明書データからのデータに依存します。考えられるデータには次のものがあります。

表 *1 : Decryption rule* 条件のデータの可用性

Decryption rule 条件	**データの存在場所**
ゾーン	ClientHello
Networks	ClientHello
VLAN タグ	ClientHello
ポート	ClientHello
ユーザ	ClientHello
アプリケーション	ClientHello（サーバ名インジケータの拡張機能）
カテゴリ	ClientHello（サーバ名インジケータの拡張機能）
Certificate	サーバー証明書（キャッシュされている可能性あり）
識別名	サーバー証明書（キャッシュされている可能性あり）
証明書のステータス（Certificate Status）	サーバー証明書（キャッシュされている可能性あり）
暗号スイート	ServerHello
Versions	ServerHello

重要 [暗号スイート（Cipher Suite）] と [バージョン（Version）] のルール条件は、[ブロック（Block）] または [リセットしてブロック（Block with reset）] のルールアクションが使用されているルールでのみ使用します。**[暗号スイート（Cipher Suite）]** および **[バージョン（Version）]** を、**[復号 - 再署名（Decrypt - Resign）]** または **[復号 - 既知のキー（Decrypt - Known Key）]** ルールアクションと併用しないでください。ルールのこれらの条件を他のルールアクションとともに使用すると、システムの ClientHello 処理に干渉し、予測できないパフォーマンスが生じる可能性があります。

ClientHello の変更

ClientHello メッセージが **[復号-再署名（Decrypt - Resign）]**、または **[復号-既知のキー（Decrypt - Known Key）]** ルールに一致したら、システムは ClientHello メッセージを次のように変更します。

- （TLS 1.2 のみ。TLS 1.3 は圧縮をサポートしていません。）圧縮方法：クライアントがサポートする圧縮方法を指定する、`compression_methods` 要素を削除します。システムは圧縮されたセッションを復号できません。
- 暗号スイート：システムがサポートしない場合、`cipher_suites` 要素から暗号スイートを削除します。システムが指定した暗号スイートのいずれもサポートしない場合、システムは、元の変更されていない要素を送信します。この変更により、復号できないトラフィックの、サポートされない暗号スイートと不明な暗号スイートが削減されます。
- セッション識別子：キャッシュされたセッションデータと一致しないセッションチケット拡張（(RFC 5077、セクション 3.2）と `Session Identifier` 要素から値を削除します。ClientHello 値がキャッシュされたデータと一致した場合、一時停止したセッションは、クライアントとサーバーが完全な TLS/SSL ハンドシェイクを実行せずに、中断したセッションを再開できます。この変更は、セッション再開の可能性を高め、復号できないトラフィックの、セッションが未キャッシュのタイプを削減します。
- 楕円曲線：システムがサポートしない場合、サポートされる楕円曲線拡張機能から楕円曲線を削除します。システムが指定した楕円曲線のいずれもサポートしない場合、管理対象デバイスは拡張機能を削除し、`cipher_suites` 要素から関連する暗号スイートを削除します。
- ALPN 拡張機能：システムでサポートされていないアプリケーション層プロトコルネゴシエーション（ALPN）拡張機能から値を削除します（たとえば、HTTP/2 プロトコル）。
- 他の拡張機能：Next Protocol Negotiation（NPN）および TLS チャネル ID 拡張機能を削除します。

  [復号 - 再署名（Decrypt - Resign）]、または **[復号 - 既知のキー（Decrypt - Known Key）]** アクションにより Decryption rules は、ClientHello ネゴシエーション時に Extended Master Secret（EMS）拡張機能をネイティブにサポートするので、よりセキュアな通信が可能になりました。EMS 拡張機能は、 RFC 7627 によって定義されています。

システムが ClientHello メッセージを変更した後、メッセージがアクセス コントロール評価（ディープインスペクションを含めることができる）を合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

ClientHello メッセージが [復号-再署名（Decrypt - Resign）] [復号-再認証（Decrypt - Replace Cert）] または [復号-既知のキー（Decrypt - Known Key）]ルールに一致しない場合、システムはメッセージを変更しません。次に、メッセージがアクセス コントロール評価（ディープ インスペクションを含めることができる）で合格するかどうかを決定します。メッセージが検査に合格すれば、システムはそれを宛先サーバーに送信します。

トラフィックが [モニター（Monitor）] ルール条件に一致する場合、ClientHello は変更されません。

Man-In-The-Middle; 中間者

メッセージを変更した後はクライアントおよびサーバで計算されたメッセージ認証コード（MAC）が一致しなくなるため、TLS/SSL ハンドシェイク時のクライアントとサーバの間の直接通信はできなくなります。すべての後続のハンドシェイクメッセージ（および一度設定された暗号化セッション）に対し、管理対象デバイスは、中間者として機能します。ここでは 2 つの TLS/SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバーの間で使用されます。その結果、暗号セッションの詳細はセッションごとに異なります。

（注） システムが復号できる暗号スイートは頻繁に更新されるので、decryption rule の条件で使用可能な暗号スイートと直接対応しません。復号できる暗号スイートの現在のリストについては、Cisco TAC に連絡してください。

