ISE と TrustSec を使用し、pxGrid を通じて Cisco WSA を統合する方法

素案

目次

このドキュメントについて

このドキュメントは、Cisco Identity Service Engine（ISE 1.3 以降）を搭載した Cisco Web Security Appliance（WSA 9.0.0-324 以降）を導入し、Cisco Platform Exchange Grid（pxGrid）を利用するパートナー、お客様、およびシスコエンジニアを対象としています。

このドキュメントの読者は、WSA、TrustSec、ISE、および pxGrid に精通している必要があります。

このドキュメントでは、認証局（CA）によって署名された環境での WSA と ISE pxGrid ノードの統合について説明します。ISE pxGrid ノードが一方はプライマリ、もう一方はセカンダリの個別のノードとして分散 ISE 展開で導入されていることを想定しています。

分散 ISE 環境に展開された pxGrid についての知識がない場合は、http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf を参照してください。

WSA と ISE pxGrid ノードの統合には、以下が含まれます。

- openSSL を使用した WSA の秘密キーと証明書の署名要求（CSR）の生成
- ISE pxGrid の ISE ノードおよび ISE モニタリング ノード（MNT）証明書のアップロード
- WSA 信頼ストアへの CA ルート証明書のアップロード
- Facebook アクセスからエンジニアリング セキュリティ グループ タグを割り当てたエンドユーザを拒否する Web アクセス ポリシーおよびアプリケーション復号化ポリシーの作成

ISE pxGrid のノードが、WSA クライアント証明書に署名する CA と同じ CA から署名された証明書を使用して、分散 ISE 環境内にすでに設定されていると想定しています。

エンジニアリング グループを表すセキュリティ グループ タグ（SGT）が作成され、許可ポリシーに割り当てられて、Windows/Domain/Users Group に所属する正常に認証されたユーザを許可します。

セキュリティ グループ タグを使用すると、企業のセキュリティ ポリシーを簡単に実装することができます。

SGT は、ACL と VLAN の制限事項に対応し、企業のセキュリティ ポリシーを実装する便利で柔軟性のある方法です。

次に、使用例を示します。

- 従業員 SGT を Windows/Domain/Users Group に所属するエンドユーザに割り当て、Box.com アクセスは許可し、Facebook アクセスは Netfilix 帯域制限で拒否する。
- ゲスト SGT をゲスト アイデンティティ グループに所属する ISE 内部ユーザに割り当て、Facebook アクセスは許可し、Box.com アクセスを拒否する。
- 請負業者 SGT を請負業者アイデンティティ グループに所属する ISE 内部ユーザに割り当て、Facebook アクセスは許可し、Box アクセスは拒否する。

これらのゲストおよび請負業者の使用例は、ISE 中央 Web 認証（CWA）に依存します。この操作については、スイッチ上で適切なコマンドが必要です。これらのコマンドについては「付録」を参照してください。

また、スイッチが RADIUS の認可変更（CoA）および中央 Web 認証（CWA）をサポートしていることも想定としています。

シスコのスイッチ互換性マトリクス（http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/compatibility/ise_sdt.html）を参照し、スイッチがサポートされていることを確認してください。

ソリューションの概要：TrustSec、ISE、および pxGrid を搭載した WSA

Cisco Web Security Appliance（WSA）は、Microsoft Active Directory（AD）、Novell の eDirectory および LDAP のサーバなど、さまざまな認証ストアのユーザやグループから組織の Web セキュリティ ポリシーを適用することによってセキュアな Web アクセスを提供します。

WSA は、認証レルムの作成に基づいてユーザやグループを認証し、それらのユーザやグループを識別プロファイルに割り当ててから、関連付けられた WSA Web アクセス ポリシーに割り当てます。エンドユーザは、自分のクレデンシャルを入力するように求められるか、透過的に WSA にリダイレクトされ、認証が行われます。透過的なユーザのリダイレクトには Cisco Context Directory Agent（CDA）が使用されます。Cisco Context Directory Agent（CDA）は Microsoft Active Directory（AD）ドメインにインストールされ、WSA の認証レルムの設定で定義されます。WSA は、コンテキスト ディレクトリ エージェントに AD 内の IP ユーザ名マッピングを問い合わせてユーザ名を取得します。エンドユーザにクレデンシャルを求めることはないため、シングルサイン オン（SSO）で Web トランザクションが実行されます。IP ユーザ名情報は、WSA でキャッシュされ、更新済みまたは新規のユーザ認証情報が CDA に問い合わせられます。

Cisco TrustSec は、正常に認証された 802.1X エンドユーザまたは 802.1X 以外の認証済みデバイスに SGT を割り当てることにより、WSA SSO プロセスを効率化するのに役立ちます。これと同じ SGT を WSA Web アクセス ポリシーに適用することで WSA アイデンティティ ポリシーを強化できます。

たとえば、エンジニアリングの セキュリティ グループ タグは、Cisco Identity Service Engine（ISE）で定義されます。このタグは、組織のエンジニアリング部門の Web セキュリティ アクセス ポリシーを表します。この SGT は、エンドユーザのエンジニアリング AD グループ、デバイス タイプ、組織の Web セキュリティ コンプライアンス ポリシーを表すポスチャ コンプライアンス ステータスを表します。

ISE を通じ、802.1X 経由でエンドユーザが正常に認証され、これらの承認条件を満たすと、それらのエンドユーザにはセキュリティ グループ タグが割り当てられます。その後で、この SGT は WSA の識別ポリシーに適用したり、Web セキュリティ ポリシーに関連付けたりできます。

ISE 管理コンソールからユーザやデバイスを一元管理できます。SSO は ISE での正常な 802.1X エンドユーザ認証によって提供されます。プリンタやカメラなどの 802.1X 以外のデバイスは、プロファイルされ、規定または規定外のネットワーク アクセスの保留中の ISE 許可ポリシーです。これらにはセキュリティ グループ タグを割り当て、WSA Web アクセス ポリシーに関連付けることもできます。

WSA が Web トランザクションの送信元のアイデンティティを認識していることが必要です。SGT がこの情報を提供しますが、他の ISE コンテキスト情報も含まれています。

Cisco Platform Exchange Grid（pxGrid）は、ISE からこのコンテキスト情報を使用するフレームワークを WSA に提供します。

Cisco Web Security Appliance（WSA）

Web Security Appliance（WSA）は、高度なマルウェア防御、アプリケーション可視性の制御、および許容可能な使用率ポリシーを提供し、企業の Web トラフィックを保護します。このドキュメントでは、アイデンティティ プロファイルと Web セキュリティ ポリシーにタグが設定され、Web アクセスのさまざまなレベルを SGT を使用して区別するようにします。

Cisco TrustSec

セキュリティ グループ タグ（SGT）は、Cisco TrustSec ソリューションの一部です。これらのセキュリティ グループ タグは ISE で定義され、入力（ネットワークへの着信）時に適用されます。これらのセキュリティ グループ タグは ISE で定義され、ユーザ、エンドポイントデバイス、ライン オブ ビジネスなどのグループを表すことができます。その場合、これらのタグは、ネットワーク アクセス ポリシーに適用され、ネットワーク デバイスによって使用されて転送決定が行われ、ネットワーク インフラストラクチャ全体にわたってアクセス制御ポリシーを共有することができます。SGT はセキュリティ グループに割り当てられる一意の 16 ビットのセキュリティ グループ番号です。簡単に理解できるように、セキュリティ グループにわかりやすい名前を付けることもできます。

これらのセキュリティ グループ タグは、組織のセキュリティ ポリシーを定義する条件ルールから構成されている ISE 許可ポリシーの許可プロファイルとして定義され、実装されます。

これらのセキュリティ グループ タグは、組織のセキュリティ ポリシーをネットワーク全体にわたって同一またはグローバルにすることができます。

このドキュメントでは、/users/domain Windows グループに所属し、正常に認証されたすべてのエンドユーザが、それらのユーザを SGT にマッピングするエンジニアリング セキュリティ タグを受け取るように許可ポリシーが作成されます。セキュリティ グループ タグは、エンドユーザのデバイスにマップされ、割り当てられたエンドユーザとエンジニアリング SGT への Facebook アクセスを拒否する制限付きの WSA アクセス ポリシーの確立に使用されます。

Cisco Identity Services Engine（ISE）

Identity Services Engine （ISE）は、セキュリティ ポリシーの管理およびアイデンティティ アクセスの管理を行うプラットフォーム ソリューションです。ISE は、802.1X 認証、ゲスト管理ポリシー、ポスチャ、クライアント プロビジョニング、および TrustSec ポリシーを定義/発行/適用することにって一元管理を実現します。ISE セッション ディレクトリは、情報を登録済みの pxGrid クライアントにパブリッシュするために pxGrid が使用する、ユーザ名、IP アドレス、デバイス タイプ、SGT、ポスチャ ステータス、MAC アドレスなど、認証済みの 802.1X および 802.1X 以外のデバイスに関するコンテキスト情報を提供します。

さらに、ISE は有線、ワイヤレス、および VPN 接続についてのアクセス制御やセキュリティ コンプライアンスを簡略化し、BYOD などのセキュリティ ポリシーに関する取り組みをサポートします。

Cisco pxGrid

Cisco Platform Exchange Grid（pxGrid）は、たとえば、セキュリティ モニタリングと検知システム、ネットワーク ポリシー プラットフォーム、アセットおよび仮想設定管理、アイデンティティおよびアクセス管理のプラットフォーム、ならびに仮想およびその他の IT 運用プラットフォームなど、IT インフラストラクチャの各部分間でのマルチベンダーのクロス プラットフォーム ネットワーク システムでのコラボレーションを可能にします。

ビジネス上または運用上のニーズが発生した場合、WSA やエコシステム パートナーなど、シスコのセキュリティ ソリューションでは pxGrid を使用し、公開またはサブスクライブの手法を通じてコンテキスト情報を交換します。

ISEは、ISE コンテキスト情報を公開する情報のトピックをセッション属性を使用して公開し、ISE が公開したセッションを WSA などの pxGrid クライアントがサブスクライブします。

次のトピックが含まれます。

- TrustSecMetadata 情報。セキュリティ グループ タグ番号と説明を公開します。

```
SecurityGroup : id=150138d0-cfc7-11e3-9e0e-000c29e66166, name=Engineering, desc=, tag=3
```

- EndpointProfileMetadata。ISE プロファイリング ポリシーへの変更や修正などの ISE エンドポイント ポリシーを提供します。

```
Endpoint Profile : id=886f7570-bd0c-11e3-a88b-005056bf2f0a, name=Apple-iDevice, fqname Apple-Device:Apple-iDevice
```

- EndpointProtectionサービス機能。認証されたエンドポイントの MAC アドレスによる IP の隔離または隔離解除などの軽減アクションを実行できる pxGrid クライアントが使用可能な適応型ネットワーク制御（ANC）の軽減アクションを公開します。

