Cisco FirePOWERへの SSLインサイト構築ガイド

目次

概要

暗号化されたトラフィックが増加し、SSLで利用する暗号鍵長がさらに長くなり、SSL暗号がより複雑になったことから、インラインセキュリティデバイスによるSSLトラフィックの復号化は一層困難になっています。このガイドでは、Cisco FirePOWERとともにA10 Networks® Thunder® CFW（Convergent Firewall）/SSL Insight®（SSLi®）アプライアンスを導入する際の構成について詳しく説明します。A10のSSLインサイトテクノロジーを利用すると、企業防御におけるSSLの盲点を排除することが可能になると同時に、プレーンテキストだけでなく暗号化されたトラフィックもセキュリティデバイスで検査できるようになります。このSSL復号化/検査ソリューションはレイヤー2環境を基盤としています。このソリューションは、アプリケーションデリバリーパーティション（ADP）を使用して複数の論理インスタンスを作成することで、1台のThunder CFW/SSLiアプライアンスでの導入が可能です。

SSLインサイトテクノロジー

このガイドでは、1台のThunder CFW/SSLiアプライアンスを使用してSSLインサイトを構成し、1つのパーティションでSSLトラフィックの復号化、もう1つのパーティションでトラフィックの再暗号化を行う方法について説明します。以下、アウトバウンドSSLトラフィックを復号化するパーティションを「内部パーティション」、アウトバウンドSSLトラフィックを暗号化するパーティションを「外部パーティション」と記述します。SSLインサイトは次のように動作します。

- クライアントから暗号化されたトラフィックが送信される。
- 内部パーティションによってトラフィックがインターセプトされて復号化され、プレーンテキストのコンテンツがCisco FirePOWERアプライアンスにリダイレクトされる。
- Cisco FirePOWERがプレーンテキスト形式のデータを検査し、次のホップのルーターに転送する。
- 外部パーティションがこのトラフィックをインターセプトし、暗号化。この時点で次のことが行われます。
  - 暗号化セッションがリモートサーバーに作成される。
  - クライアントのMedia Access Control（MAC）がこのセッション用に保存される。
  - アウトバウンドトラフィックがデフォルトゲートウェイに転送される。
- リモートサーバーが暗号化された要求を受信する。
- リモートサーバーが暗号化された応答を送信する。
- 外部パーティションが応答を復号化し、プレーンテキストのトラフィックをセキュリティデバイスに転送する。この時点で次のことが行われます。
  - セッションのマッチングが行われ、ソースMACアドレスが取得される。
  - トラフィックがクライアントMACアドレスに送信される。
- リモートサーバーから戻されたトラフィックがCisco FirePOWERアプライアンスに送信され、詳しい検査が行われる。Thunder CFW/SSLiで複数のFirePOWERアプライアンスの負荷分散を行っている場合、アウトバウンド要求の検査を行ったアプライアンスにインバウンドのトラフィックが転送される。
- 内部パーティションがCisco FirePOWERからプレーンテキストのトラフィックを受信し、これを暗号化してクライアントに送信する。
- クライアントが暗号化された応答を受信する。

導入の要件

SSLインサイトソリューションをCisco FirePOWERとともに導入するには、以下が必要です。

- A10 Networks Advanced Core Operating System（ACOS®）4.0.1ビルド214以上（ハードウェアベースのThunderアプライアンスでサポート）
- Cisco FirePOWER 4.5.1.1以上（ハードウェアベースのCisco FirePOWERアプライアンスでサポート）
- Cisco FirePOWERセンサー
- Cisco FirePOWER Defense Management Center（必須）

注：*このソリューションはレイヤー2モードで導入されます。*

導入モード

A10は、単一デバイスのトポロジーでSSLインサイト機能を導入することを推奨しています。アプリケーションデリバリーパーティション（ADP）を使用することで、1台のThunder CFW/SSLiアプライアンスを「内部」および「外部」パーティションに分離できます。A10 Thunder CFW/SSLiアプライアンスは、デバイスあたり32から1,023のADPをサポートできます（モデルにより異なります）。このSSLインサイトソリューションを機能させるためには2つ以上のパーティションが必要です。

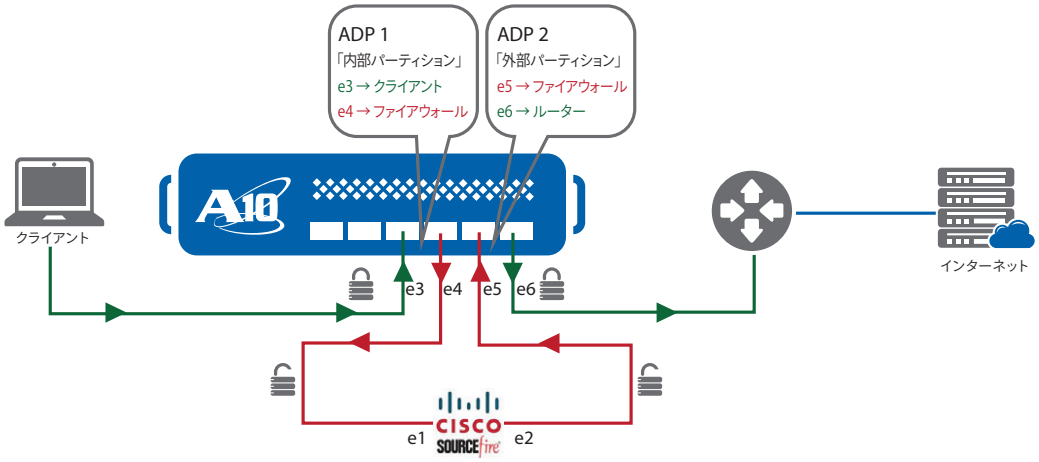

図1：1台のアプライアンスへのSSLインサイトの導入

導入時の考慮事項：

- アプライアンスベースのCisco FirePOWERセンサーの導入は、レイヤー2透過モードでのみサポートされています。
- 単一デバイスのソリューション内のインターフェイスポート数に制限されます。
- シスコのセンサーを管理するためにCisco FirePOWER Management Centerが必要です。各Cisco FirePOWER Management Centerは最大25センサーをサポートできます。
- ポリシーはパケット検査ソリューションごとに異なるため、このガイドではCisco製アプライアンスのインターフェイス構成のみを説明します。

その他の導入オプションについては、付録B（マルチデバイス導入の詳細）を参照してください。

Thunder CFW/SSLiへのアクセス

このセクションでは、Thunder CFW/SSLiアプライアンスへのアクセス方法を説明します。Thunder CFW/SSLiには、コマンドラインインターフェイス（CLI）またはグラフィカルユーザーインターフェイス（GUI）のいずれかからアクセスできます。

- CLI
  - コマンドラインにコマンドを入力するテキストベースのインターフェイス。CLIには、シリアルコンソールから直接、または以下のプロトコルを使用しネットワークを介してアクセスできます。
    - › 安全なプロトコル – Secure Shell（SSH）バージョン2
    - › 保護されていないプロトコル – Telnet（有効化されている場合、推奨はしません）
- GUI
  - クリック操作で構成ページや管理ページにアクセスし、デバイスの構成や管理のために値を入力または選択できるWebベースのインターフェイス。GUIには以下のプロトコルを使用してアクセスできます。
    - › 安全なプロトコル – HTTPS（Hypertext Transfer Protocol over Secure Socket Layer）

***注：**HTTP要求は、Thunder CFW/SSLiデバイス上ではデフォルトでHTTPSにリダイレクトされます。*

- デフォルトユーザー名：**admin**
- デフォルトパスワード：**a10**
- デバイスのデフォルトIPアドレス：**172.31.31.31**

Thunder CFW/SSLiアプライアンスへのアクセス方法の詳細については、『Thunder System Configuration and Administration Guide [1]』を参照してください。