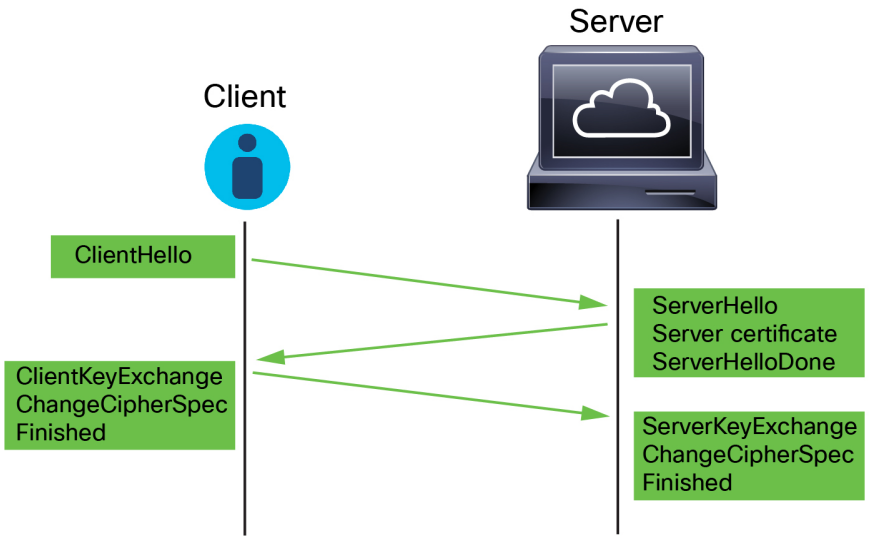
関連トピック

復号できないトラフィックのデフォルト処理オプション
ServerHello とサーバー証明書メッセージの処理 （7 ページ）

ServerHello とサーバー証明書メッセージの処理

概要

次の図は例を示しています。RFC 8446, sec. 4 も参照してください。cloudflare.com で「What Happens in a TLS Handshake?」 などのリソースを参照することもできます。



このプロセスは次のように要約できます。

1. ClientHello がプロセスを開始します。

   ClientHello メッセージには、サーバーの完全修飾ドメイン名を持つ Server Name Indication（SNI）が含まれています。

2. 管理対象デバイスが ClientHello メッセージを処理し、宛先サーバに送信した後、サーバはクライアントがメッセージで指定した復号属性をサポートするかどうかを決定します。その属性をサポートしない場合、サーバはクライアントにハンドシェイクの失敗のアラートを送信します。その属性をサポートする場合、サーバは ServerHello メッセージを送信します。同意済みキー交換方式で認証に証明書が使用される場合、サーバー証明書メッセージのすぐ後に ServerHello メッセージが送信されます。

   サーバー証明書には、完全修飾ドメイン名と IP アドレスを持つサブジェクトの代替名（SAN）が含まれています。SAN の詳細については、識別名を参照してください。

3. 管理対象デバイスはこれらのメッセージを受信すると、システムに設定されている decryption rules との照合を試みます。これらのメッセージには、ClientHello メッセージまたはセッション データ キャッシュにはなかった情報が含まれます。具体的には、decryption rules の識別名、証明書ステータス、暗号スイート、およびバージョン条件で、これらのメッセージと照合される可能性があります。

プロセス全体が暗号化されます。

Decryption rule アクション

メッセージが decryption rules と一致しない場合、管理対象デバイスは、復号ポリシーのデフォルトアクションを実行します。

メッセージが、アクセス コントロール ポリシーに関連付けられた decryption policy に属するルールに一致する場合、管理対象デバイスは必要に応じて以下を続行します。

アクション：モニター（Monitor）
TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスはトラフィックを追跡してログに記録しますが、復号はしません。

アクション：ブロック（Block）、またはリセットしてブロック（Block with Reset）

管理対象デバイスは TLS/SSL セッションをブロックし、設定されている場合は TCP 接続をリセットします。

アクション：復号しない（Do Not Decrypt）

TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスは、TLS/SSL セッションの間で交換されるアプリケーション データを復号しません。

アクション：復号 - 既知のキー（Decrypt - Known Key）

管理対象デバイスは、以前に Secure Firewall Management Center にインポートした内部証明書オブジェクトをサーバー証明書データに一致させようとします。内部証明書オブジェクトは作成できないため、また、秘密キーを所有する必要があるため、既知のキー復号を使用しているサーバーを所有していることを想定しています。

証明書が既知の証明書と一致した場合、TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、TLS/SSL セッション中に交換されたアプリケーション データを復号および再暗号化します。

クライアントとの初回接続と後続の接続の間でサーバーが証明書を変更した場合、将来の接続を復号するには、Secure Firewall Management Center に新しいサーバー証明書をインポートする必要があります。

アクション：復号 - 再署名（Decrypt - Resign）

管理対象デバイスはサーバー証明書メッセージを処理し、サーバー証明書に以前にインポートまたは生成した認証局（CA）で再署名します。TLS/SSL ハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、TLS/SSL セッション中に交換されたアプリケーションデータを復号し、再暗号化します。

（注） Firepower システムは相互認証をサポートしていません。つまり、クライアント証明書を Secure Firewall Management Center にアップロードして、[復号-再署名（Decrypt - Resign）] アクションまたは [復号-既知のキー（Decrypt - Known Key）] decryption rule アクションに使用することはできません。

関連トピック
ClientHello メッセージ処理 （4 ページ）

Decryption ルールとポリシーの基本

ここでは、decryption policies とルールの作成時に注意する必要がある情報について説明します。

（注） TLS と SSL は相互に使用されることが多いため、*TLS/SSL* という表現を使用していずれかのプロトコルについて説明していることを示しています。SSL プロトコルは、よりセキュアな TLS プロトコルを選択することにより IETF によって廃止されました。そのため、*TLS/SSL* は通常、TLS のみを指すものとして解釈できます。

SSL プロトコルと TLS プロトコルの詳細については、「SSL vs. TLS - What's the Difference?」[英語] などのリソースを参照してください。

関連トピック

復号のケース （10 ページ）
トラフィックを復号する場合としない場合 （11 ページ）
その他の decryption rule アクション （14 ページ）
Decryption rule コンポーネント （14 ページ）
復号ルール 評価順序 （15 ページ）
TLS 1.3 復号のベストプラクティス

復号のケース

システムを通過するときに暗号化されたトラフィックは許可またはブロックできますが、ディープ インスペクションやすべての範囲のポリシー適用（侵入防御など）は対象にできません。

すべての暗号化された接続：

- 復号またはブロックする必要があるか判断するために、decryption policyを介して送信されます。

  また、 decryption rulesを設定し、非セキュアな SSL プロトコルを使用するトラフィックや、期限切れまたは無効な証明書を使用するトラフィックなど、ネットワークに必要ないとわかっているタイプの暗号化トラフィックをブロックできます。

- ブロックされていないトラフィックは、復号の有無に関係なく、アクセス コントロール ポリシーを経由して、最終的に許可またはブロックの判断が行われます。

以下のような、システムの Threat Defense およびポリシーの適用機能を利用できるのは、復号されたトラフィックのみです。

- [高度なマルウェア防御（Advanced Malware Protection）]
- セキュリティ インテリジェンス
- Threat Intelligence Director
- アプリケーション ディテクタ
- URL およびカテゴリのフィルタリング