- SessionDirectory。ユーザ名やデバイス情報などの認証された使用セッション属性情報を公開します。

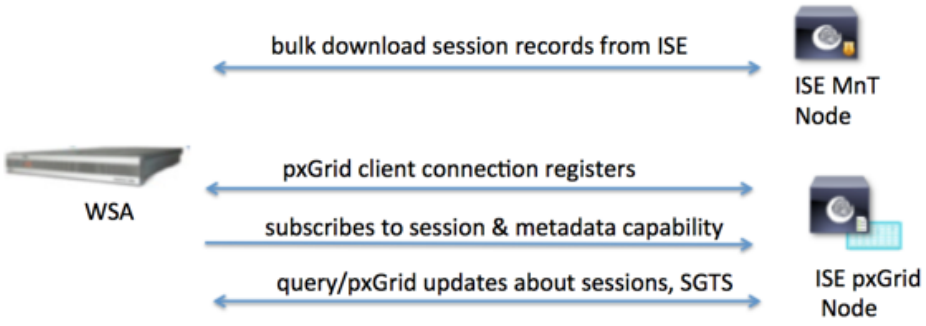
```
session (ip=192.168.1.14, Audit Session Id=0A0301030000001E00FEBAD7, User Name=jsmith, Domain=lab4.com,
Calling station id=00:0C:29:77:A8:C7, Session state= STARTED, Epsstatus=null,Security Group=Engineering,
Endpoint Profile=Microsoft-Workstation, NAS IP=192.168.1.2, NAS Port=GigabitEthernet1/0/9,
RADIUSAVPairs=[ Acct-Session-Id=00000027], Posture Status=null, Posture Timestamp=, Session Last Update
Time=Tue Apr 29 15:11:46 GMT-05:00 2014
```

- IdentityGroup。グループがプロファイリングされている場合も、ISE ユーザ情報およびグループ情報を公開します。

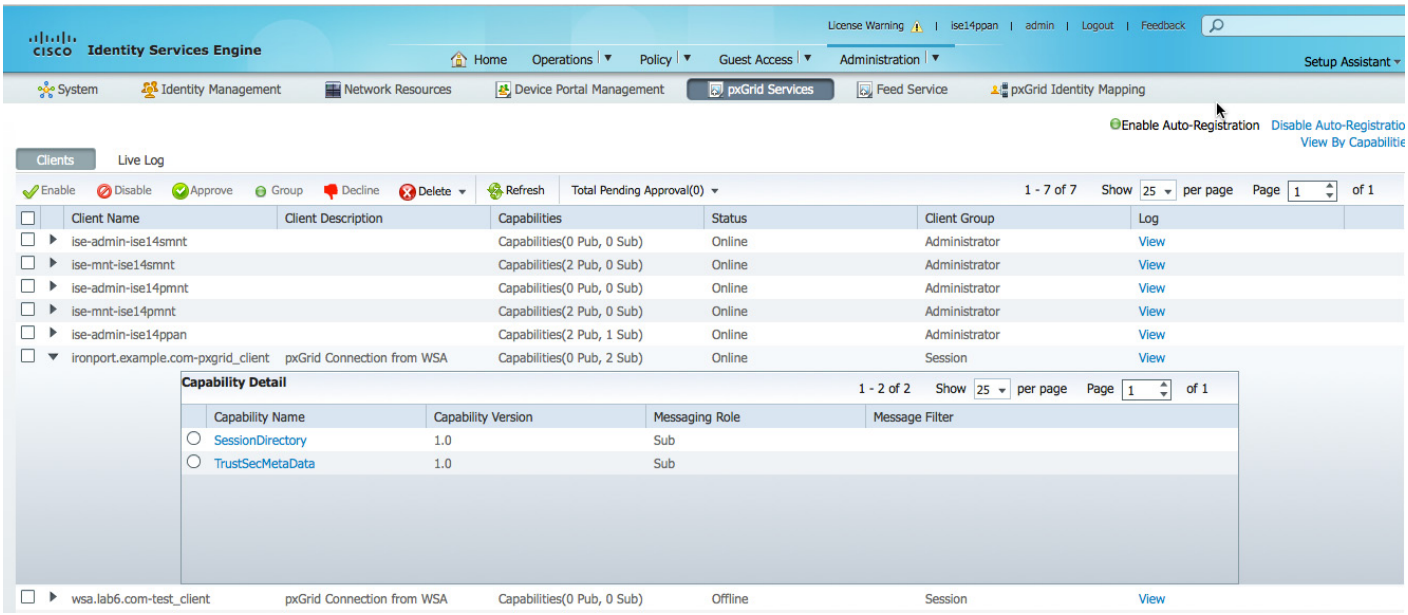
```
user=jeppich,WIN7-PC001.lab6.com
group=Workstation
user=18:E2:C2:91:BD:3B
group=Profiled
```

シスコのセキュリティ ソリューションおよびエコシステム パートナーは ISE pxGrid ノードに pxGrid クライアントとして登録し、ユーザ識別情報、デバイスのオペレーティング システム、セキュリティ グループ タグ（SGT）など、イベントに関連するより詳しいコンテキスト情報を提供するトピックをサブスクライブします。これらの pxGrid クライアントはセッション レコードを一括してダウンロードすることもできます。

WSA の場合と同様に、セッションおよび SGT の一括ダウンロードは、WSA ISE サービスの起動時または（WSA ISE の設定変更による）再起動時にのみ実行され、ISE MNT ノードから ISE RESTful API を通じてダウンロードされます。エンドユーザは、ISE から取得したセッション情報、IP アドレス、および関連付けられた IP セッション マッピングに基づいて識別されます。SGT の IP セッション マッピングはローカルにキャッシュされます。WSA が要求の IP アドレスを検出すると、IP-SGT マッピングをローカルにルックアップし、対応する SGT にトランザクションを関連付けます。または、セッション ディレクトリおよび TrustSec Metadata トピックのサブスクリプションに基づいて、その SGT の ISE pxGrid ノードにオンデマンド クエリで新しい IP アドレスを問い合わせます。



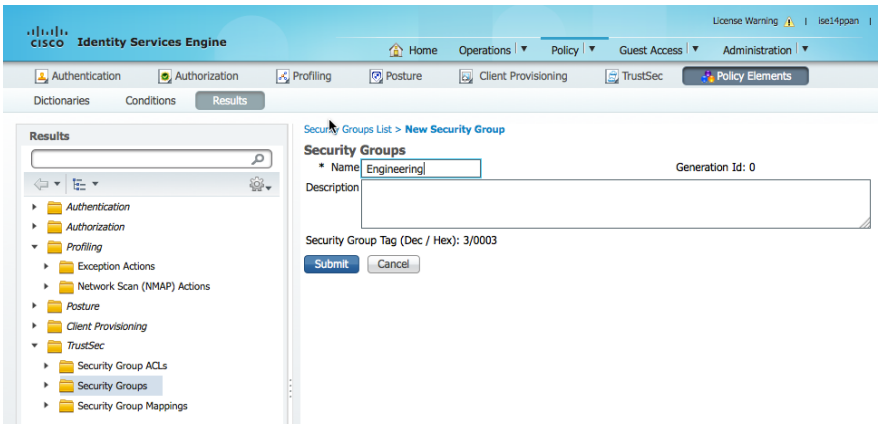
次に、ISE pxGrid として登録され、公開された情報トピックをサブスクライブする WSA を示します。



ISE を使用した動的セキュリティ グループ タグの割り当て

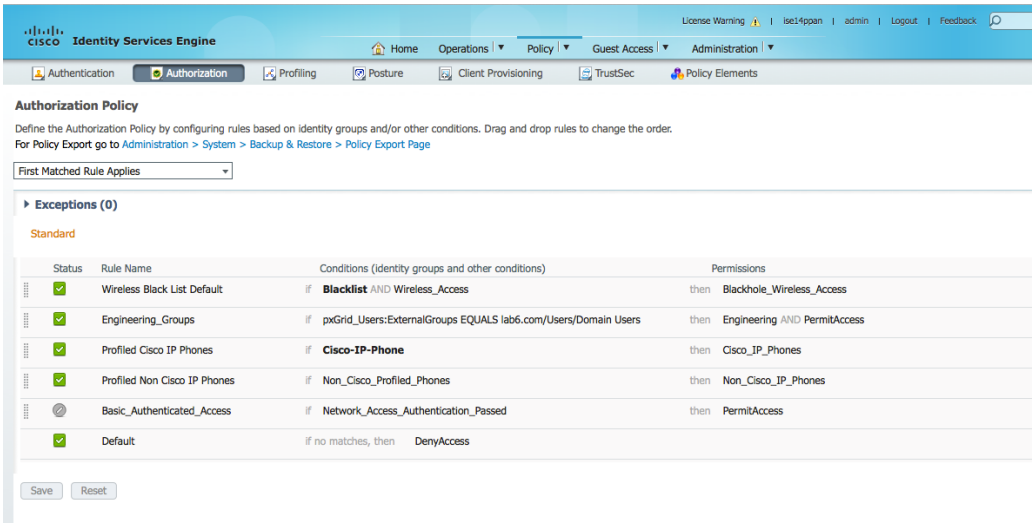
組織のセキュリティ ポリシーは、次のセキュリティ グループ タグ（SGT）に基づいて定義できます。そのため、組織にネットワーク全体に同一のグローバルなセキュリティ ポリシーを設定できます。他の例として、企業のエンドユーザと、企業の許容使用法に関するポリシーに従って社内ネットワークに導入される推奨デバイスなどがあります。これは、1 つの SGT で表すことができます。Cisco TrustSec が組織のスイッチで有効になっている場合は、これらのセキュリティ グループ タグもネットワーク上で適用できます。通常、スイッチ、ルータ、ファイアウォールなどのネットワーク デバイスには 2 というセキュリティ グループ タグが付与されます。

ステップ 1 エンジニアリング セキュリティ グループ タグを作成します。
[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [TrustSec] > [セキュリティ グループ（Security Groups）] > [追加（Add）] > [エンジニアリング（Engineering）] > [送信（Submit）]



ステップ 2 許可ポリシーを作成し、SGT 許可プロファイルをポリシーに割り当てます。
[ポリシー（Policy）] > [承認（Authorization）] に移動し、次の許可ルールを追加します。

ルール名：Engineering
新しい条件：External Groups:equals:pxGrid_Users
許可プロファイル：Engineering and Permit Access



ステップ 3 [保存(Save)] を選択します。

Cisco WSA のインストール

この最初の WSA セットアップは WSA のシステム ウィザードを使用して実行します。これには、WSA のネットワーク設定、管理およびトラフィック モニタリング用のインターフェイス、デフォルトの管理者クレデンシャルの変更が含まれます。

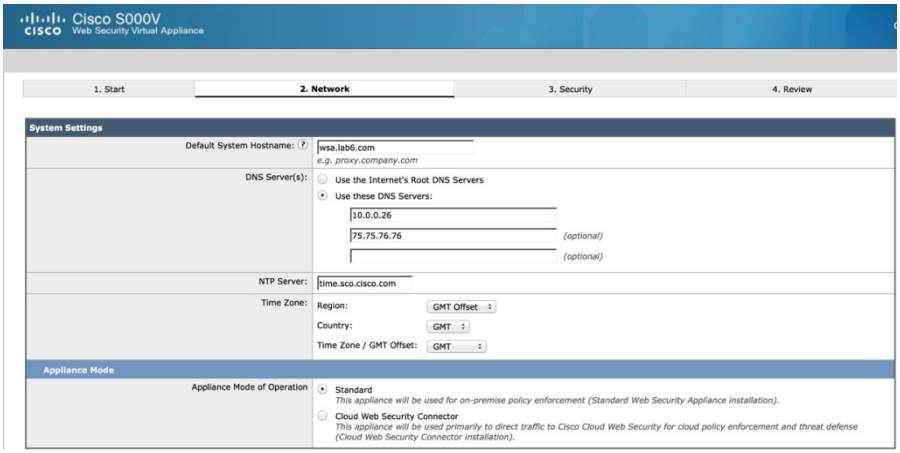
WSA システム ウィザード

ステップ 1 [システム管理（System Administration）] > [システムのセットアップ（System Setup）] > [システム セットアップ ウィザード（System Setup Wizard）] に移動し、WSA の管理 IP アドレスを入力します。