***注:** 2台のアプライアンスを使用してSSLインサイトを導入する場合は、両方のシステムに管理アドレスを構成するようにしてください。*

Thunder CFW/SSLiでのパーティションの構成方法

このセクションの内容は、1台のアプライアンスでSSLインサイトを導入する場合のみを対象としています。2台のアプライアンスを導入する場合（SSLトラフィックの復号化用とSSLトラフィックの暗号化用に1台ずつアプライアンスを導入する場合）は、このセクションをスキップしてください。1台のアプライアンスに導入する場合は、キャパシティと同様に、プラットフォームに割り当てられているインターフェイス数に制限がありますので注意してください。

パーティションを作成するには、GUIの右上隅の部分にマウスポインターを移動して[**Partition:shared**]の下のドロップダウンをクリックし、[**+Create**]を選択します。

パーティションを作成するには、Administratorアカウント権限が必要です。

パーティション名	**デバイスID**	**タイプ**
Internal	一意の数字	ADC
External	一意の数字	ADC

図2：パーティションの作成

1つのパーティションから別のパーティションに移動するには、右上隅の[Partition:"xxxx"]の下から適切なパーティションを選択します。

ADP構成に一般的に使用されるCLIコマンドの一部を紹介します。

- パーティションの作成：**SSLi(config)#partition Internal id 2 application-type adc**
- パーティションの切り替え：**SSLi(config)#active-partition Internal**
- 現在のアクティブなパーティション：Internal
- **SSLi[Internal](config)#**

SSLインサイトのパーティションを構成すると、Thunder CFW/SSLiアプライアンスには少なくともShared、Internal、Externalの3つのパーティションが存在しているはずです。

***注:** 設定時には適切なパーティション上で操作していることを確認してください。また、単一デバイスでSSLインサイトを導入するソリューションでMACアドレスの重複をサポートするために、Sharedパーティションで system ve-mac-scheme system-mac コマンドを実行する必要があります。*

ネットワーク構成

パーティションを構成したら、SSLインサイトソリューションの導入に必要なインターフェイスを選択します。このケースではL2モードが使用されているため、タグなしポートが必要です。この導入例では、内部のネットワークアドレスレンジに192.0.2.xを使用します。簡易な構成の場合、CLIによりポートを構成することを推奨します。

***注:** 以下に登場するイーサネット番号は、参照のために使用されています。*

[1] このガイドをダウンロードまたは表示するには、https://www.a10networks.com/support にアクセスしてください（サイトへの登録が必要です）。

インターフェイス割り当て

- イーサネット3 インターフェイスをクライアントネットワークに接続
- イーサネット4 インターフェイスを Cisco FirePOWER (ingress) に接続
- イーサネット5 インターフェイスを Cisco FirePOWER (egress) に接続
- イーサネット6 インターフェイスをパブリックネットワークに接続

注: *図1を参照してください。*

内部パーティション (Internal パーティション) の構成

```
vlan 100
  untagged ethernet 3
  untagged ethernet 4
  router-interface ve 100
interface ve 100
  enable
  ip address 192.0.2.1 255.255.255.0
  ip allow-promiscuous-vip
```

注: ip allow-promiscuous-vip *コマンドは、ワイルドカード仮想IP (VIP) 0.0.0.0を使用するすべての構成で必要です。このコマンドを使用すると、このインターフェイスで受信される任意のポートにアドレス指定されたクライアントトラフィックを、任意のVIPアドレスに負荷分散できます。*

外部パーティション (External パーティション) の構成

```
vlan 101
  untagged ethernet 5
  untagged ethernet 6
  router-interface ve 101
interface ve 101
  enable
  ip address 192.0.2.2 255.255.255.0
  ip allow-promiscuous-vip   (外部パーティションの構成にも必要)
```

導入前の要件

このセクションでは、単一アプライアンスでSSLインサイトを構成する方法を説明します。

内部パーティション (Internal パーティション) の要件

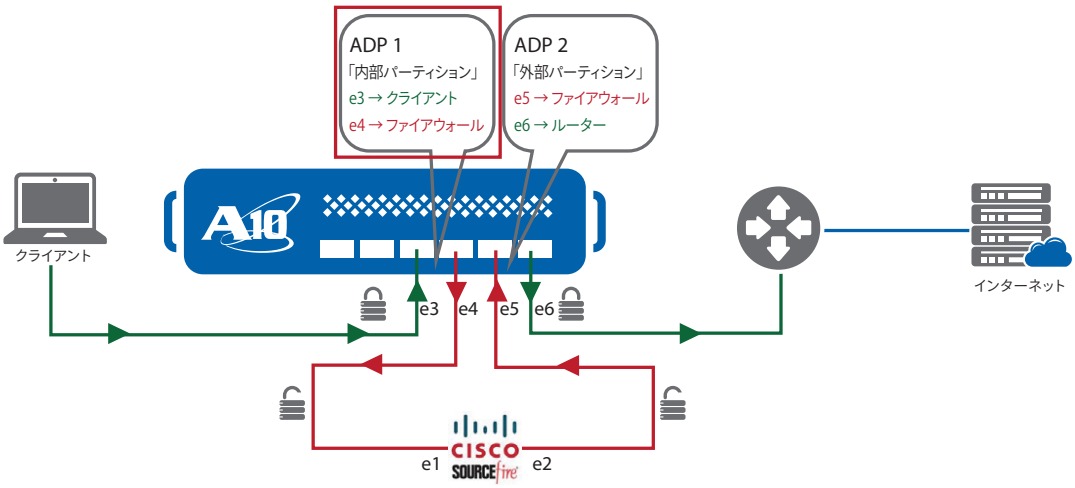

図3: 内部パーティションの実装

[2] このガイドを表示またはダウンロードするには、https://www.a10networks.com/sites/default/files/A10-DG-16140-EN.pdf にアクセスしてください。

- Thunder CFW/SSLiで自己署名付き証明書と秘密鍵を作成するか、既知の認証局（CA）証明書と秘密鍵をインポートします。
- **forward-proxy-enable**が設定されたclient-sslテンプレートを作成します。
- インターセプトされるすべてのTCPまたはUDPトラフィック用のアクセス制御リスト（ACL）をワイルドカードVIPに設定し、対象となるトラフィックを定義しておく必要があります。正しいソースIPアドレスおよび宛先IPアドレスを使用してACLを作成したら、VIP内でこのACLを適用します。
- CA証明書をすべてのクライアントマシンにプッシュ配信する必要があります。これにより、リモートサーバーへのSSLセッションを作成したときに、クライアントが内部パーティションから自己署名付き証明書を受理できるようになります。CA証明書を作成し、作成した証明書をMicrosoft WindowsマシンおよびGoogle Chrome/Mozilla Firefoxブラウザーにインポートする方法の詳細については、『SSL Insight Certificate Installation Guide[2]』を参照してください。
- ポート443へのSSLトラフィックをインターセプトするために、ワイルドカードVIP内にポート443を定義する必要があります。
- HTTPS（443）からHTTP（8080）に宛先を変更するため、サービスグループをポート8080で定義し、仮想ポート（443）にバインドする必要があります。
- **no-dest-nat port-translation**コマンドを使用して、宛先IPをそのまま維持し、ポート番号のみ宛先ポートに変更（内部から外部へプレーンテキストトラフィックを送信するためにポート8080に変更）する必要があります。
- インターセプトされて復号化される受信SSLセッションは、HTTP（ポート8080）を介してプレーンテキストとしてCisco FirePOWERに転送されます。