トラフィックの復号とその後の再暗号化は、全体的なシステムパフォーマンスを低下させるデバイスの処理負荷が増加することに注意してください。

次に要約を示します。

- 暗号化されたトラフィックはポリシーで許可またはブロックすることができます。暗号化されたトラフィックは検査できません
- 復号されたトラフィックは脅威に対する防御とポリシーの適用に従います。復号されたトラフィックはポリシーで許可またはブロックできます。

  システムはStartTLS（SMTPS、POPS、FTPS、TelnetS、IMAPSなど）を使用して暗号化されたアプリケーショントラフィックを検出できます。また、TLS ClientHelloメッセージのサーバー名の指定、またはサーバー証明書のサブジェクト識別名の値に基づいて特定の暗号化アプリケーションを特定できます。

関連トピック

ファイル ポリシーと侵入ポリシーを使用したディープ インスペクション

トラフィックを復号する場合としない場合

ここでは、トラフィックを復号する場合と暗号化されたファイアウォールの通過を許可する場合のガイドラインを示します。

トラフィックを復号しない場合

次によって禁止されている場合は、トラフィックを復号してはいけません。

- 法律：たとえば、一部の法域では、財務情報の復号が禁止されています
- 会社のポリシー：たとえば、会社によって特権的な通信の復号が禁止されている場合があります
- プライバシー規制
- 証明書のピン留め（*TLS/SSL* ピニングとも呼ばれる）を使用するトラフィックは、接続の切断を防ぐため、暗号化されたままにする必要があります

（Snort 3）Decryption policy は、トラフィックがプレフィルタされている場合を除き、[信頼（Trust）]、[ブロック（Block）]、または [リセットしてブロック（Block With Reset）] のアクションを持つアクセスコントロールルールに一致する接続に関してバイパスされません。暗号化トラフィックは最初に decryption policy によって評価され、次にアクセス コントロール ポリシーに進みます。ここで最終的な許可またはブロックの決定が行われます。

暗号化されたトラフィックは、次のものを含むがこれらに限定されない任意の decryption rule 条件で許可またはブロックできます。

- 証明書のステータス（期限切れまたは無効な証明書など）
- プロトコル（セキュアでない SSL プロトコルなど）

- ネットワーク（セキュリティ ゾーン、IP アドレス、VLAN タグなど）
- URL のカテゴリとレピュテーション
- ポート
- ユーザー グループ

Decryption rules は、復号しないトラフィックに対して **[復号しない（Do not Decrypt）]** アクションを提供します。詳細については、Decryption rule 復号アクションを実行しない を参照してください。

（注） このトピックの最後にある関連情報リンクでは、ルール評価のいくつかの側面について説明します。URL やアプリケーション フィルタリングなどの条件には、暗号化されたトラフィックに関する制限があります。これらの制限事項を必ず確認してください。

[復号しない（Do Not Decrypt）] ルールでの URL フィルタリング使用の詳細については、Decryption rule 復号アクションを実行しないを参照してください。

トラフィックを復号する場合

システムの脅威に対する防御とポリシーの適用機能を利用できるのは、暗号化されたすべてのトラフィックです。管理対象デバイスにトラフィックを復号化するのに十分なメモリと処理能力がある場合、法令や規制で禁止されていないトラフィックは復号化すべきです。

復号するトラフィックを決定する必要がある場合は、ネットワーク上のトラフィックを許可するリスクに基づいて決定します。システムは、URL の評価、暗号スイート、プロトコル、その他多くの要因を含む、ルール条件を使用してトラフィックを分類するための柔軟なフレームワークを提供します。

関連トピック

復号と再署名（発信トラフィック） （12 ページ）
復号ルール 注意事項と制約事項
Decryption policy ルールの順序
URL 条件（URL フィルタリング）
アプリケーション ルールの順序
TLS 1.3 復号のベストプラクティス
既知のキーでの復号（着信トラフィック） （13 ページ）

復号と再署名（発信トラフィック）

[復号と再署名（Decrypt - Resign）] decryption ruleアクションでは、システムは中間者となり、傍受、復号、および検査（トラフィックの通過が許可されている場合）し、再暗号化することができます。[復号と再署名（Decrypt - Resign）] ルール アクションは発信トラフィックで使用されます。つまり、宛先サーバーは保護ネットワーク外にあります。

Firewall Threat Defense デバイスは、ルールで指定された内部認証局（CA）オブジェクトを使用してクライアントとネゴシエートし、クライアントと Firewall Threat Defense デバイス間に TLS/SSL トンネルを構築します。同時に、デバイスは宛先 Web サイトに接続し、サーバーと Firewall Threat Defense デバイス間に TLS/SSL トンネルを作成します。

このため、クライアントには、宛先サーバーからの証明書ではなく、decryption ruleで設定された CA 証明書が表示されます。クライアントは、接続を完了するためにファイアウォールの証明書を信頼する必要があります。Firewall Threat Defense デバイスは、クライアントと宛先サーバー間のトラフィックで両方向に復号/再暗号化を実行します。

前提条件

[復号と再署名（Decrypt - Resign）] ルール アクションを使用するには、CA ファイルとペアの秘密キー ファイルを使用して、内部 CA オブジェクトを作成する必要があります。CA と秘密キーをまだ使用していない場合は、システムで生成できます。

暗号化から除外するトラフィックのタイプ（復号できないアプリケーションなど）の選択に基づいて復号ポリシーに [復号しない（Do Not Decrypt）] ルールを自動的に追加することで、[復号 - 再署名（Decrypt - Resign）] ルールの設定プロセスが簡素化されます（通常、このようなアプリケーションでは、接続を復号すると接続が解除されるように、証明書のピン留めが使用されています）。詳細については、「アウトバウンド接続保護を使用した復号ポリシーの作成」を参照してください。