注：このドキュメントでは、WSA 管理 IP アドレスに 10.0.0.9 を使用しています。

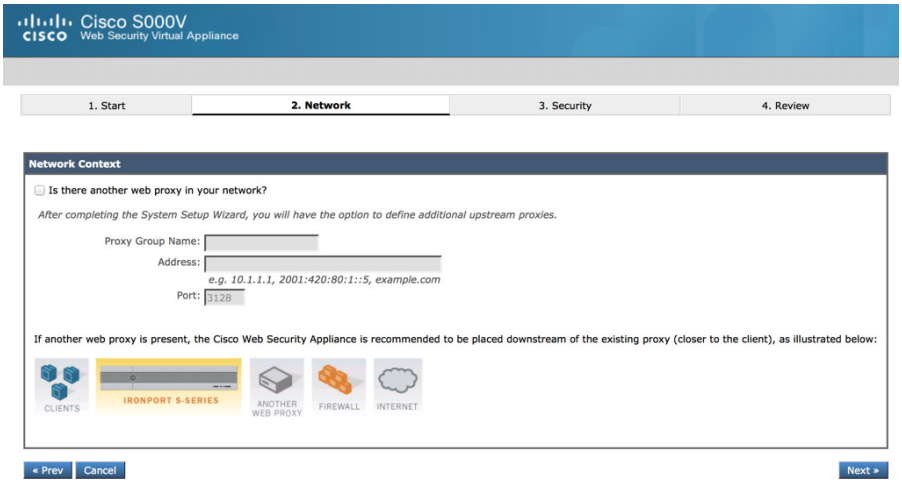
```
http://10.0.0.9:8080
```

ステップ 2 システム情報および DNS サーバ情報を入力します。

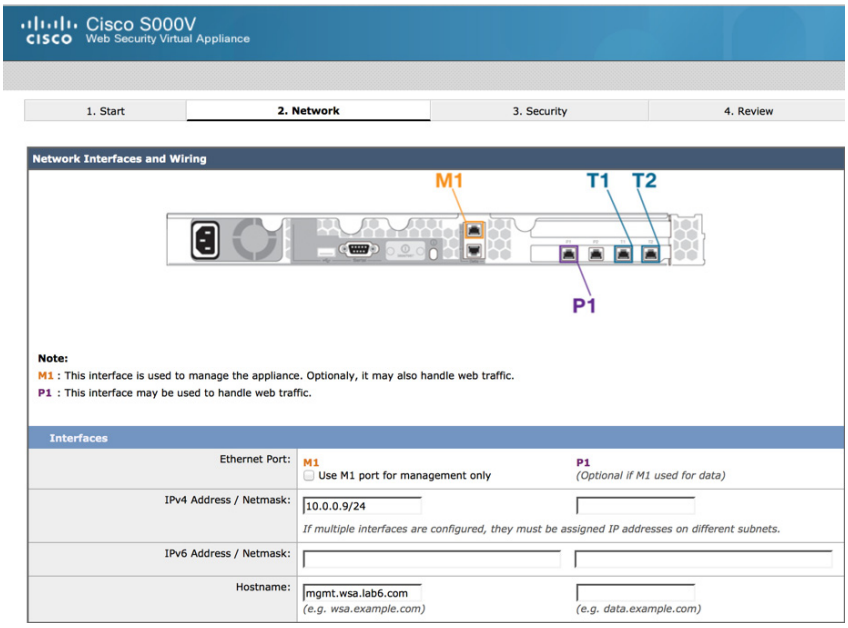


ステップ 3 [次へ（Next）] を選択します。

ステップ 4 ネットワーク内に他の Web プロキシがない場合は、[次へ（Next）] を選択します。

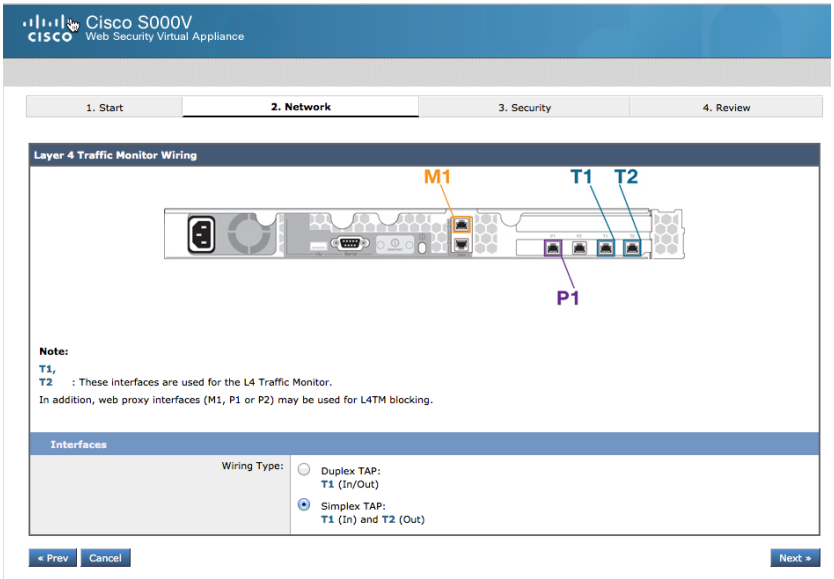


ステップ 5 このドキュメントでは、すべてのトラフィックの管理と処理にすべて M1 を使用しています。



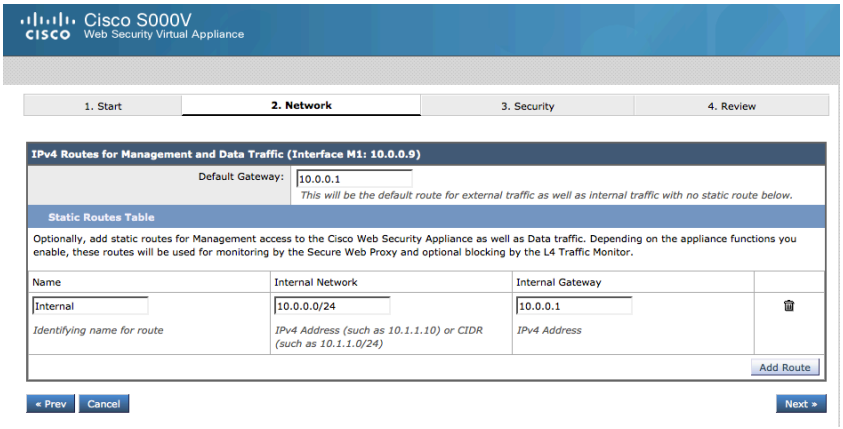
ステップ 6 [次へ(Next)] をクリックします。

ステップ 7 このドキュメントでは、シンプレックス タップを設定します。



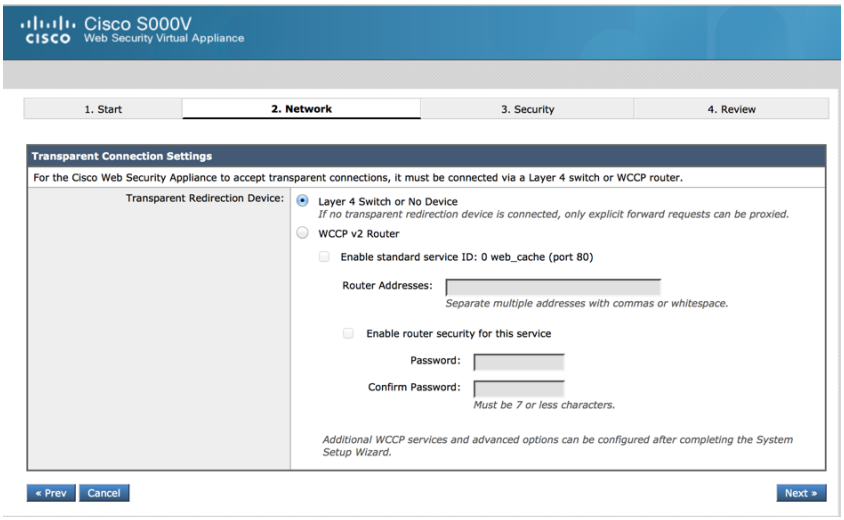
ステップ 8 [次へ(Next)] をクリックします。

ステップ 9 ネットワーク ルートを入力します。

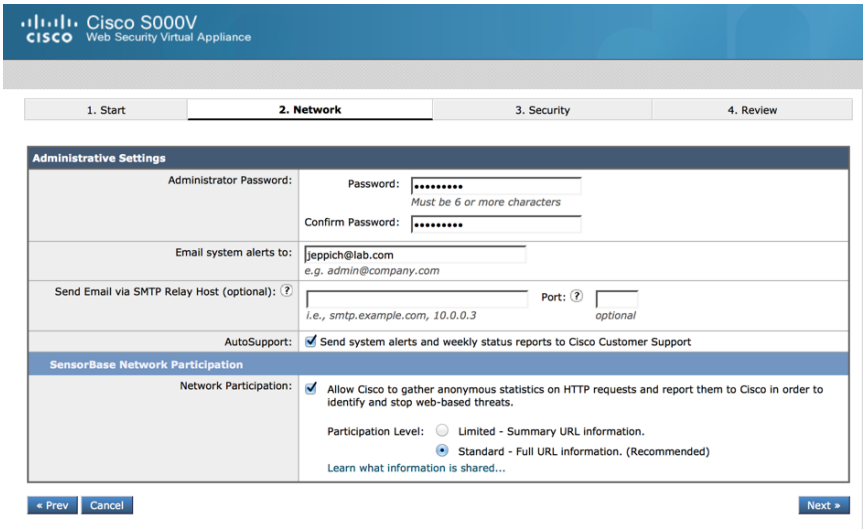


ステップ 10 このドキュメントでは、明示的なプロキシが使用されます。[次へ(Next)] をクリックします。

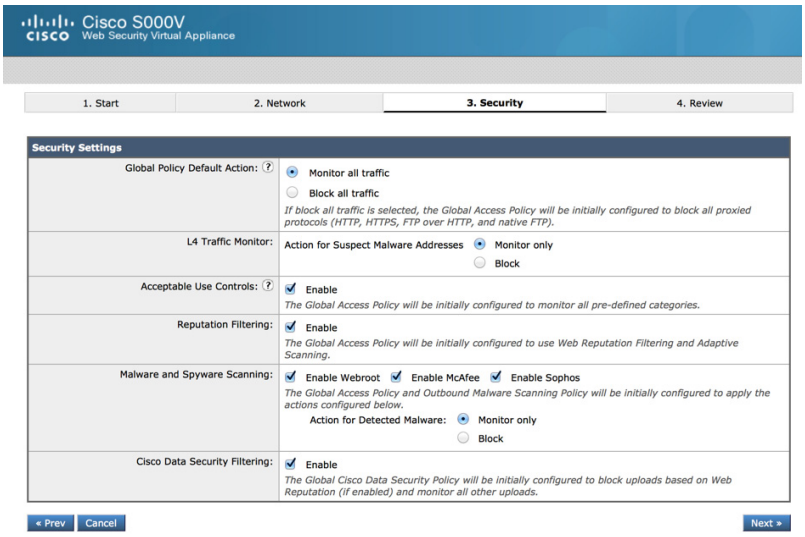
注:PC クライアント プロキシの設定については、「付録」を参照してください。



ステップ 11 管理者名、パスワード、および電子メール アドレスを入力します。

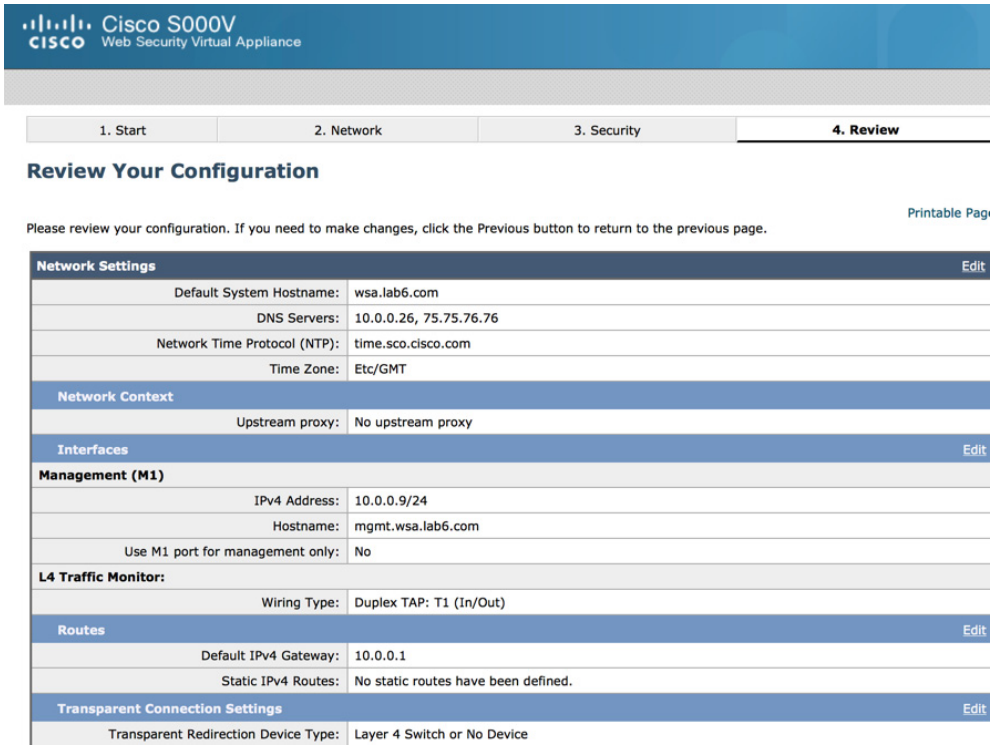


ステップ 12 [次へ(Next)] をクリックします。
ステップ 13 このドキュメントでは、すべてデフォルト値を設定します。



ステップ 14 [次へ(Next)] をクリックします。

ステップ 15 設定を確認します。



ステップ 16 [この設定をインストール（Install This Configuration）] をクリックします。

CA 署名付き証明書を使用した WSA および ISE pxGrid ノードの設定

ここでは、アクティブ/スタンバイ設定の専用プライマリおよびセカンダリ pxGrid ノードを設定した分散 ISE 展開での WSA および ISE pxGrid ノードの設定について説明します。Microsoft Enterprise 2008 CA 認証局（CA）サーバを使用して ISE ノード、ISE pxGrid ノードおよび WSA を署名したことに注意してください。クライアント認証とサーバ認証の両方の EKU を含めてカスタマイズした pxGrid テンプレートを作成し、WSA と ISE pxGrid ノードの証明書に使用しています。

最初に、WSA 信頼ストアに CA ルート証明書をアップロードします。

注：CA ルート証明書は ISE 信頼システム ストアにすでにインポートされています。

WSA の秘密キーおよび証明書署名要求（CSR）が作成されます。カスタマイズした pxGrid テンプレートを使用して、CSR 要求がコピーされ、Microsoft の詳細なユーザ要求に貼り付けられます。WSA 証明書がダウンロードされ、WSA 公開証明書と秘密キーの両方が WSA にアップロードされます。