外部パーティション（External パーティション）の要件

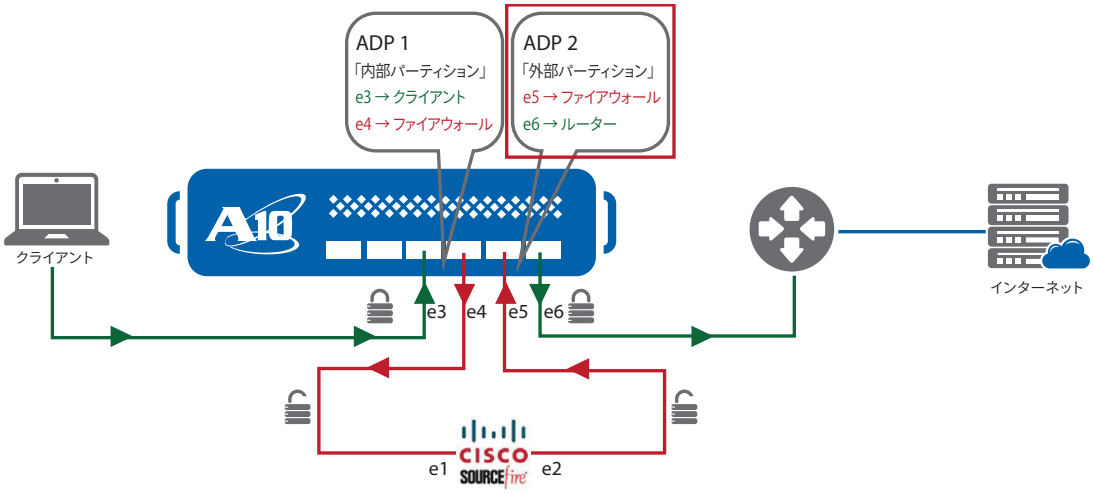

図4：外部パーティションの実装

- ワイルドカードVIPを使用して、ポート8080のクリアテキストHTTPトラフィックが外部パーティションによってインターセプトされます。
- インターセプトされるすべてのTCPまたはUDPトラフィック用のアクセス制御リストをワイルドカードVIPに設定し、対象となるトラフィックを定義しておく必要があります。正しいソースIPアドレスおよび宛先IPアドレスを使用してACLを作成したら、VIPにこのACLを適用します。
- ネクストホップゲートウェイ（デフォルトルート）を、サーバー負荷分散サーバー（ポート443）として定義します。
- Cisco機器から転送されるすべてのプレーンテキストのHTTPトラフィックは、HTTPSトラフィック（ポート443）に変換されます。サービスグループは、ポート443で構成する必要があります。
- **no-dest-nat port-translation**コマンドを使用して、宛先IPをそのまま維持する必要があります。またこのコマンドによって、TCPポート8080で受信したトラフィックがHTTPSポート443に変換されます。
- server-sslテンプレートでは、**forward-proxy-enable**を設定しておく必要があります。
- **use-rcv-hop-for-resp**コマンドによって、すべての受信トラフィックのソースMACアドレスが保持されるため、トラフィックは送信元と同一のセキュリティデバイスに送信されます。

[3] このガイドをダウンロードするには、https://www.a10networks.com/support にアクセスしてください（サイトへの登録が必要です）。

***注:** 自己署名付き証明書の作成やThunder CFW/SSLiアプライアンスへのCA証明書のインポート方法の詳細については、A10の『Thunder SSL Configuration Guide [3]』を参照してください。*

CLIでclient-sslテンプレートを作成するには、以下のコマンドを入力します。

```
slb template client-ssl SSLInsight_clientside
  forward-proxy-ca-cert ssli-inside-cert
  forward-proxy-ca-key ssli-inside-key
  forward-proxy-enable
```

***注:** 同一の証明書を信頼されるCA証明書としてすべてのクライアントにインストールする必要があります。*

forward-proxy-enableコマンドにより、client-sslまたはserver-sslテンプレートでSSLインサイトが有効化されます。client-sslテンプレートをGUIで作成するには、[**ADC > Templates > SSL**]の順にマウスポインターを操作してから[**+Create**]をクリックし、[**Client SSL**]を選択します。

***注:** ここでは、SSL証明書が作成済みでThunder CFW/SSLiアプライアンスにインポート済みであることを前提としています。このガイドでは、この証明書を **ssli-inside-cert** と呼びます。*

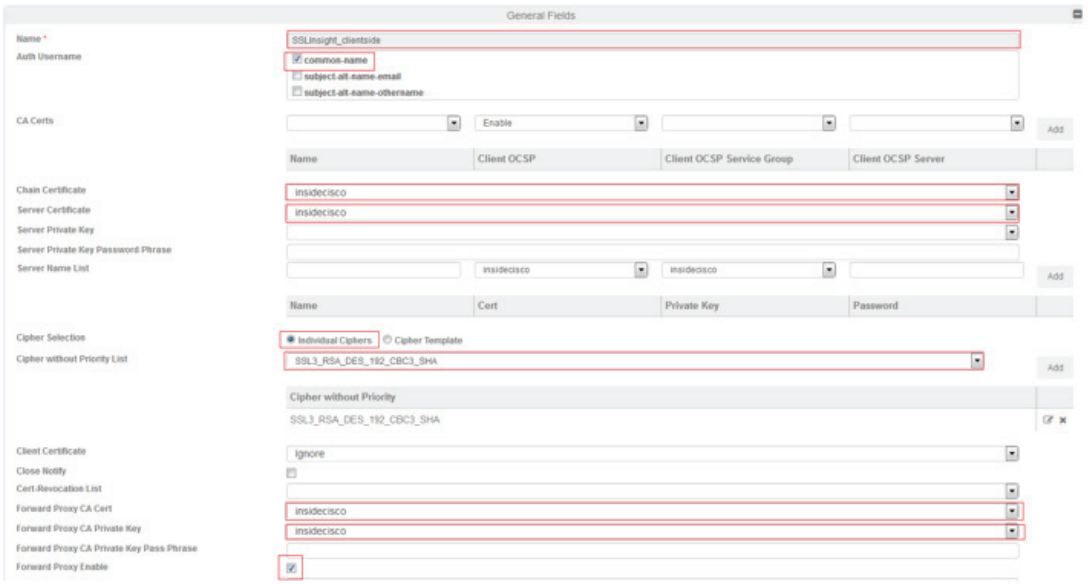

図5：client-sslテンプレート

A10 Networksによる Cisco FirePOWER導入ソリューション

前のセクションで説明した通り、SSLインサイトソリューションを導入するには、2つのパーティションが必要です。このセクションでは、内部パーティションと外部パーティションの構成方法を説明します。

内部パーティションの構成

内部パーティションは、SSLトラフィックを復号化し、検査を実施するCisco FirePOWERにプレーンテキストを送信する役割を果たします。プレーンテキストのトラフィックは、Cisco FirePOWERのingressポートに送信されます。

内部パーティションの設定には、以下のコマンドを実行します。

ACLの構成：

```
access-list 100 permit ip x.x.x.0 0.255.255.255 any vlan 100 log
```

[3] このガイドをダウンロードするには、https://www.a10networks.com/support にアクセスしてください（サイトへの登録が必要です）。

サーバーの構成：

```
slb server gateway 192.0.2.10
   health-check-disable
   port 0 tcp
     health-check-disable
   port 0 udp
     health-check-disable
   port 8080 tcp
     health-check-disable
```

tcp、udp、othersのワイルドカード仮想ポートにより、許可されたすべてのトラフィックがワイルドカードVIPの対象トラフィックとして扱われます。

- これらのワイルドカード仮想ポートが必要な理由を以下に示します。
  - tcpワイルドカード仮想ポートは、非SSLトラフィックの負荷分散に加え、新しいリモートサイトからのSSL証明書のフェッチのために内部パーティションで使用されます。
  - udpワイルドカード仮想ポートは、DNS要求/応答などのすべてのUDPトラフィックで使用されます。
  - othersのワイルドカード仮想ポートは、ICMPエコーやエコー応答など、すべての非TCP/非UDPトラフィックで使用されます。