（注） Firepower システムは相互認証をサポートしていません。つまり、クライアント証明書を Secure Firewall Management Center にアップロードして、[復号-再署名（Decrypt - Resign）] アクションまたは [復号-既知のキー（Decrypt - Known Key）] decryption rule アクションに使用することはできません。

関連トピック

Decryption ruleの復号アクション
外部証明書オブジェクト

既知のキーでの復号（着信トラフィック）

[復号 - 既知のキー（Decrypt - Known Key）] decryption rule アクションは、サーバーの秘密鍵を使用してトラフィックを復号します。[復号と既知のキー（Decrypt - Known Key）] ルール アクションは着信トラフィックで使用されます。つまり、宛先サーバは保護ネットワーク内にあります。

既知のキーを使用して復号する主な目的は、社内サーバーを外部の攻撃から保護することです。

前提条件

[復号 - 既知のキー（Decrypt - Known Key）] ルール アクションを使用するには、サーバーの証明書ファイルとペアの秘密キー ファイルを使用して、内部証明書オブジェクトを作成する必要があります。

（注） Firepowerシステムは相互認証をサポートしていません。つまり、クライアント証明書をSecure Firewall Management Centerにアップロードして、[復号-再署名（Decrypt - Resign）]アクションまたは[復号-既知のキー（Decrypt - Known Key）] decryption ruleアクションに使用することはできません。

関連トピック

Decryption ruleの復号アクション
内部証明書オブジェクト
既知のキーでの復号（着信トラフィック） （13 ページ）

その他の decryption rule アクション

以降のトピックでは、他の decryption rule アクションについて説明します。

関連トピック

Decryption ruleのブロック アクション
Decryption ruleのモニター アクション

Decryption rule コンポーネント

decryption ruleにはそれぞれ次のコンポーネントがあります。

状態（State）

ルールは、有効または無効の2つの状態のいずれかになります。デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置（Position）

decryption policy のルールには、1から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。

条件

条件は、ルールが処理する特定のトラフィックを指定します。こうした条件では、セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求されたURLのカテゴリーと評価、ユーザー、証明書、証明書のサブジェクトまたは発行元、証明書の状態、暗号スイート、暗号化プロトコルバージョンなどによってトラフィックを照合できます。使用する条件は、ターゲット デバイスのライセンスによって異なります。

操作（Action）

ルールのアクションによって、一致したトラフィックの処理方法が決まります。暗号化された一致したトラフィックは、モニタ、許可、ブロック、または復号できます。復号したトラフィックには、さらにインスペクションが適用されます。システムは、ブロックされた暗号化トラフィックに対してインスペクションを実行しないことに注意してください。

ログ

ルールのロギング設定によって、システムが記録する処理済みトラフィックのレコードを管理します。1つのルールに一致するトラフィックのレコードを1つ保持できます。decryption policyでの設定に従って、システムが暗号化セッションをブロックするか、復号なしで渡すことを許可するときに、その接続をログに記録できます。アクセス コントロール ルールに従ってより詳細な評価のために復号した場合の接続ログを記録するようにシステムを強制することも可能で、これはその後でどのような処理やトラフィックの検査がされるかとは無関係です。接続のログは、Secure Firewall Management Center のデータベースの他に、システム ログ（Syslog）または SNMP トラップ サーバーに記録できます。

ロギングの詳細については、*Cisco Secure Firewall Management Center Administration Guide*の「Best Practices for Connection Logging」を参照してください。

ヒント　decryption rule を適切に作成し順序付けするのは、複雑なタスクです。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。想定どおりにトラフィックを処理できるように、decryption policyインターフェイスには、ルールに関する強力な警告およびエラーのフィードバックシステムが用意されています。

カテゴリ

decryption rule カテゴリ（アプリケーション、カテゴリ、証明書ステータスなど）の使用方法については、復号ルール 条件を参照してください。

復号ルール 評価順序

復号ポリシー で復号ルール を作成する場合、ルールエディタの [挿入（Insert）] リストを使用してその位置を指定します。decryption policy内のDecryption rulesには、1 から始まる番号が付けられています。decryption rulesは、ルール番号の昇順で上から順にトラフィックと照合されます。

ほとんどの場合、ネットワークトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初のdecryption ruleに従って実行されます。モニター ルール（トラフィックをログに記録するがトラフィック フローには影響しないルール）の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることはありません。こうした条件には、単純なものと複雑なものがあります。セキュリティゾーン、ネットワークまたは地理的位置、VLAN、ポート、アプリケーション、要求された URL カテゴリとレピュテーション、ユーザー、証明書、証明書の識別名、証明書ス

テータス、暗号スイート、暗号化プロトコルバージョンなどによってトラフィックを制御できます。

各ルールにはアクションも設定されます。アクションにより、アクセス制御と一致する暗号化または復号トラフィックに対してモニター、ブロック、検査のいずれを行うかが決まります。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが行われないことに注意してください。暗号化されたトラフィックおよび復号できないトラフィックはアクセス コントロールの対象です。ただし、アクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなります。

Rules that use *specific* conditions (such as network and IP addresses) should be ordered *before* rules that use general conditions (such as applications). If you're familiar with the Open Systems Interconnect (OSI) model, use similar numbering in concept. Rules with conditions for layers 1, 2, and 3 (physical, data link, and network) should be ordered first in your rules. Conditions for layers 5, 6, and 7 (session, presentation, and application) should be ordered later in your rules. For more information about the OSI model, see this Wikipedia article.