ISE アクセス ログが WSAで設定されると、WSA サービスの再起動などの WSA と ISE の統合の問題や、WSA を通じて ISE と pxGrid の IP アドレスまたは FQDN が解決できないなどといった問題のトラブルシューティングに役立ちます。

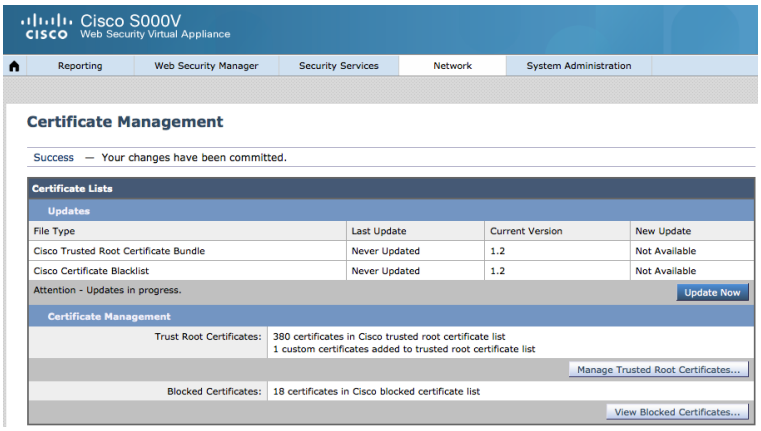
CA ルート証明書が pxGrid プライマリ ノードと pxGrid セカンダリ ノードから WSA にアップロードされます。pxGrid のノードは、管理者ノードを問い合わせて、動作可能なノードを確認します。デフォルトでは、プライマリ pxGrid ノードがアクティブで、セカンダリ pxGrid ノードが非アクティブになります。完全な PPAN 障害が発生し、SPAN がアクティブになった場合、プライマリ pxGrid ノードは SPAN をアクティブな PPAN と見なします。

プライマリおよびセカンダリ ISE および MNT ノードの公開証明書は最初の WSA の起動時の一括セッション ダウンロード情報として WSA にアップロードされます。プライマリ MNT がダウンした場合、WSA のキャッシュには SGT と IP のマッピングが含まれています。さらに、プライマリ管理ノード（PPAN）からのクエリ チェックによりプライマリ MNT がダウンしていることを検知します。MNT ノードも動作しているノードについて管理ノードに問い合わせます。MNT ノードに複数の証明書がある場合は、管理者用に指定された証明書が選択されます。

WSA 証明書信頼ストアへの CA ルート証明書の追加

WSA 信頼ストアへの CA ルート証明書の追加

ステップ 1 [ネットワーク（Network）] > [証明書の管理（Certificate Management）] > [信頼ルート証明書の管理（Manage Trusted Root Certificates）] > [CA ルート証明書のインポートとアップロード（Import and upload the CA root certificate）] > [送信（Submit）] > [確定する（Commit）] を選択します。



CA 署名付き WSA クライアント証明書の設定

WSA 秘密キーおよび CSR 要求の作成

MAC または Linux サーバを使用して、秘密キーと CSR 要求を作成できます。この例では、MAC を使用しています。

次の例では、WSA 秘密キーを作成しています。

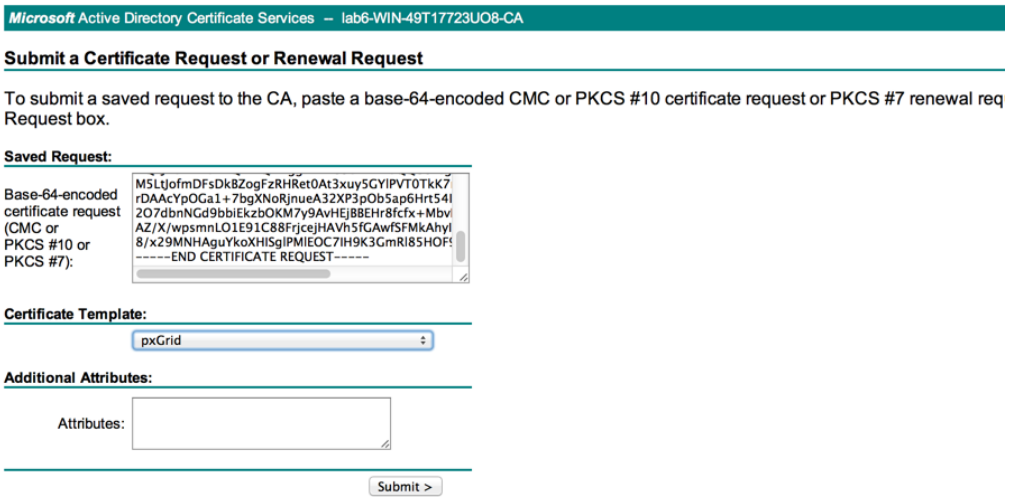
```
openssl genrsa -out wsa1.key 4096
Generating RSA private key, 4096 bit long modulus
.....................................................................................................
.....................................................................++
.....................................................++
e is 65537 (0x10001)
```