GUIでサーバーを構成するには、[**ADC > SLB > Servers**]の順にマウスポインターを操作し、[**+Create**]をクリックします。

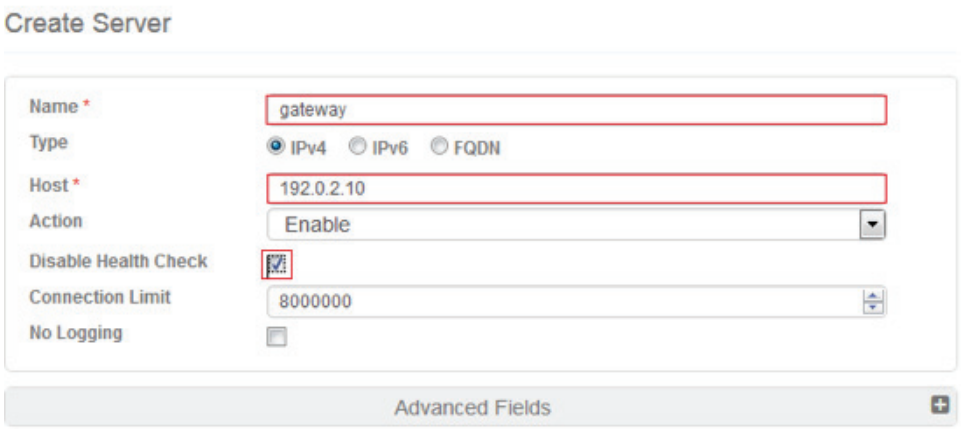

図6：サーバーテンプレート

サーバーポートの構成：

サーバーのポートセクションで、以下を追加します。

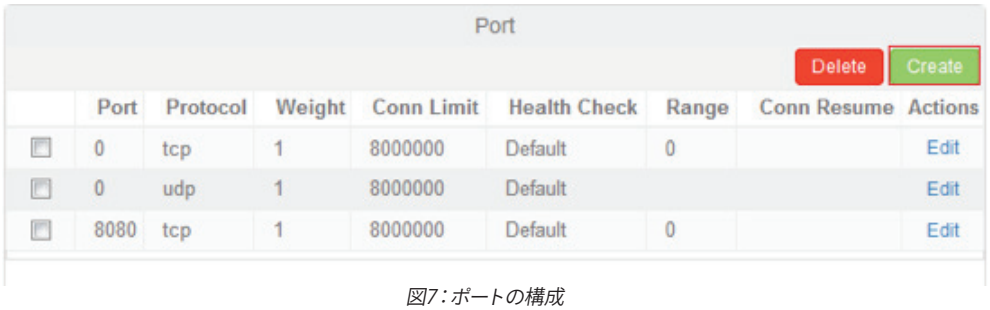

図7：ポートの構成

サーバーポートを構成したら、サーバーグループ/プールと必要なサーバーを作成します。このガイドでは、プール内にあるのは1つのCisco FirePOWERのみですが、必要に応じてサーバーを追加できます。サーバーグループは、容易に管理できるように、ポート番号とプロトコルの詳細情報に応じた名前を付けることが推奨されます。

```
slb service-group gateway_tcp_0 tcp
  member gateway 0
!
slb service-group gateway_tcp_8080 tcp
  member gateway 8080
!
slb service-group gateway_udp_0 udp
  member gateway 0
```

GUIでサービスグループを構成するには、**[ADC > SLB > Service Groups]**の順にマウスポインターを操作し、[**+Create**]をクリックします。

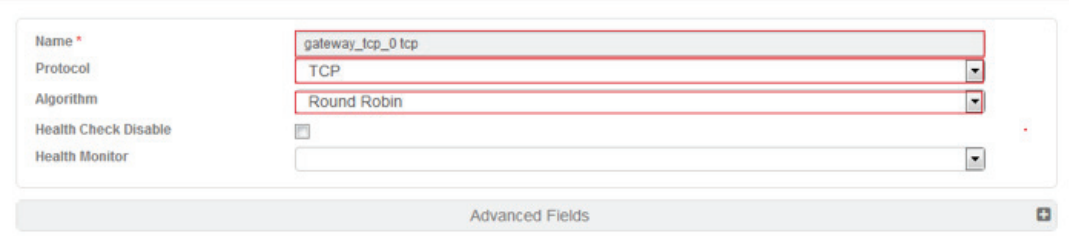

図8：サービスグループの構成

サービスグループへのサーバーメンバーの追加：

サービスグループにサーバーを追加するには、GUIの右側にある[**Create**]をクリックします。正しいサーバー名とポート（ポート0 TCP、ポート0 UDP、ポート8080 TCP）を入力する必要があります。

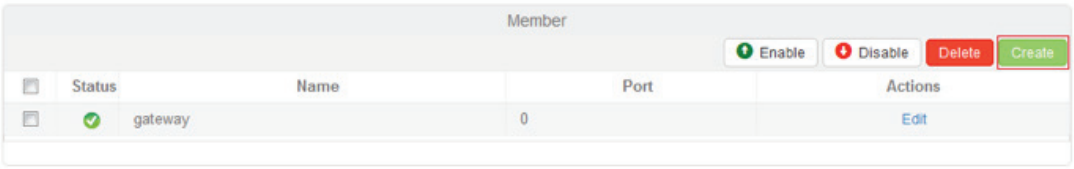

図9：サーバーメンバーの構成

仮想サーバーの構成：

VIPを設定するには、以下のCLIコマンドを使用します。

```
slb virtual-server inbound_to_cisco 0.0.0.0 acl 100
   port 0 tcp
      name to_gw_tcp
      service-group gateway_tcp_0
      use-rcv-hop-for-resp
      no-dest-nat
   port 0 udp
      name to_gw_udp
      service-group gateway_udp_0
      use-rcv-hop-for-resp
      no-dest-nat
   port 0 others
      name to_gw_others
      service-group gateway_udp_0
      use-rcv-hop-for-resp
      no-dest-nat
   port 443 https
      name internal_in_to_out_443
      service-group gateway_tcp_8080
      template client-ssl SSLInsight_clientside
      use-rcv-hop-for-resp
      no-dest-nat port-translation
```

仮想サーバー構成を作成するには、[**ADC > SLB > Virtual Servers**]の順にマウスポインターを操作し、[**+Create**]をクリックします。

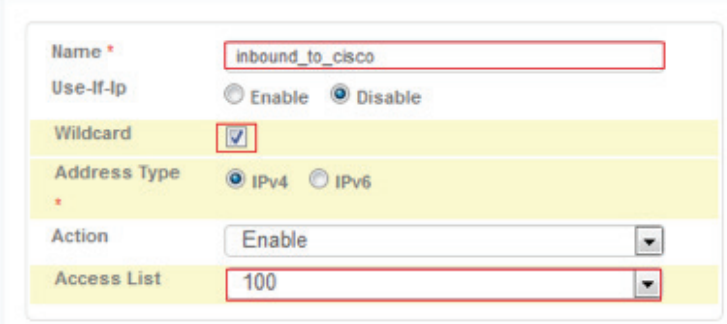

図10：仮想サーバーの構成

仮想ポート構成で、ポート番号0 TCPおよびポート番号0 UDPを設定し、対応するサービスグループを指定します。各仮想ポートで「**no-dest-nat**」を使用する必要があります。仮想ポート443ではHTTPSを使用します。

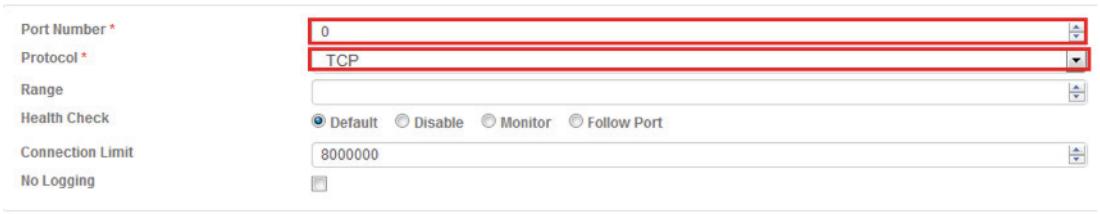

図11：仮想サーバーポートのオプション

次に仮想ポートの確認を行います。確認が完了すると仮想ポートは次のようになります。[Update]をクリックして、操作を続行します。

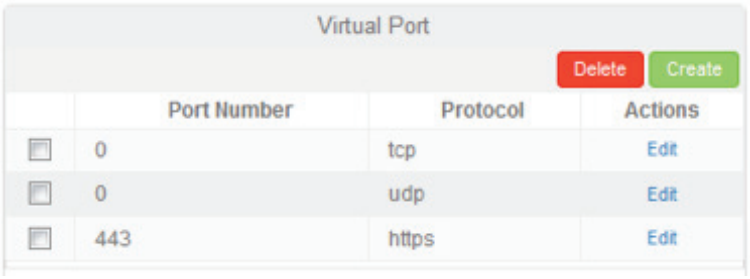

図12：仮想ポートの構成

外部パーティション（External パーティション）の構成

外部パーティションは、Cisco FirePOWERのegressポートから出力されるポート番号8080のトラフィックの暗号化を行います。外部パーティションがトラフィックを受信すると、プレーンテキストのトラフィックがHTTPS/443に向けて暗号化され、デフォルトのルーター/インターネットに送信されます。