ヒント　適切なdecryption ruleの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。ユーザーが作成するルールはすべての組織と展開に固有のものですが、ユーザーのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

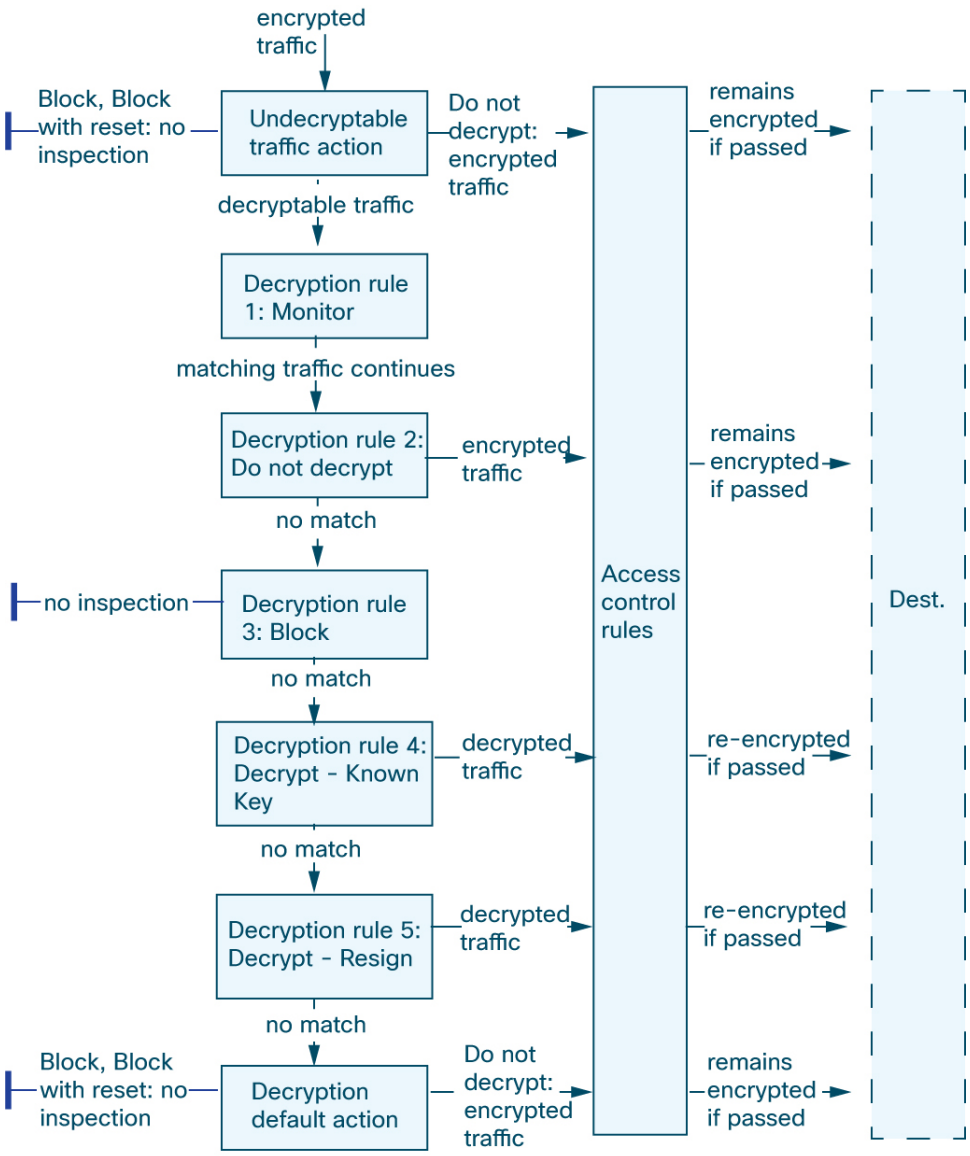
番号ごとのルールの順序付けに加えて、カテゴリ別にルールをグループ化できます。デフォルトでは、3つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、システム提供のカテゴリを削除したり、それらの順序を変更したりすることはできません。

関連トピック

アクセス コントロール ルールのベストプラクティス
復号できないトラフィックのデフォルト処理オプション
Decryption policy ルールの順序

複数ルールの例

次のシナリオは、インライン展開での decryption rules によるトラフィックの処理を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **復号できないトラフィック アクション（Undecryptable Traffic Action）**は、暗号化されたトラフィックを最初に評価します。復号できないトラフィックについてシステムは、それ以上のインスペクションなしでブロックするか、あるいはアクセスコントロールによるインスペクション用に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **Decryption rule 1：モニター（Monitor）**は、暗号化トラフィックを次に評価します。モニタールールは、暗号化トラフィックのログ記録と追跡を行いますが、トラフィック フローには影響しません。システムは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。

- **Decryption rule 2**：**復号しない（Do Not Decrypt**）は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号されません。システムはこのトラフィックをアクセス コントロールにより検査しますが、ファイルや侵入インスペクションは行いません。一致しなかったトラフィックは、次のルールへと進められます。
- **Decryption rule 3**：**ブロック（Block**）は、暗号化トラフィックを 4 番目に評価します。一致するトラフィックは、追加のインスペクションなしでブロックされます。一致しないトラフィックは、引き続き次のルールと照合されます。
- **Decryption rule 4**：**復号 - 既知のキー（Decrypt - Known Key**）は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザーのアップロードする秘密キーを使用して復号されます。復号トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加検査の結果、システムがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。decryption rule に一致しないトラフィックは、引き続き次のルールと照合されます。
- **Decryption rule 5**：**復号 - 再署名（Decrypt - Resign**）は、最後のルールです。トラフィックが一致した場合、システムはアップロードされた CA 証明書を使用してサーバー証明書を再署名してから、トラフィックを復号します。復号化されたトラフィックは、その後、復号化されたトラフィックと暗号化されていないトラフィックを同じように処理するアクセス コントロール ルールに対して評価されます。この追加検査は、システムがトラフィックをブロックすることを許可します。他のすべてのトラフィックは、その宛先への送信される前に再暗号化されます。decryption rule ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **Decryption policyデフォルトアクション**は、いずれの decryption rules にも一致しないすべてのトラフィックを処理します。デフォルトアクションでは、暗号化トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号しないで、アクセス コントロールによる検査を行います。

TLS 暗号化アクセラレーション

TLS 暗号化アクセラレーション 次のことを促進します。

- TLS/SSL 暗号化および復号
- VPN（TLS/SSL および IPsec を含む）

サポート対象ハードウェア

以下のハードウェア モデルは TLS 暗号化アクセラレーションをサポートしています。

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

- Firepower 4100/9300

  Firepower 4100/9300 Firewall Threat Defense container instanceでの TLS 暗号化アクセラレーションのサポートの詳細については、『*FXOS Configuration Guide*』を参照してください。