次の例では、CSR 要求が WSA 秘密キーから生成されます。

```
openssl req -new -key wsa1.key -out wsa1.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]: Maryland
Locality Name (eg, city) []:Germantown
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:wsa.lab6.com
Email Address []:
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

CSR 要求をコピーし、pxGrid のカスタマイズされたテンプレートに貼り付け、base-64 のエンコードされたフォーマットでダウンロードします。



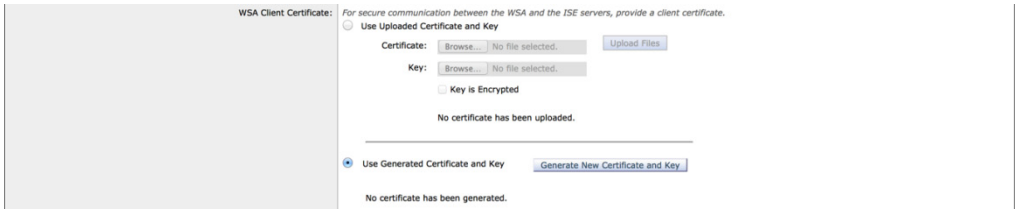
ステップ 1 [送信（Submit）] を選択します
ステップ 2 「base-64」をダウンロードします。

ステップ 3 [base-64」をダウンロードし、送信します
ステップ 4 また、「base-64」でルート証明書をダウンロードします。

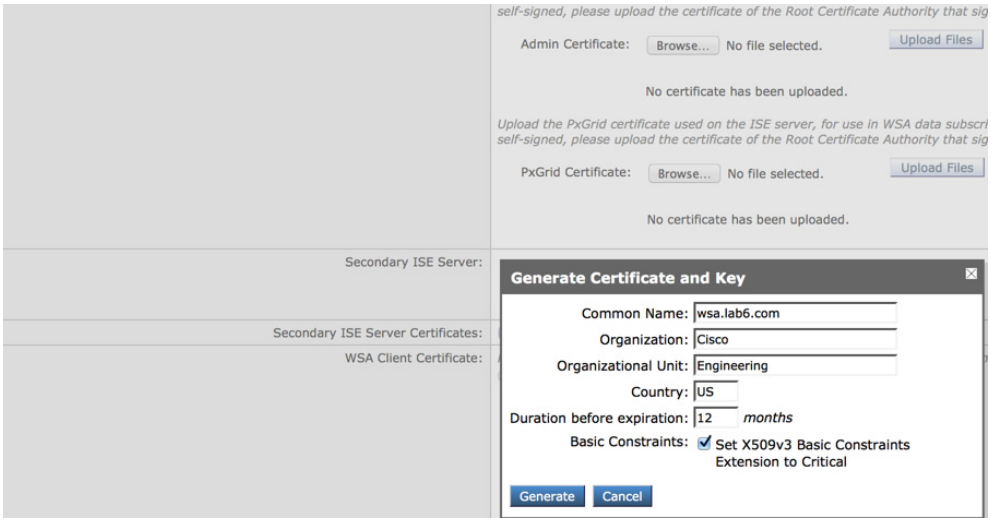
WSA からの WSA 秘密キーおよび CSR 要求の作成（代替策）

pxGrid 動作用の WSA CSR を生成します。

ステップ 1 [ネットワーク（Network）] > [識別サービス（Identification Service）] > [Identity Service Engine] > [設定の編集（Edit Settings）] > [WSA クライアント証明書（WSA Client Certificate）] > [新しい証明書とキーを生成（Generate New Certificate and Key）] を選択します。

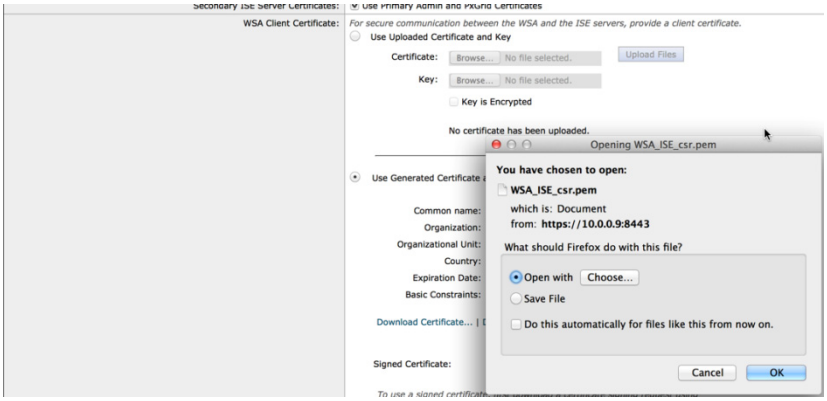


ステップ 2 次の手順で、CSR 要求が生成されます。情報を入力してください。

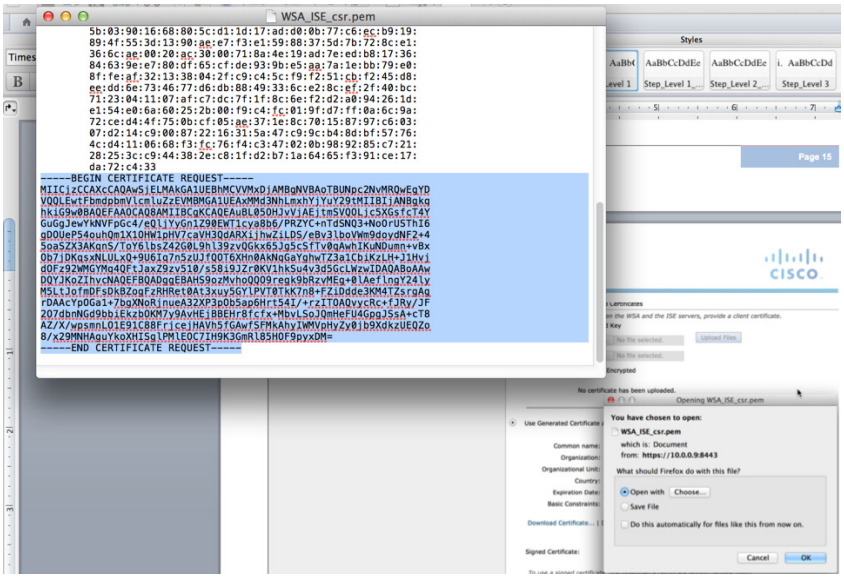


ステップ 3 [生成（Generate）] を選択し、証明書とキーが正常に生成されていることを確認します。

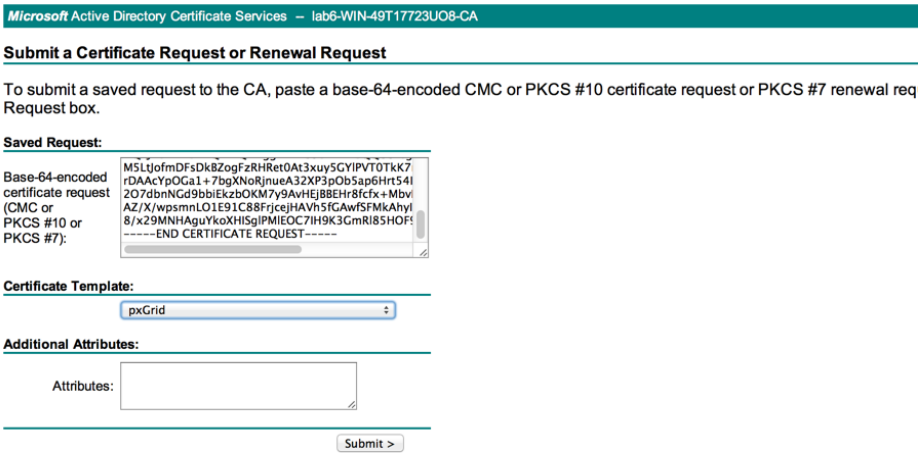
ステップ 4 [証明書署名要求をダウンロード（Download the Certificate Signing Request）] を選択し、エディタを使用して開きます。



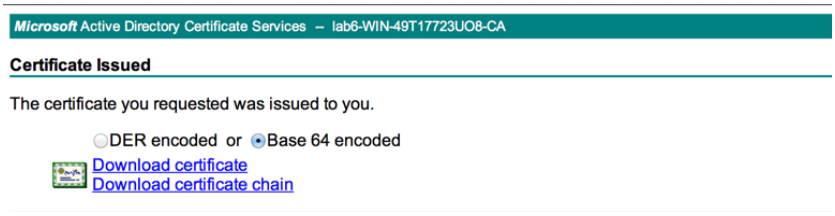
ステップ 5 コピーして、カスタマイズした pxGrid テンプレートに貼り付けます。



ステップ 6 詳細ユーザ要求を送信します。

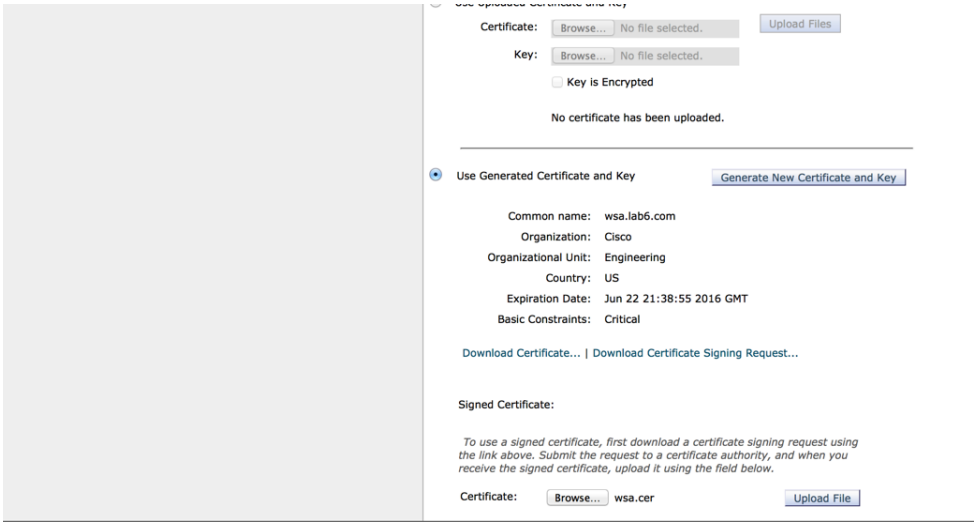


ステップ 7 [送信(Submit)] を選択します
ステップ 8 「Base-64 符号化」をダウンロードします。



ステップ 9 [Submit(送信)] をクリックします。
ステップ 10 また、「Base-64 符号化」のルート証明書もダウンロードします。

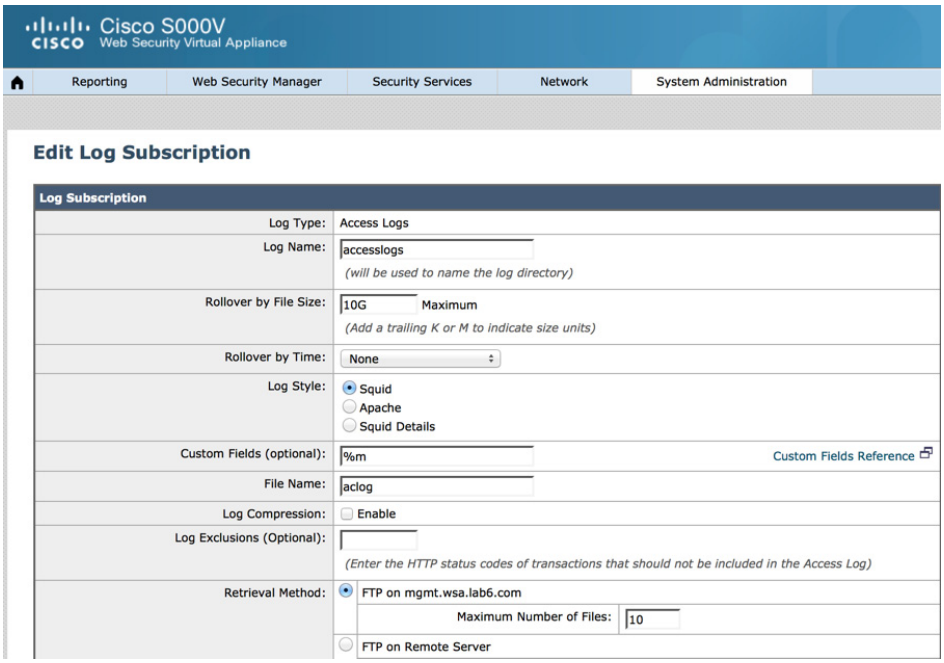