構成前の要件：

最初の手順はserver-sslテンプレートの準備と、このテンプレート内での**forward-proxy**機能の有効化です。CLIでserver-sslテンプレートを作成するには、以下のコマンドを使用します。

```
slb template server-ssl OutsideSSL
  forward-proxy-enable
```

GUIでは、[**ADC > Templates > SSL**]の順にマウスポインターを操作し、[**+Create**]をクリックします。

サーバーSSL名を入力し、[**SSL Forward Proxy**]を有効化します。このSSLテンプレートが、仮想サービスポートにバインドされます。

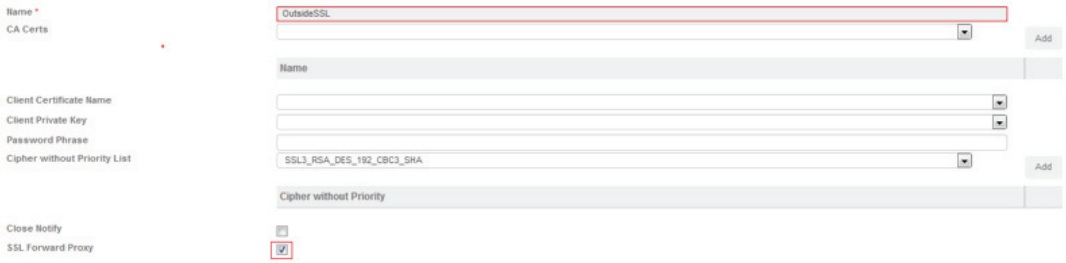

図13：SSL forward proxyの構成

ACLの構成：

アクセス制御リストを構成するには、以下のCLIコマンドを使用します。

```
access-list 101 permit ip x.x.x.0 0.255.255.255 any vlan 101 log
```

次の手順は、サーバーロードバランシング対象となるサーバーの構成です。通常このサーバーは、インターネットまたはサーバーに接続するルーター上にあります。CLIを使用して、以下のようにサーバーのIPアドレスおよびポート番号を設定する必要があります。

```
slb server Default_Gateway 20.1.1.10
  health-check-disable
  port 443 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 0 tcp
    health-check-disable
```

GUIで構成するには、[**ADC > SLB > Server**]の順にマウスポインターを操作し、[**+Create**]をクリックします。

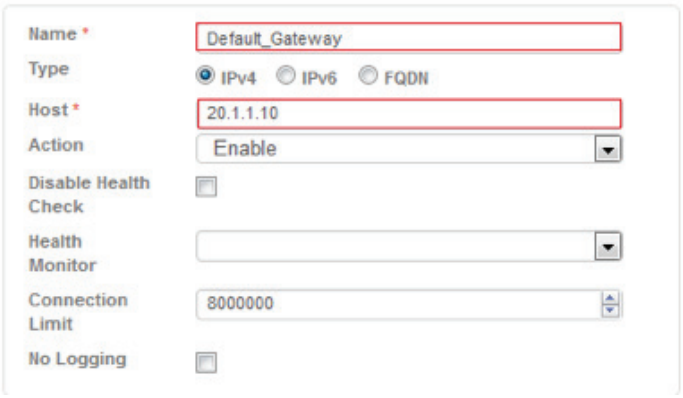

図14：サーバーの負荷分散の構成

サービスグループの構成：

次の手順は、サービスグループへのサーバーの追加手順になります。

サービスグループにサーバー/ポート構成を追加するには、以下のCLIを使用します。

```
slb service-group DG_TCP tcp
  member Default_Gateway 0

slb service-group DG_UDP udp
  member Default_Gateway 0

slb service-group DG_SSL tcp
  member Default_Gateway 443
```

GUIを使用してサービスグループを構成するには、[**ADC > SLB > Service Groups**]の順にナビゲートし、[**+Create**]をクリックします。名前とプロトコルを入力し、メンバーセクションにサーバー名を追加します。TCP、UDP、およびSSLのサービスグループを構成する必要があります。

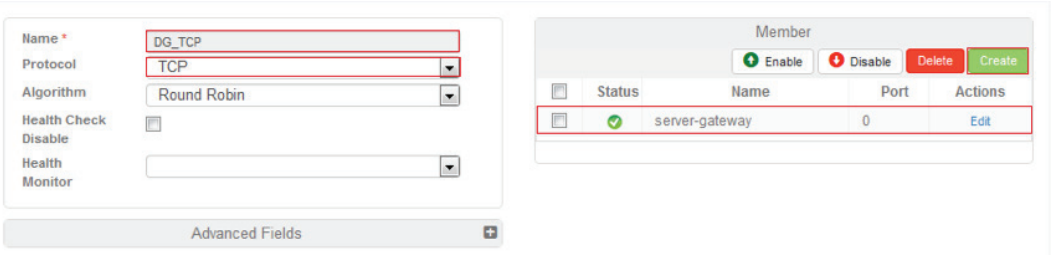

図15：サービスグループの構成

仮想サーバーの構成：

仮想サーバーの構成では、port 0 TCP、port 0 UDP、port 0 others（その他のすべてのトラフィック）、および port 8080 http の4つの仮想ポートセットが必要です。また、前章で事前に構成した server-ssl をポート 8080 にバインドします。さらに、宛先 IP アドレスが変更されないように **no-dest-nat port-translation** コマンドを使用する必要があります。

```
slb virtual-server SSLi-Wildcard 0.0.0.0 acl 101
   port 0 tcp
     no-dest-nat
     service-group DG_TCP
     use-rcv-hop-for-resp
   port 0 udp
     no-dest-nat
     service-group DG_UDP
     use-rcv-hop-for-resp
   port 0 others
     no-dest-nat
     service-group DG_UDP
     use-rcv-hop-for-resp
   port 8080 http
     no-dest-nat port-translation
     service-group DG_SSL
     use-rcv-hop-for-resp
     template server-ssl OutsideSSL
```

GUIで仮想サーバーを構成するには、[**ADC > SLB > Virtual Servers**]の順にマウスポインターを操作し、[**+Create**]をクリックします。