仮想アプライアンス上および上記以外のハードウェアでの TLS 暗号化アクセラレーション はサポートされていません。

（注） TLS 暗号化アクセラレーションおよび 4100/9300 の詳細については、『*FXOS Configuration Guide*』を参照してください。

サポートしていない機能 TLS 暗号化アクセラレーション

TLS 暗号化アクセラレーション でサポートしていない機能は次のとおりです。

- Firewall Threat Defense container instance が有効になっている管理対象デバイス。
- インスペクション エンジンが接続を維持するように設定されていて、インスペクション エンジンが予期せず失敗した場合は、エンジンが再起動されるまでTLS/SSL トラフィックはドロップされます。

  この動作はによって制御されます、**configure snort preserve-connection {enable | disable}**コマンド。

TLS 暗号化アクセラレーション 注意事項と制約事項

管理対象デバイスで TLS 暗号化アクセラレーションが有効になっている場合は、次の点に留意してください。

HTTP のみのパフォーマンス

トラフィックを復号しない管理対象デバイスでTLS暗号化アクセラレーションを使用すると、パフォーマンスに影響を与えることがあります。

Federal Information Processing Standards（FIPS）

TLS暗号化アクセラレーションと連邦情報処理標準（FIPS）が両方とも有効になっている場合は、次のオプションの接続が失敗します。

- サイズが 2048 バイト未満の RSA キー
- Rivest 暗号 4（RC4）
- 単一データ暗号化標準規格（単一 DES）
- Merkle–Damgard 5（MD5）
- SSL v3

セキュリティ認定準拠モードで動作するようにFirewall Management Centerと管理対象デバイスを設定すると、FIPS が有効になります。このモードで動作しているときに接続を許可するには、よりセキュアなオプションを採用するように Web ブラウザを設定します。

詳細については、次を参照してください。

- FIPS でサポートされている暗号方式：SSL 設定について。
- セキュリティ認定準拠のモード。
- コモン クライテリア。

TLS ハートビート

一部のアプリケーションでは、RFC6520 で定義されている Transport Layer Security（TLS）および Datagram Transport Layer Security（DTLS）プロトコルに対して、TLS ハートビート エクステンションが使用されます。TLS ハートビートは、接続がまだ有効であることを確認する方法を提供します。クライアントまたはサーバが指定されたバイト数のデータを送信し、応答を返すように相手に要求します。これが成功した場合は、暗号化されたデータが送信されます。

TLS 暗号化アクセラレーションが有効になっている管理対象デバイスは、TLS ハートビート エクステンションを使用するパケットを処理する場合、decryption policyの [復号不可のアクション（Undecryptable Actions）] の [復号エラー（Decryption Errors）] の設定で指定されているアクションを実行します。

- Block
- Block with reset

詳細については、復号できないトラフィックのデフォルト処理オプションを参照してください。

アプリケーションが TLS ハートビートを使用しているかどうかを判断するには、TLS ハートビートのトラブルシュートを参照してください。

ネットワーク分析ポリシー（NAP）で [最大ハートビート長（Max Heartbeat Length）] を設定して TLS ハートビートの処理方法を決定できます。詳細については、SSL プリプロセッサを参照してください。

TLS/SSL オーバーサブスクリプション

TLS/SSL オーバーサブスクリプションとは、管理対象デバイスが TLS/SSL トラフィックにより過負荷になっている状態です。すべての管理対象デバイスで TLS/SSL オーバーサブスクリプションが発生する可能性がありますが、TLS 暗号化アクセラレーションをサポートする管理対象デバイスでのみ処理方法を設定できます。

TLS 暗号化アクセラレーションが有効になっている管理対象デバイスがオーバーサブスクライブされた場合、管理対象デバイスによって受信されるパケットの扱いは、decryption policyの [復号不可のアクション（Undecryptable Actions）] の [ハンドシェイクエラー（Handshake Errors）] の設定に従います。

- デフォルト アクションを継承（Inherit default action）

- Do not decrypt
- Block
- Block with reset

decryption policy の [復号不可のアクション（Undecryptable Actions）] の [ハンドシェイクエラー（Handshake Errors）] の設定が [復号しない（Do Not decrypt）] で、関連付けられたアクセスコントロール ポリシーがトラフィックを検査するように設定されている場合は、インスペクションが行われます。復号は行われません。

大量のオーバーサブスクリプションが発生している場合は、次のオプションがあります。

- 管理対象デバイスをアップグレードして、TLS/SSL の処理能力を向上させます。
- decryption policies を変更して、復号の優先順位が高くないトラフィック用に [Do Not Decrypt] ルールを追加します。

View the status of TLS crypto acceleration

This topic discusses how you can determine if TLS crypto acceleration is enabled.

Perform the following task in the Firewall Management Center.

手順

ステップ 1 Log in to the Firewall Management Center.
ステップ 2 Click **Devices** > **Device Management**.
ステップ 3 Click **Edit** (✎) to edit a managed device.
ステップ 4 Click **Device** page. TLS crypto acceleration status is displayed in the General section.

DTLS 暗号化アクセラレーション

Firewall Threat Defense は、次のモデルの Datagram Transport Layer Security（*DTLS*）暗号化アクセラレーションをサポートします。

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

Cisco Secure Firewall 3100 および 4200 シリーズ デバイスは、FPGA および Nitrox V 暗号化アクセラレータを使用して、DTLS 暗号化アクセラレーションをサポートします。

この機能により、DTLS で暗号化および復号されたトラフィックのスループットが向上します。IPv4 と IPv6 の両方のトラフィックがサポートされます。

Firewall Threat Defenseは、遅延を改善するために、出力暗号化パケットの最適化も実行します。データパスを最適化して、単一トンネルフローのパフォーマンスを向上させます。

どちらの機能もデフォルトで有効になっており、DTLS 1.2 でのみ動作します。

これらの機能は以下ではサポートされていません。

- DTLS 1.0 またはパケット圧縮を使用しているフロー
- キー再生成された DTLS キー
- クラスタリングまたはマルチインスタンスモード

FlexConfig および **no flow-offload-dtls** および **no flow-offload-dtls egress-optimization** コマンドを使用して、DTLS 暗号化アクセラレーションを無効化できます。