ステップ 11 WSA+pxGrid の識別証明書をアップロードします。



WSA での ISE サービスの設定

ステップ 1 アクセス ログを作成し、カスタム フィールドを含めます。
[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscription）] > [アクセス ログ（access logs）] - [カスタム フィールド-%m（Custom Fields-%m）]

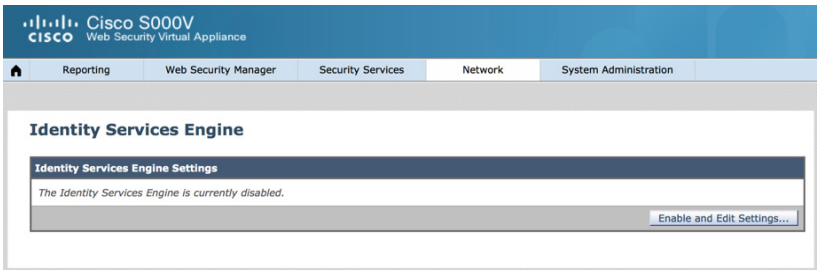
注：これは、WSA RESTful API が起動時に確立できないなど、解決されていないホストなどの WSA と ISE+pxGrid ノードの接続上の問題のトラブルシューティングに使用されます。



ステップ 2 変更を送信し、確定します。

プライマリ pxGrid ノード証明書のアップロード

ステップ 1 [ネットワーク（Network）] > [識別サービス（Identification Services）] > [識別サービスエンジン（Identification Service Engine）] を選択します。

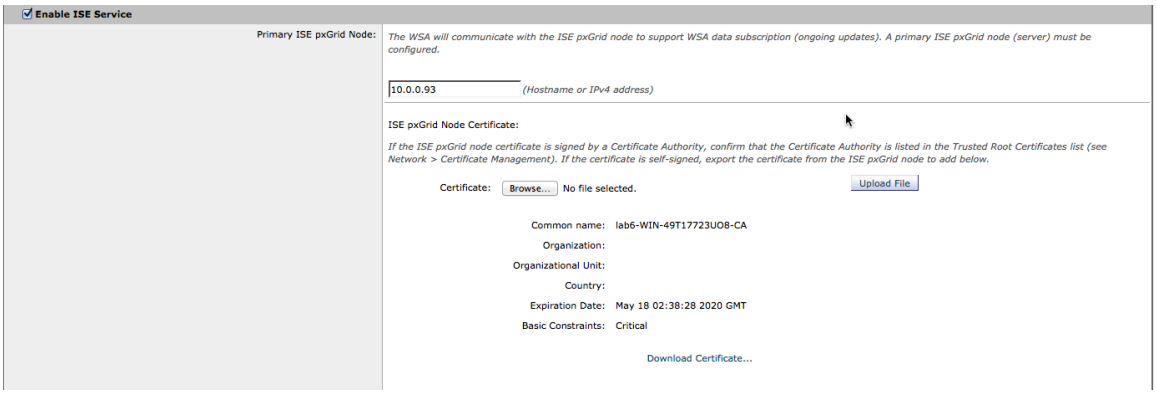


ステップ 2 [設定の有効化および編集（Enable and Edit Settings）] を選択します。

ステップ 3 pxGrid1 IP アドレスまたは FQDN を入力します。

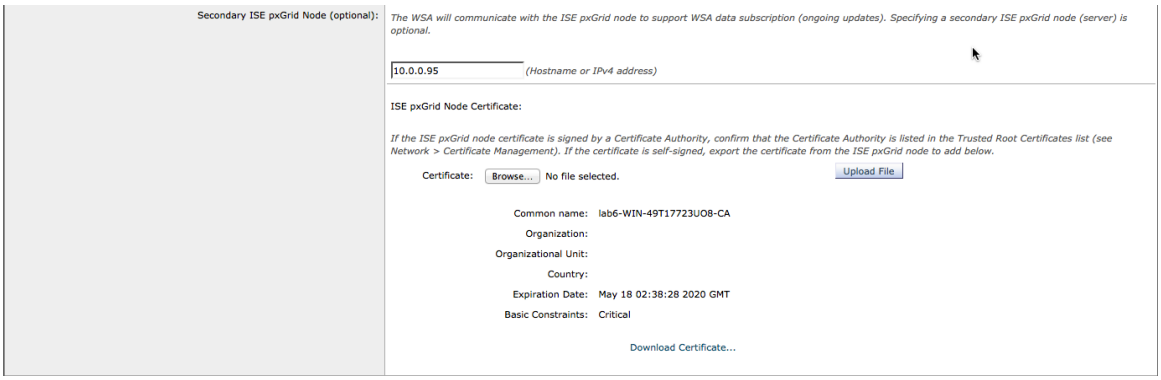
注：ISE の展開ごとに使用できるのは 2 つの pxGrid ノードのみです。これは、pxGrid アクティブ/スタンバイ設定として機能します。一度にアクティブにできるのは 1 つの ISE+pxGrid のみです。pxGrid アクティブ/スタンバイ設定では、2 番目の ISE+pxGrid ノードが非アクティブを維持していれば、すべての情報が PPAN を通じて渡されます。

ステップ 4 プライマリ pxGrid ノードの CA ルート証明書をアップロードします。
CA ルートの公開証明書をアップロードします。



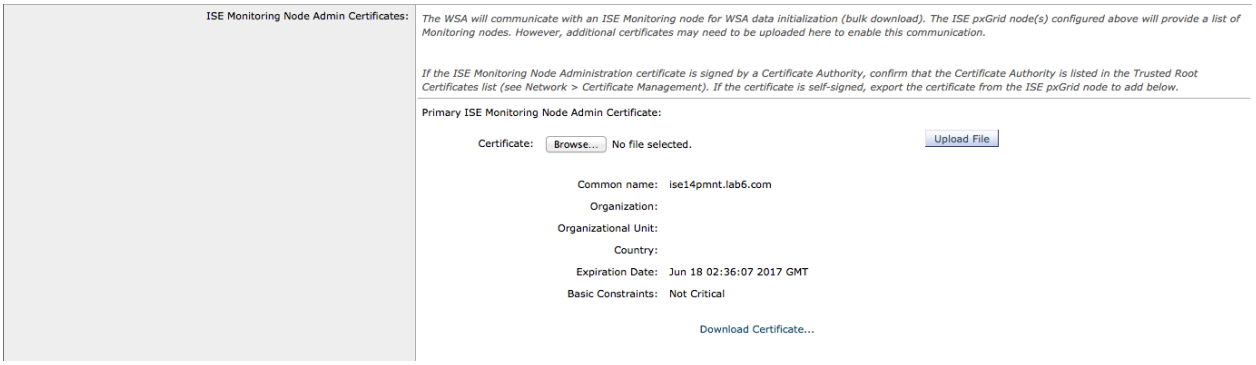
セカンダリ pxGrid ノードの証明書のアップロード

ステップ 1 pxGrid2 の IP アドレスまたは FQDN を入力します。
ステップ 2 プライマリ pxGrid ノードの CA ルート証明書をアップロードします。
CA ルートの公開証明書をアップロードします。



プライマリ モニタリング ノードの証明書のアップロード

ステップ 1 プライマリ MNT の公開証明書をアップロードします。

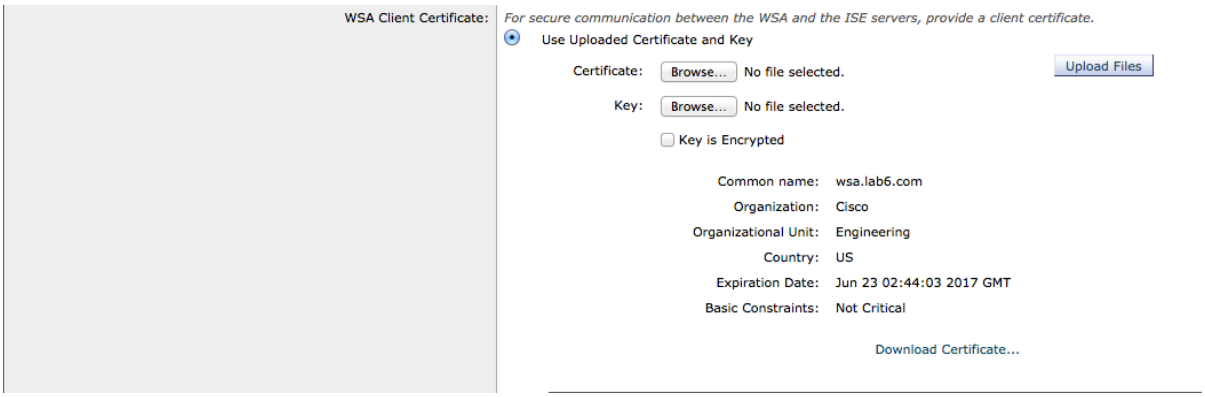


セカンダリ モニタリング ノードの証明書のアップロード

ステップ 1 セカンダリ MNT の公開証明書をアップロードします。

WSA の証明書と秘密キーのアップロード

ステップ 1 WSA クライアント認証で、公開証明書の wsa1.cer と WSA 秘密キーの wsa1.key をアップロードします。

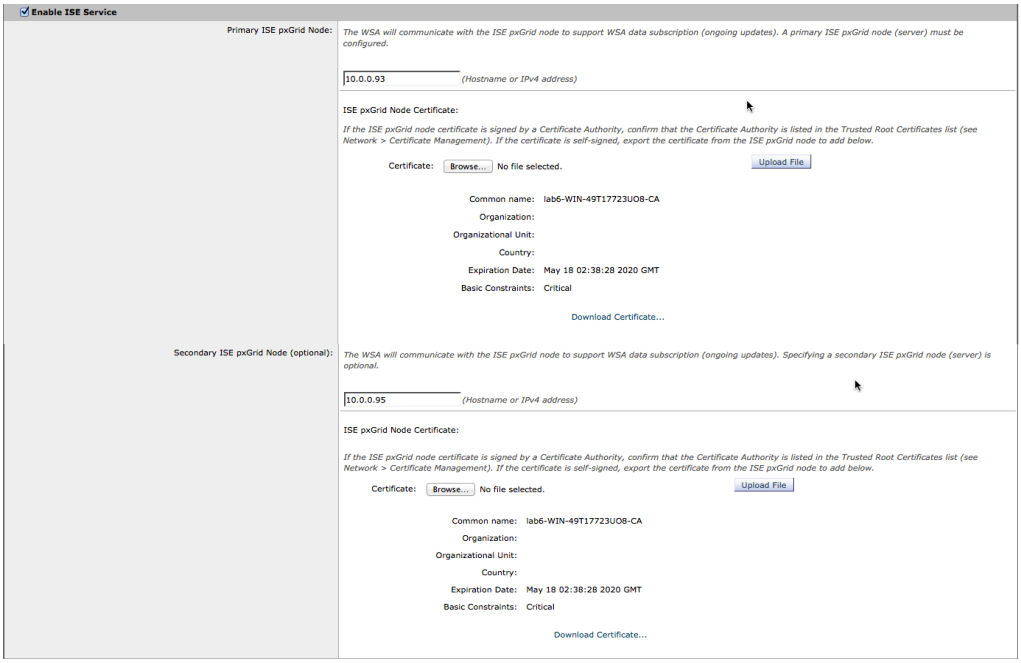


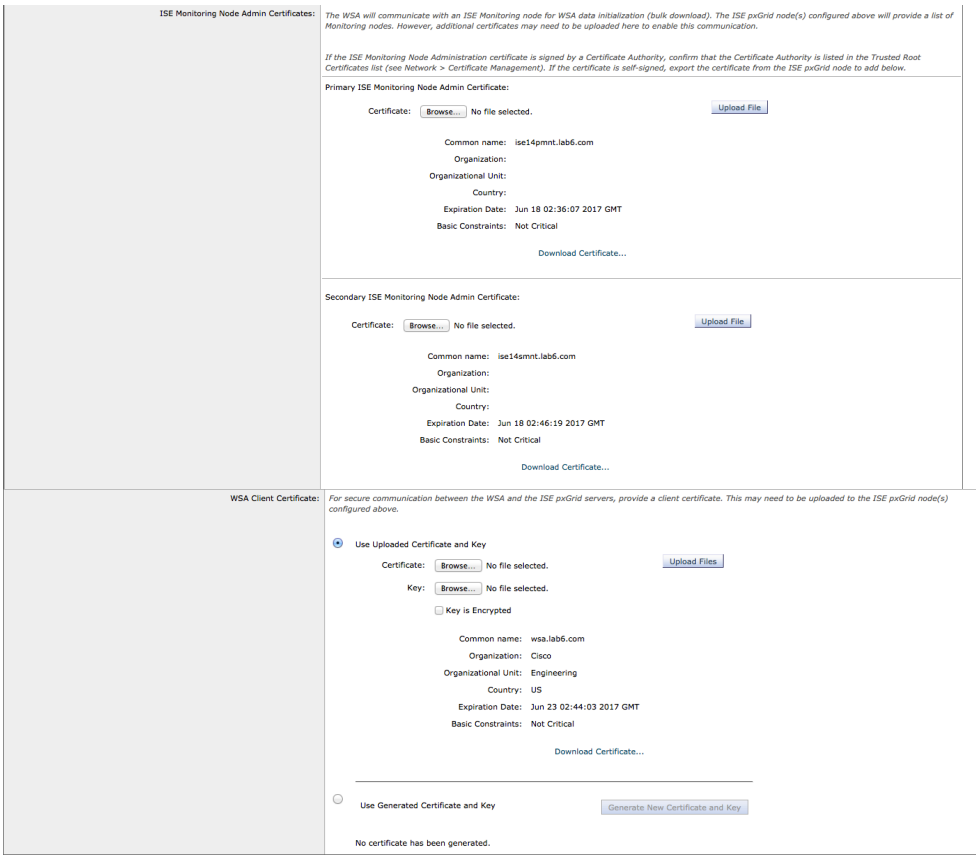
テストの実行

ステップ 1 テストを開始すると、次の情報が表示されます。