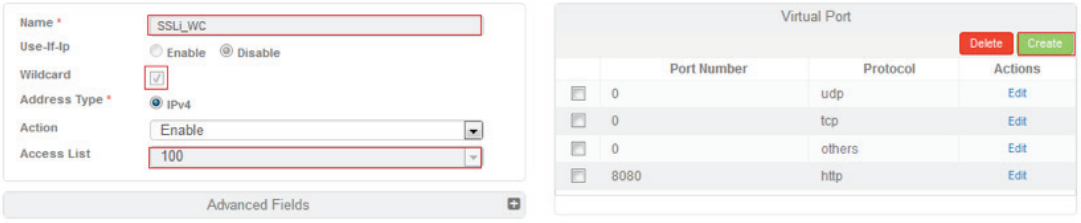

図16：仮想サーバーの構成

URLクラシフィケーションの構成：

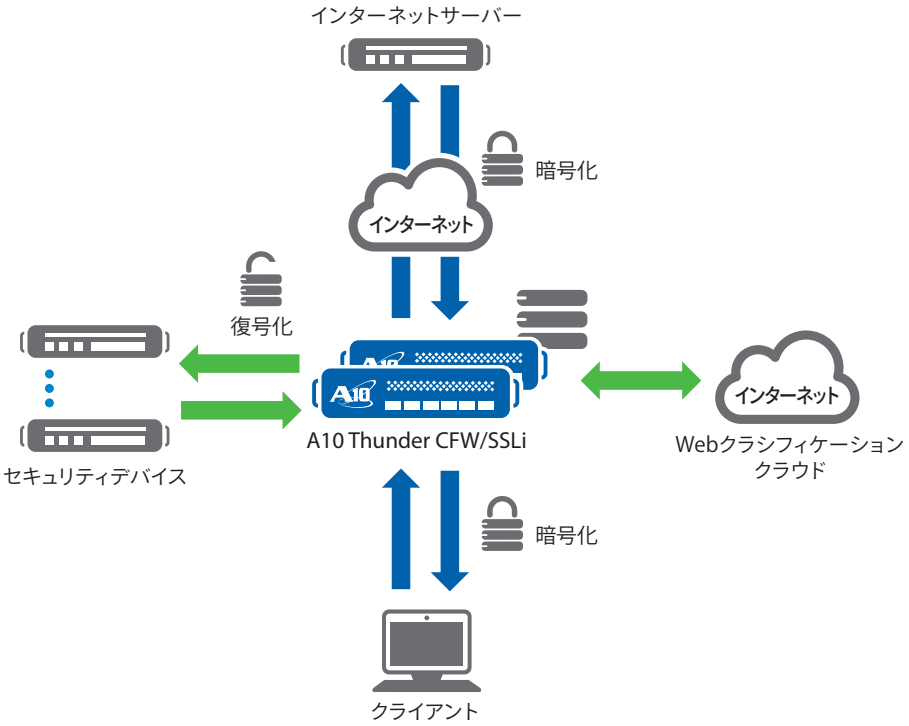

図17：A10とWebrootのアーキテクチャー

SSLインサイトテクノロジーには、「A10 URLクラシフィケーションサービス」と呼ばれるWebroot BrightCloudの有料サブスクリプションサービスを追加できます。このサービスにより、お客様は復号化するSSLトラフィックのタイプや、検査を行わずに転送する通信のタイプをきめ細かく制御できます。Thunder CFW/SSLiをご利用のお客様は、SSLトラフィックを分析して保護する一方で、バンキングアプリケーションや医療アプリケーションなどの機密性の高いサイトへの通信を分析対象外とすることができます。

本サービス利用時には、ユーザーのクライアントブラウザーがURLに要求を送信するとURLカテゴリーがチェックされます。

- URLカテゴリーが構成上バイパス許可されている場合、SSLインサイトの内部パーティションは暗号化データをそのままSSLインサイト外部パーティションに送信します。外部パーティションは暗号化されたデータをサーバーに送信します。
- URLカテゴリーが構成上バイパス許可されていない場合、SSLインサイトの内部パーティションはトラフィックを復号化してトラフィック検査デバイスに送信します。

インストールの要件：

- 各Thunder CFW/SSLiにおいて、A10 URLクラシフィケーションサブスクリプションを利用している必要があります（費用については、営業担当にお問い合わせください）。
- Thunder CFW/SSLiの内部パーティションが、BrightCloud内のWebカテゴリーデータベースサーバーにアクセスするために、インターネットにアクセスできる必要があります。
- DNS構成が必要です。

URLクラシフィケーション機能をインストールするには、A10 Global License Manager（GLM）で作成されたURLクラシフィケーショントークンライセンスが必要です。このライセンスを受領したら、以下のコマンド（CLIでのみ設定可能）を開始します。

```
SSLi(config)#internal Imp.ort web-category-license "license token name"
```

ライセンスがインポートされたら、**web-category enable**コマンドを実行します。この機能により、Thunder CFW/SSLiデバイスはWebカテゴリーデータベースサーバーと通信し、URLクラシフィケーションデータベースをダウンロードできるようになります。ダウンロードが完了すると、インポートが正常に行われた場合は「Done」メッセージが表示されます。それ以外の場合はエラーメッセージが表示されます。

```
SSLi(config)#import web-category-license license use-mgmt-port scp://
example@10.100.2.20/home/jsmith/webroot_license.json
Done.                    <--   これはライセンスが正常にインポートされたことを示す確認メッセージです。
```

障害が発生すると、以下のようなエラーメッセージが表示されます。

```
SSLi(config)# import web-category-license license use-mgmt-port scp://
example@10.100.2.20/home/jsmith/webroot_license.json
Communication with license server failed     <-- これはインポートの失敗を示すメッセージです。
```

注:*Webroot データベースはデフォルトでデータインターフェイスからのダウンロードを行います。管理インターフェイスからのダウンロードを構成できるオプションもありますが、このオプションは推奨していません。*

WebrootによるURLクラシフィケーション機能を有効化するには、client-sslテンプレートで以下の設定を行う必要があります。

設定例:

```
forward-proxy-enable
forward-proxy-bypass web-category financial-services
forward-proxy-bypass web-category business-and-economy
forward-proxy-bypass web-category health-and-medicine
```

Explicit Proxy(明示的プロキシ)の構成

Explicit Proxy機能により、Thunder CFW/SSLiデバイスは、許可されているトラフィックの送信元(クライアント)と宛先(ホスト)のリストに基づいてクライアントからホストへのアクセスを制御できます。

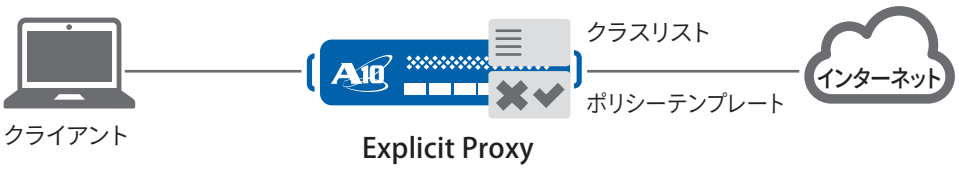

図18:Explicit Proxyのトポロジー

この機能は、ACOSリリース2.7.2およびACOSリリース4.0.1 SP9で実装されました。この機能を有効にすると、Thunder CFW/SSLiデバイスのHTTP仮想ポートでクライアントからのHTTP要求をインターセプトし、送信元と宛先両方を検証し、送信元と宛先が有効な要求のみを転送し、許可された宛先に送信することができます。宛先は、URLまたはホスト名文字列に基づいて検証されます。許可されている宛先は、DNSを使用してIPアドレスが取得されます。

Explicit Proxyの構成例については、付録Cを参照してください。高度なExplicit Proxyソリューションの構成方法の詳細は、『A10 Thunder Application Delivery and Server Load Balancing Guide [4]』を参照してください。

[4] このガイドをダウンロードするには、https://www.a10networks.com/support にアクセスしてください(サイトへの登録が必要です)。

Cisco FirePOWERの構成

Cisco FirePOWERインスタンスにアクセスするには、Webブラウザーを使用し、HTTPSを使用して管理IPにアクセスします。

デフォルトのアクセス方法：

- ユーザー名：**admin**
- パスワード：**Admin123**

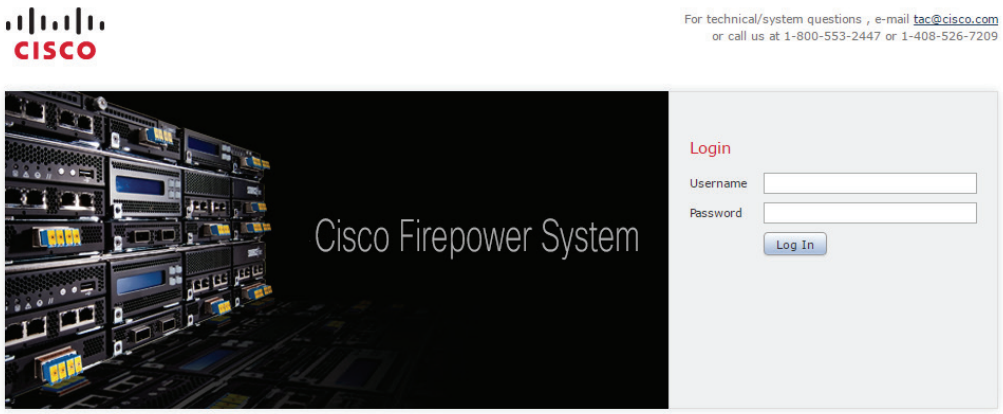

図19：FirePOWERログインポータル

シスコセンサーの導入時に、インターフェイスをインラインモードに設定するようにしてください。

インターフェイスの設定と検証を行うには、[Devices > Device Management > Interfaces]の順にマウスポインターを操作します。インターフェイスが[Default Inline Set]として設定されていることを確認してください。Thunder CFW/SSLiデバイスとCisco FirePOWERの連携では、このインターフェイス設定のみサポートされています。