DTLS 暗号化アクセラレーションの前提条件

サポートされているライセンス

- Management Center Essentials（旧 Base）ライセンスでは、輸出規制対象機能を許可する必要があります。

  Management Center でこの機能を確認するには、**System (⚙) > Licenses > Smart Licenses**の順に選択します。

サポートされるバージョン

- Firewall Management Center はバージョン 7.6.0 以降である必要があります。
- Cisco Secure Firewall 4200 および 3100 シリーズ デバイスは、バージョン 7.6.0 以降である必要があります。

サポートされるデバイス

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

DTLS 暗号化アクセラレーションのモニタリング

DTLS暗号化アクセラレーションと出力暗号化パケットの最適化を確認してモニターするには、Threat Defense デバイスで以下の CLI コマンドを使用します。

- DTLS 暗号化アクセラレーションと出力暗号化パケットの最適化のステータスを確認するには、以下のコマンドを使用します。

```
> show flow-offload-dtls info
  DTLS offload : Enabled
```

```
  Egress Optimization: Enabled
```

- DTLS 暗号化アクセラレーションの統計を表示するには、以下のコマンドを使用します。

```
> show flow-offload-dtls statistics
  Packet stats of Pipe 0
  ----------------------
  Rx Packet count : 975638666
  Tx Packet count : 975638666
  Error Packet count : 0
  Drop Packet count : 0

  CAM stats of Pipe 0
  ----------------------
  Option ID Table CAM Hit Count : 1145314723
  Option ID Table CAM Miss Count : 0
  Tunnel Table CAM Hit Count : 0
  Tunnel Table CAM Miss Count : 0
  6-Tuple CAM Hit Count : 975638666
  6-Tuple CAM Miss Count : 169676057
   NOTE: The counters displayed are cumulative counters
   for all offload applications and indicates the total packets
  offloaded
```

- Secure Firewall 3100 および 4200 の、デバイスの Nitrox V 暗号化アクセラレータの統計を表示するには、以下のコマンドを使用します。

```
> show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
<snip>
[Offloaded SSL Input statistics, Pipe 0]
      Input packets: 290593023
      Input bytes: 147049729714
      Decrypted packets: 290593023
      Decrypted bytes: 147049729714
   [Offloaded SSL Output statistics, Pipe 0]
      Output packets: 254271808
      Output bytes: 136352952720
      Encrypted packets: 254271808
      Encrypted bytes: 136352952720
.
.
.
```