```
Checking DNS resolution of ISE pxGrid Node hostname(s) ...
Success: Resolved '10.0.0.93' address: 10.0.0.93
Success: Resolved '10.0.0.95' address: 10.0.0.95

Validating WSA client certificate ...
Success: Certificate validation successful

Validating ISE pxGrid Node certificate(s) ...
Success: Certificate validation successful
Success: Certificate validation successful

Validating ISE Monitoring Node Admin certificate(s) ...
Success: Certificate validation successful
Success: Certificate validation successful

Checking connection to ISE pxGrid Node(s) ...
Success: Connection to ISE pxGrid Node was successful.
Retrieved 4 SGTs from: 10.0.0.93

Checking connection to ISE Monitoring Node (REST server(s)) ...
Success: Connection to ISE Monitoring Node was successful.
REST Host contacted: ise14pmnt.lab6.com

Test completed successfully.
```

次に、分散 ISE 環境で pxGrid がアクティブ/スタンバイの CAが署名した WSA 証明書の設定の概要を示します。



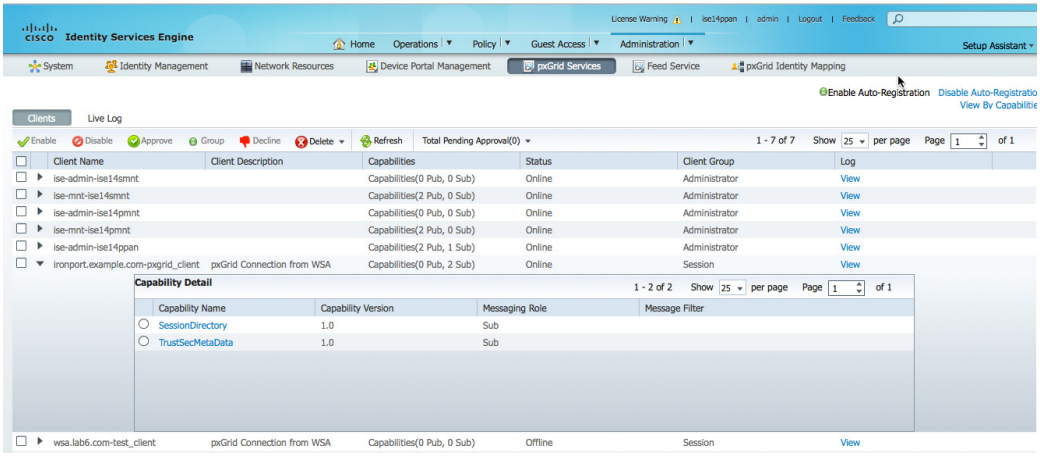


ステップ 2 [変更を確定(Commit changes)] を 2 回選択します。

登録済み pxGrid クライアントとしての WSAの確認

ここでは、WSA が pxGrid クライアントとして登録されていることを確認します。

ステップ 1 [管理（Administration）] > [pxGrid サービス（pxGrid Services）] を選択し、WSA が pxGrid クライアントとして登録されていることを確認します。

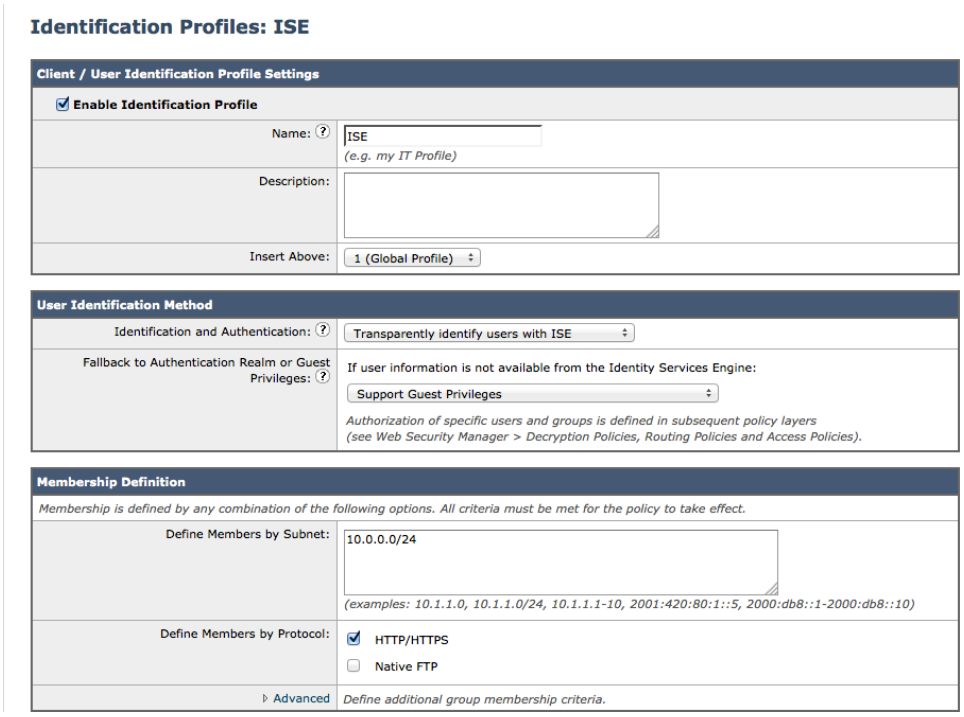


WSA ポリシー

ISE 識別プロファイルは WSA で作成され、ISE 認証を許可します。エンジニアリング セキュリティ グループ タグに割り当てられたエンドユーザ用に Web アクセス ポリシーが作成されます。この Web アクセス ポリシーは、URL フィルタリングとアプリケーション復号化ポリシーに基づいて、Facebook アクセスを拒否します。

WSA での識別プロファイルの作成

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [認証（Authentication）] > [識別プロファイル（Identification Profiles）] > [識別プロファイルを追加（Add Identification Profile）] を選択します。
[名前（Name）] を指定：**ISE**
[識別および認証（Identification and Authentication）]：ISE で透過的にユーザを変更（Transparently modify users with ISE）
[認証レルムまたはゲスト権限にフォールバック（Fallback to Authentication Realm or Guest Privileges）]：ゲスト権限をサポート（Support Guest Privileges）



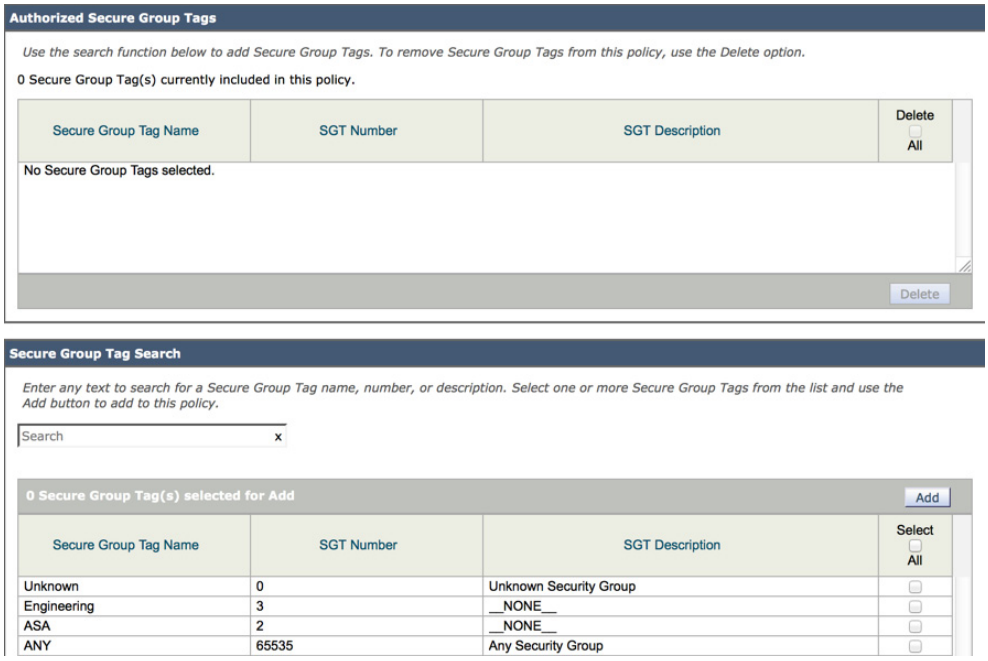
ステップ 2 [変更を送信（Submit Changes）] を選択し、[確定する（Commit）] を 2 回選択します。

WSA アクセス ポリシーの作成