図20：デバイスインターフェイスの設定

Cisco FirePOWERが機能するには、シスコセンサーに一致するNetwork Time Protocol（NTP）設定が必要です。CiscoのNTPを構成するには、[**System > Local Policy > Time Synchronization**]の順にマウスポインターを操作します。[**Serve via NTP Time**]セクションで[**Enabled**]を選択したら、使用するNTPサーバーを選択します。

図21：Cisco FirePOWERのNTP構成

FirePOWERに新しいデバイスを追加するには、ポータル右上隅の[**Add**]をクリックし、[**new device**]を選択します。

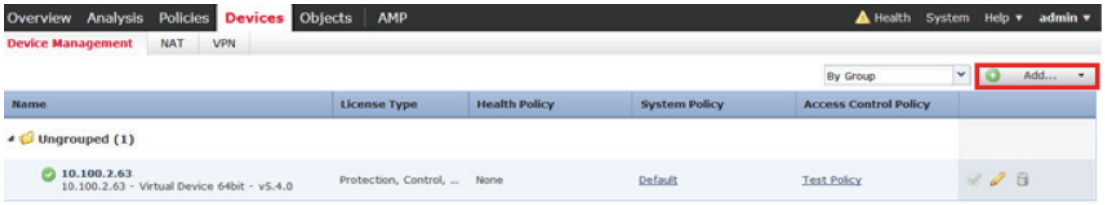

図22：Cisco FirePOWERシステムポータルでのデバイスの追加

[**Add Device**]セクションで、以下のように入力します。

- Host：シスコセンサーのIPアドレス
- Registration Key：FirePOWERにデバイスを登録するための一意の識別子
- Access Control Policy：[Policy]タブ内で作成された事前構成済みのアクセスポリシー。企業によってセキュリテイポリシーは異なるため、アクセスポリシー構成はさまざまです。

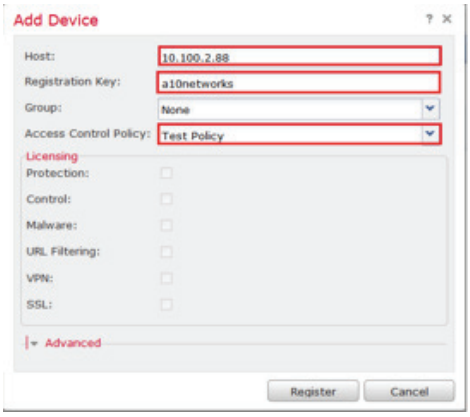

図23：デバイスの構成

Cisco FirePOWERシステムのライセンス

Cisco FirePOWERのライセンスを取得するには、[**System > Add New System License**]の順にマウスポインターを操作します。以下の例では、ライセンスキー「66:00:0C:29:4B:9D:E6」をコピーする例です（ライセンスを生成するにはライセンスキーが必要です）。ライセンスキーが生成されたら、ライセンスをカットアンドペーストし、[**Submit License**]をクリックします。

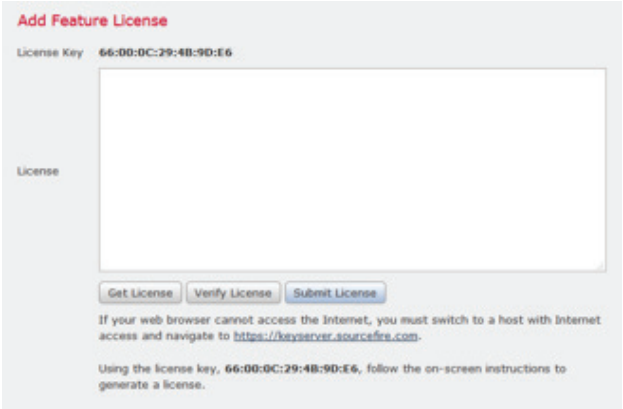

図24：ライセンスの追加

完了すると、図25のようなWebページが表示されます。

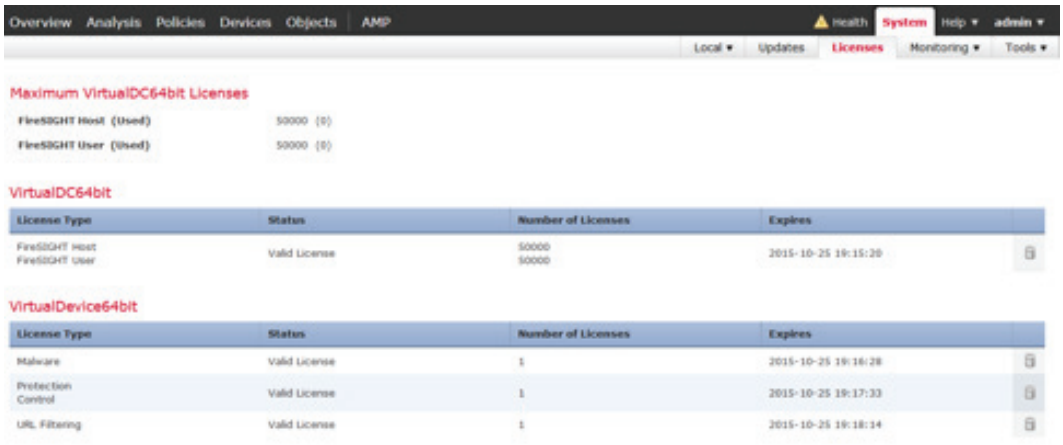

図25：ライセンス構成

まとめ

暗号化されたトラフィックが増加し、SSLで利用する暗号化鍵長がさらに長くなり、SSL暗号化の複雑化が進んでいるため、インラインセキュリティデバイスによるSSLトラフィックの復号化は難しくなっています。Cisco FirePOWERアプライアンスをはじめとする幅広いセキュリティデバイスは、攻撃、侵入、マルウェアを発見するために、暗号化されたトラフィックに対する可視性を必要としています。このガイドでは、Cisco FirePOWERとA10 Thunder CFW/SSLiを構成するために必要な手順を説明しました。 このガイドに記載されている手順を完了すると、SSLトラフィックを復号化する準備が整います。

A10 Thunder CFW/SSLiの標準機能として装備されているSSLインサイトテクノロジーは、負荷分散、高可用性、およびSSL復号化機能を提供する強力なソリューションを提供します。SSLインサイト機能を利用すると、次のことが可能になります。

- 暗号化されたデータを含むすべてのネットワークデータを分析し、脅威保護ソリューション内の盲点を排除する
- サードパーティ製セキュリティデバイスに高度なSSL検査機能とSSL復号化機能を提供する
- SSL/TLSを介して送信される暗号化されたマルウェア、内部者による悪質な活動、攻撃を検出する
- 業界最高レベルのコンテンツ検査ソリューションを導入してサイバー攻撃を回避する
- A10の64ビットACOS®（Advanced Core Operating System）プラットフォーム、Flexible Traffic Acceleration（FTA）テクノロジー、専用セキュリティプロセッサーを活用して、企業ネットワークのパフォーマンス、可用性、拡張性を最大限に高める

Thunder CFW/SSLi製品の詳細情報については、以下のWebサイトをご覧ください：

http://www.a10networks.co.jp/products/thunderseries/thunder-SSLi.html

http://www.a10networks.co.jp/download/solutionbrief/

http://www.a10networks.co.jp/case/

付録 A

オプションのトポロジー：SSLインサイト用アプライアンスを2台導入する場合は、1台のA10 Thunder CFW/SSLiアプライアンスでトラフィックを復号化し、2台目のThunder CFW/SSLiアプライアンスでトラフィックを暗号化します。