decryption policy の履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Hardware DTLS 1.2 crypto acceleration for the Secure Firewall 3100/4200.	7.6.0	7.6.0	The Secure Firewall 3100/4200 now supports DTLS 1.2 cryptographic acceleration and egress optimization, which improves throughput of DTLS-encrypted and decrypted traffic. This is automatically enabled on new and upgraded devices. To disable, use FlexConfig. New/modified FlexConfig commands: **flow-offload-dtls**, **flow-offload-dtls egress-optimization**, **show flow-offload-dtls**
QUIC decryption.	7.7.0（試験版） 7.6.0（試験版）	Snort 3 搭載の 7.6.0	You can configure the decryption policy to apply to sessions running on the QUIC protocol. QUIC decryption is disabled by default. You can selectively enable QUIC decryption per decryption policy and write decryption rules to apply to QUIC traffic. By decrypting QUIC connections, the system can then inspect the connections for intrusion, malware, or other issues. You can also apply granular control and filtering of decrypted QUIC connections based on specific criteria in the access control policy. We modified the decryption policy Advanced Settings to include the option to enable QUIC decryption.
Easily bypass decryption for sensitive and undecryptable traffic.	7.6.0	7.6.0	It is now easier to bypass decryption for sensitive and undecryptable traffic, which protects users and improves performance. New decryption policies now include predefined rules that, if enabled, can automatically bypass decryption for sensitive URL categories (such as finance or medical), undecryptable distinguished names, and undecryptable applications. Distinguished names and applications are undecryptable typically because they use TLS/SSL certificate pinning, which is itself not decryptable. For outbound decryption, you enable/disable these rules as part of creating the policy. For inbound decryption, the rules are disabled by default. After the policy is created, you can edit, reorder, or delete the rules entirely. New/modified screens: **Policies** > **Access Control** > **Decryption** > **Create Decryption Policy**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
復号ポリシー。	7.3.0	7.3.0	機能をより適切に反映するために、機能の名前が復号ポリシーに変更されました。1 つ以上の [復号-再署名（Decrypt - Resign）] または [復号-既知のキー（Decrypt - Known Key）] ルールを同時に使用して復号ポリシーを構成できるようになりました。 新規/変更された画面： • 新規/変更された画面：**[ポリシー（Policies）]** > **[アクセス制御のヘディング（Access Control heading）]** > **[復号（Decryption）]**（復号ポリシーの新規作成） • [復号ポリシーの作成（Create Decryption Policy）] ダイアログボックスには、[アウトバウンド接続（Outbound Connections）] と [インバウンド接続（Inbound Connections）] の 2 つのタブページが追加されました。 [アウトバウンド接続（Outbound Connections）] タブページを使用して、1 つ以上の復号ルールを [復号-再署名（Decrypt - Resign）] ルールアクションで構成します。(You can either upload or generate certificate authorities at the same time）. CA とネットワークおよびポートの組み合わせごとに、1 つの復号ルールが作成されます。 [インバウンド接続（Inbound Connections）] タブページを使用して、1 つ以上の復号ルールを [復号-既知のキー（Decrypt - Known Key）]ルールアクションで構成します。（同時にサーバーの証明書をアップロードできます。）サーバー証明書とネットワークおよびポートの組み合わせごとに、1 つの復号ルールが作成されます。 • **[ポリシー（Policies）]** > **[アクセス制御のヘディング（Access Control heading）]** > **[復号（Decryption）]**（複合ルールの編集）**[詳細設定（Advanced Settings）]** には、TLS 1.3 復号のベストプラクティス で説明されている新しいオプションがあります。 • **[ポリシー（Policies）]** > **[アクセス制御のヘディング（Access Control Heading）]** > **[アクセス制御（Access Control）]**（アクセス制御ポリシーの編集）、**[復号（Decryption）]** という単語をクリックして、復号ポリシーをアクセス制御ポリシーに関連付けます。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
TLS 1.3 復号。	7.2.0	7.2.0	SSL ポリシーの詳細なアクションで TLS 1.3 復号を有効にできるようになりました。TLS 1.3 復号では、管理対象デバイスで Snort 3 を実行する必要があります。 他のオプションも利用できます。詳細については、TLS 1.3 復号のベストプラクティスを参照してください。 新規/変更画面：**[SSLポリシー（SSL Policy）]** > **[詳細設定（Advanced Settings）]**
SSL ポリシーの詳細設定。	7.2.0	7.1.0	SSL ポリシーの詳細設定 新規/変更画面：**[SSLポリシー（SSL Policy）]** > **[詳細設定（Advanced Settings）]**
レピュテーションが不明な URL の処理を指定する機能。	6.7.0	6.7.0	詳細については、カテゴリおよびレピュテーションによる URL のフィルタリングについてを参照してください。
[復号-既知（Decrypt - Known）] キールールのための ClientHello の変更。	6.7.0	6.7.0	詳細については、ClientHello メッセージ処理 （4 ページ）を参照してください。
TLS 1.3 トラフィックで証明書を抽出して、アクセス制御ルールの URL およびアプリケーションの条件とのトラフィックの照合を有効にする機能。	6.7.0	6.7.0	新規/変更された画面：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **（アクセス コントロール ポリシーの編集）** > **[詳細（Advanced）]** リンク。 詳細は、復号ポリシー 詳細オプションを参照してください。
カテゴリとレピュテーションに基づく URL フィルタリングの変更。	6.7.0	6.5.0	詳細については、カテゴリおよびレピュテーションによる URL のフィルタリングについてを参照してください。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
TLS 暗号化アクセラレーションを無効にすることはできません。	6.4.0	6.4.0	TLS暗号化アクセラレーションすべてのサポート対象デバイスで有効にします。 ネイティブインターフェイスを持つ管理対象デバイスでは、TLS暗号化アクセラレーションを無効にできません。 Firewall Threat Defense container instance の TLS 暗号化アクセラレーションは、この表の次の行で示すように限定されています。 削除されたコマンド： • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status**
Firepower 4100/9300 モジュール/セキュリティエンジンのいずれかの Firewall Threat Defense container instance での TLS 暗号化アクセラレーション のサポート。	6.4.0	6.4.0	モジュール/セキュリティ エンジンのいずれかの Firewall Threat Defense container instanceで TLS 暗号化アクセラレーションを有効にできるようになりました。他のコンテナ インスタンスの TLS 暗号化アクセラレーションは無効ですが、ネイティブインスタンスでは有効になっています。 新規/変更されたコマンド： • **config hwCrypto enable** • **show crypto accelerator status** replaces **system support ssl-hw-status**)
TLS/SSL ハードウェアアクセラレーションは *TLS* 暗号化アクセラレーションと呼ばれるようになりました。	6.4.0	6.4.0	名前の変更は、TLS/SSL 暗号化と復号アクセラレーションがより多くのデバイスでサポートされていることを反映しています。デバイスによっては、アクセラレーションがソフトウェアまたはハードウェアで実行される場合があります。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** > **[デバイス（Device）]** > **[全般（General）]** > **[TLS暗号化アクセラレーション（TLS Crypto Acceleration）]**
Extended Master Secret 拡張機能がサポートされています（RFC 7627 を参照）。	6.3.0.1	6.3.0.1	TLS Extended Master Secret 拡張機能は、SSL ポリシー（具体的には、[復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Known Key）] のルール アクションを持つポリシー）でサポートされています。
Extended Master Secret 拡張機能はサポートされていません。	6.3.0	6.3.0	拡張機能は [復号 - 再署名（Decrypt - Resign）] ルールの ClientHello 変更時に削除されます。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
TLS/SSL ハードウェアアクセラレーションはデフォルトでは、有効です。	6.3.0	6.3.0	TLS/SSL ハードウェア アクセラレーション デフォルトですべてのサポート対象デバイスで有効になっていますが、必要に応じて無効にすることができます。
Extended Master Secret 拡張機能がサポートされています（RFC 7627 を参照）。	6.2.3.9	6.2.3.9	TLS Extended Master Secret 拡張機能は、SSL ポリシー（具体的には、[復号 - 再署名（Decrypt - Resign）] または [復号 - 既知のキー（Known Key）] のルール アクションを持つポリシー）でサポートされています。
アグレッシブ TLS 1.3 ダウングレード。	6.2.3.7	6.2.3.7	**system support ssl-client-hello-enabled aggressive_tls13_downgrade {true|false}** CLI コマンドを使用して、TLS 1.2 への TLS 1.3 トラフィックのダウングレードの動作を決定できます。詳細については、*Cisco Secure Firewall Threat Defense Command Reference* を参照してください。
TLS/SSL ハードウェアアクセラレーションが導入されました。	6.2.3	6.2.3	特定の管理対象デバイス モデルでは、パフォーマンスが向上する、ハードウェアでの TLS/SSL 暗号化および復号が実行されます。デフォルトでは、この機能は有効です。 影響を受ける画面：TLS/SSL ハードウェア アクセラレーションのステータスを表示するには、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）]**、[全般（General）] ページ。
カテゴリとレピュテーションの条件がサポートされています。	6.2.2	6.2.2	カテゴリ/レピュテーションの条件を使用したアクセス コントロール ルールまたは SSL ルール。
セーフサーチをサポート	6.1.0	6.1.0	SSL ポリシーにより復号され、その後アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションによりブロック（またはインタラクティブにブロック）された接続については、HTTP 応答ページが表示されます。このような場合、システムは応答ページを暗号化して、再暗号化された SSL ストリームの最後にそれを送信します。 SafeSearch により好ましくないコンテンツがフィルタリングされ、成人向けサイトの検索が停止されます。
TLS/SSL ポリシー	6.0.0	6.0.0	導入された機能。

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。