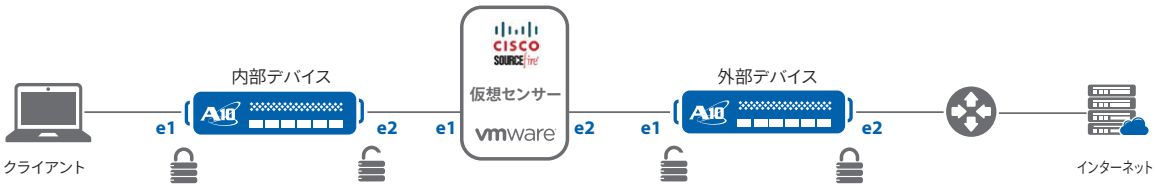

図26：マルチデバイス導入時のSSLインサイト

導入時の考慮事項：

- アプライアンスベースのセンサーの導入は、レイヤー2透過モードでのみサポートされています。
- ハードウェアベースのASAとシスコセンサーは、レイヤー2またはレイヤー3の導入がサポートされています。

付録 B

以下に、マルチデバイス構成に基づいた構成例を示します。

内部デバイス構成

```
!
multi-config enable
!
system promiscuous-mode
!
terminal idle-timeout 60
!
access-list 100 permit ip x.x.x.0 0.255.255.255 any vlan 77 log
ip dns primary 8.8.8.8
!
ip dns suffix a10lab.local
!
vlan 77
  untagged ethernet 1 to 2
  router-interface ve 77
!
hostname A10-SSL-Inside
!
timezone America/Los Angeles
!
interface management
  ip address 192.0.2.20 255.255.255.0
  ip control-apps-use-mgmt-port
  ip default-gateway 192.0.2.1
!
interface ethernet 1
  name A10-SSL-Client
  enable
!
interface ethernet 2
  name A10-Inside-Sourcefire
  enable
!
interface ve 77
  ip address 203.0.113.20 255.255.255.0
  ip allow-promiscuous-vip
```

```
!
ip route 0.0.0.0 /0 203.0.113.1
!
web-category
  enable
!
slb server gateway 203.0.113.1
  health-check-disable
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 8080 tcp
    health-check-disable
!
slb service-group gateway_tcp_0 tcp
  member gateway 0
!
slb service-group gateway_tcp_8080 tcp
  member gateway 8080
!
slb service-group gateway_udp_0 udp
  member gateway 0
!
slb template client-ssl ssli-client-template
  forward-proxy-ca-cert ssli-inside-cert
  forward-proxy-ca-key ssli-inside-key
  forward-proxy-enable
  forward-proxy-bypass web-category financial-services
  forward-proxy-bypass web-category business-and-economy
  forward-proxy-bypass web-category health-and-medicine
!
slb virtual-server SSLi-Wildcard 0.0.0.0 acl 100
  port 0 tcp
    no-dest-nat
    service-group gateway_tcp_0
    use-rcv-hop-for-resp
  port 0 udp
    no-dest-nat
    service-group gateway_udp_0
    use-rcv-hop-for-resp
  port 0 others
    no-dest-nat
    service-group gateway_udp_0
    use-rcv-hop-for-resp
  port 443 https
    no-dest-nat port-translation
    service-group gateway_tcp_8080
    use-rcv-hop-for-resp
    template client-ssl ssli-client-template
!
end
```

外部デバイス構成

```
!
multi-config enable
!
system promiscuous-mode
!
terminal idle-timeout 60
!
access-list 101 permit ip x.x.x.0 0.255.255.255 any vlan 77 log
!
ip dns primary 8.8.8.8
!
ip dns suffix a10lab.local
!
vlan 77
  untagged ethernet 1 to 2
  router-interface ve 77
!
hostname A10-SSL-Outside
!
timezone America/Los Angeles
!
interface management
  ip address 192.0.2.100 255.255.255.0
  ip control-apps-use-mgmt-port
  ip default-gateway 192.0.2.1
!
interface ethernet 1
  name A10-Outside-Sourcefire
  enable
!
interface ethernet 2
  name Datacenter-Services
  enable
!
interface ve 77
  ip address 203.0.113.30 255.255.255.0
  ip allow-promiscuous-vip
!
!
ip route 0.0.0.0 /0 203.0.113.1
!
slb template server-ssl SSLi
  forward-proxy-enable
!
!
slb server gateway 203.0.113.1
  health-check-disable
  port 0 tcp
    health-check-disable
  port 0 udp
    health-check-disable
  port 443 tcp
    health-check-disable
!
slb service-group default_gateway_tcp_0 tcp
  member gateway 0
!
```

```
 slb service-group default_gateway_tcp_443 tcp
   member gateway 443
 !
 slb service-group default_gateway_udp_0 udp
   member gateway 0
 !
 slb virtual-server SSLi-Wildcard 0.0.0.0 acl 101
   port 0 tcp
     no-dest-nat
     service-group default_gateway_tcp_0
     use-rcv-hop-for-resp
   port 0 udp
     no-dest-nat
     service-group default_gateway_udp_0
     use-rcv-hop-for-resp
   port 0 others
     no-dest-nat
     service-group default_gateway_udp_0
     use-rcv-hop-for-resp
   port 8080 http
     no-dest-nat port-translation
     service-group default_gateway_tcp_443
     use-rcv-hop-for-resp
     template server-ssl SSLi
 !
 end
```

付録C

以下にExplicit Proxyの構成例を示します。

クラスリストは、英語アルファベット26文字のいずれかを含む英字列にマッチします。文字列がマッチした場合に適切な宛先に転送されます。

```
class-list dest ac
  contains example
  contains google
  contains test
!
class-list dest1 ac
  contains example1
  contains america
!
class-list dest2 ac
  contains bank
  contains sample
!
class-list src ipv4
  192.0.2.212/32
  203.0.113.0/24
  198.51.100.0/24
!
slb server fake-server 192.168.230.101
  port 80 tcp
  port 443 tcp
    health-check-disable
!
slb server ubuntu_serv 192.168.221.70
  port 80 tcp
  port 443 tcp
```

```
slb service-group fake-sg tcp
  health-check-disable
  member fake-server 80
  member fake-server 443
!
slb service-group ubuntu_sg tcp
  member ubuntu_serv 80
  member ubuntu_serv 443
!
slb template policy test
  forward-policy
    action a1
      forward-to-internet fake-sg snat snat fallback ubuntu_sg snat snat
      log
    action a2
      forward-to-service-group ubuntu_sg snat snat
      log
    action a3
      drop
      log
    source s1
      match-class-list src
      destination class-list dest action a1 url priority 10
      destination class-list dest1 action a2 url priority 300
      destination class-list dest2 action a3 url priority 15
   source s2
      match-any
      destination any action a1
slb virtual-server test 10.50.10.123
  port 8080 http
    service-group fake-sg
    template policy test
!
```

注:*fake-server および fake-sg は、アクション forward-to-internet 用のプレースホルダーとして必要です。*

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はアプリケーションネットワーキングおよびセキュリティ分野におけるリーダーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。詳しくはホームページをご覧ください。

www.a10networks.co.jp
Facebook：http://www.facebook.com/A10networksjapan

A10ネットワークス株式会社
〒105-0001
東京都港区虎ノ門 4-3-20
神谷町MTビル 16階
TEL : 03-5777-1995
FAX: 03-5777-1997
jinfo@a10networks.com
www.a10networks.co.jp

海外拠点

北米（A10 Networks本社）
sales@a10networks.com
ヨーロッパ
emea_sales@a10networks.com
南米
latam_sales@a10networks.com
中国
china_sales@a10networks.com
香港
HongKong@a10networks.com
台湾
taiwan@a10networks.com
韓国
korea@a10networks.com
南アジア
SouthAsia@a10networks.com
オーストラリア/ニュージーランド
anz_sales@a10networks.com

お客様のビジネスを強化するA10のアプリケーションサービスゲートウェイ、Thunderの詳細は、A10ネットワークスのWebサイト**www.a10networks.co.jp**をご覧になるか、A10の営業担当者にご連絡ください。

Part Number: A10-DG-16152-JA-04
June 2016