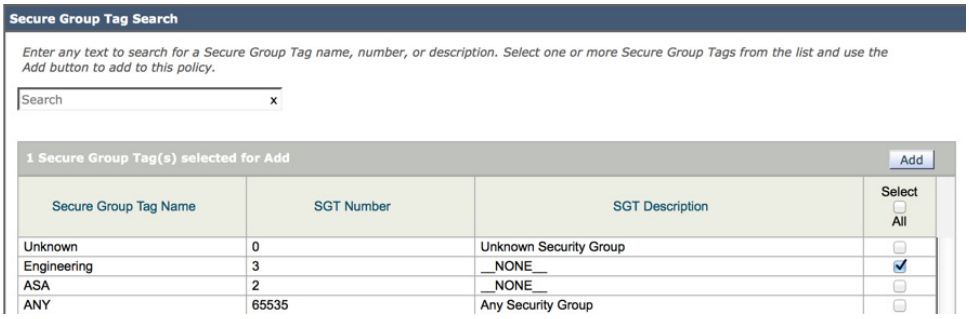
ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [Web ポリシー（Web Policies）] > [ポリシーを追加（Add Policy）] > [ポリシー名 : Engineering（Policy Name: Engineering）] を選択します。

ステップ 2 [Web セキュリティ マネージャ（Web Security Manager）] > [Web ポリシー（Web Policies）] > [ポリシーを追加（Add Policy）] > [識別プロファイルとユーザ（Identification Profiles and Users）] > [1 つ以上の識別ポリシーを選択（Select one or more identification policies）] > [ISE] > [グループとユーザを選択（Select Groups and Users）] > [タグを入力しない（No Tags Entered）] を選択します。

次が表示されます。

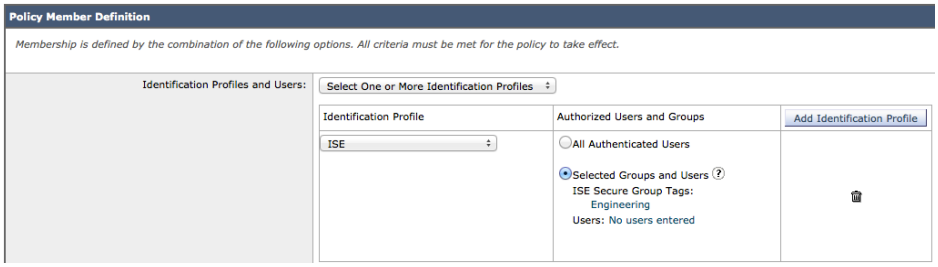


ステップ 3 [エンジニアリング（Engineering）] > [追加（Add）] を選択すると、アクセス ポリシーに SGT が追加されます。



ステップ 4 [完了（Done）] をクリックします。[エンジニアリング（Engineering）] SGT タグが選択されています。

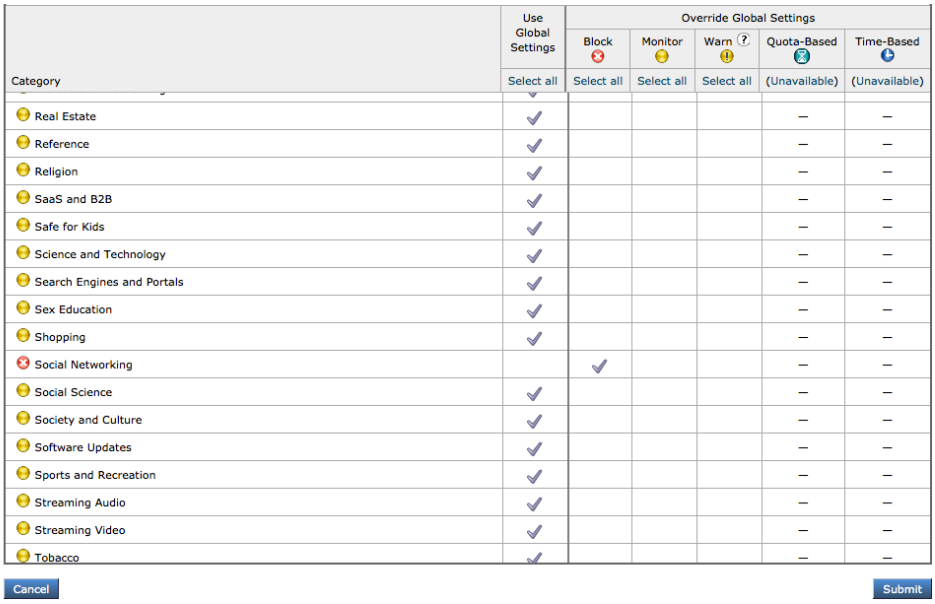
次が表示されます。



ステップ 5 [完了（Done）] をクリックします。

ステップ 6 [Submit（送信）] をクリックします。

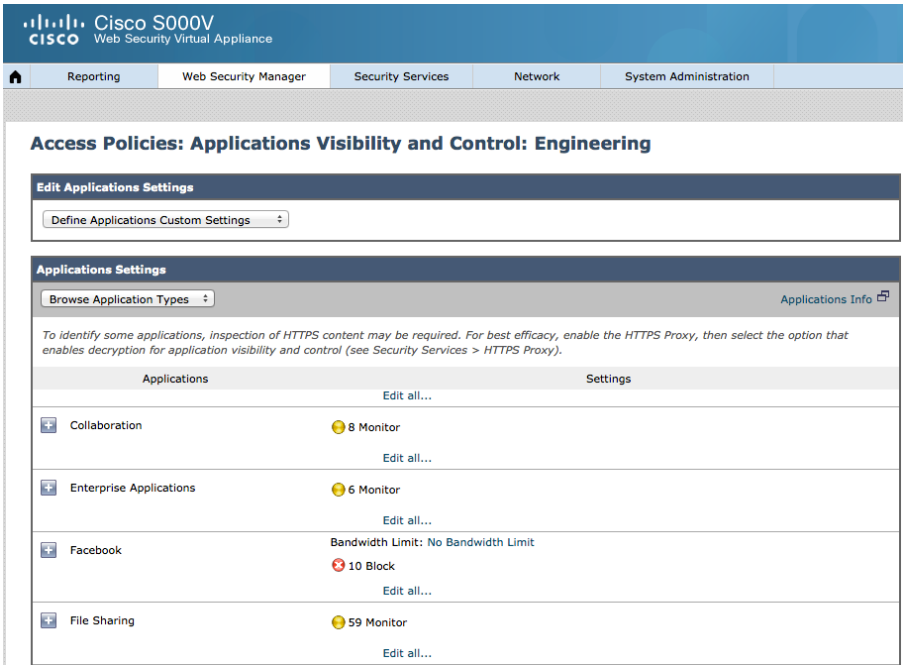
ステップ 7 [URL フィルタリング（URL Filtering）] で、[グローバル ポリシー（Global Policy）] を選択し、次のように設定します。



ステップ 8 [送信（Submit）] を選択します

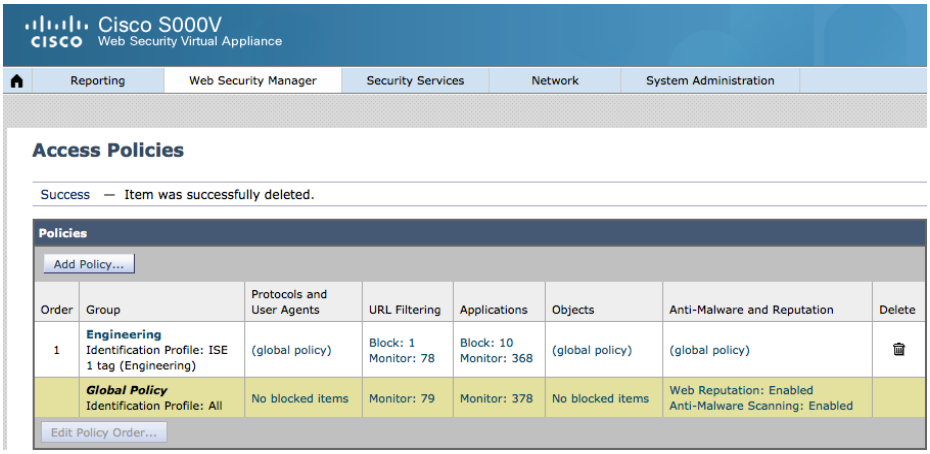
ステップ 9 [グローバル ポリシー（Global Policy）] で [アプリケーション（Applications）] をクリックします。

ステップ 10 [アプリケーション設定を編集（Edit Applications Settings）] で、[アプリケーションのカスタム設定を定義（Define Applications Customs Settings）] を選択し、すべての Facebook アプリケーションをブロックします。



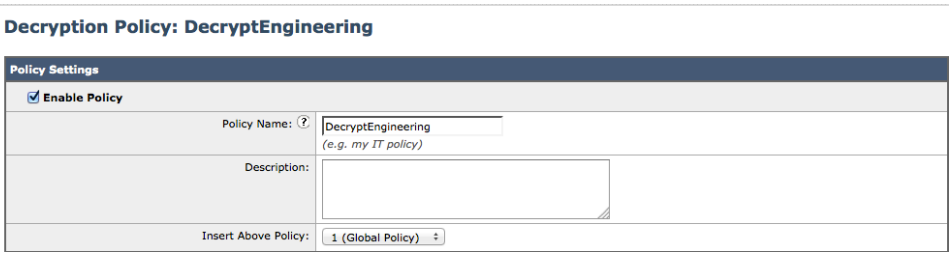
ステップ 11 [変更（Submit）] をクリックし、[変更を確定（Commit Changes）] を 2 回クリックします。

次が表示されます。

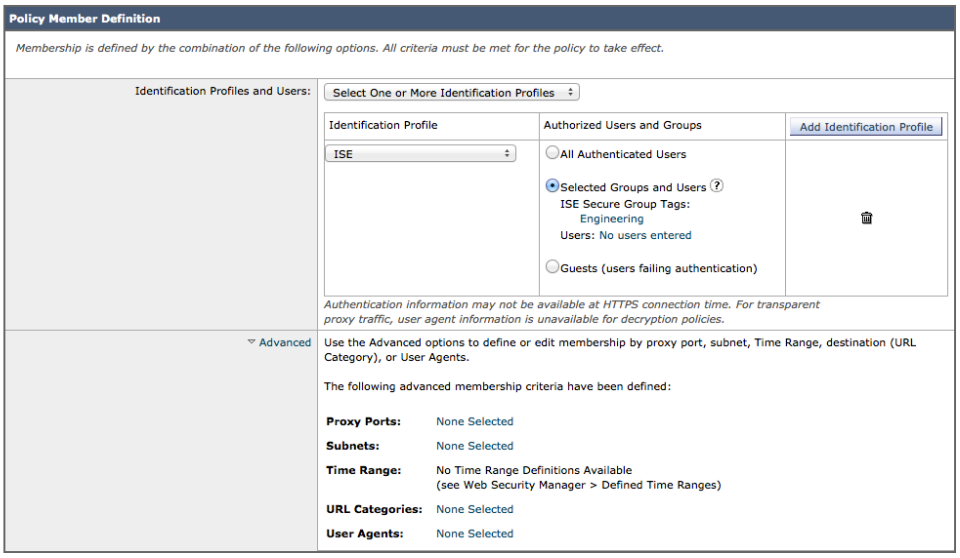


WSA の復号化アプリケーション ポリシーの作成

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [Web ポリシー（Web Policies）] > [復号化ポリシー（Decryption Policies）] > [ポリシーを追加（Add Policy）] > [ポリシーを有効化（Enable Policy）] > [ポリシー名：DecryptEngineerig（Policy Name: DecryptEngineerig）]

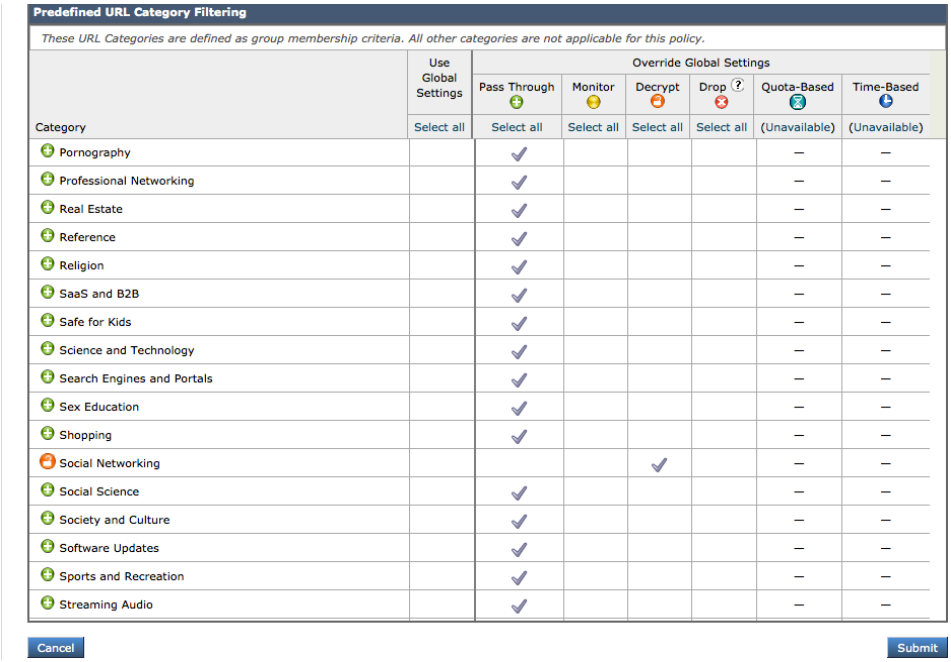


ステップ 2 [識別プロファイルおよびユーザ（Identification Profiles and Users）] > [1 つ以上の識別プロファイルを選択（Select One or More Identification Profiles）] > [ISE] > [ISE セキュア グループ タグ：タグを入力しない（ISE Secure Group Tags: No Tags Entered）] > [エンジニアリング SGT（Engineering SGT）] を選択します。



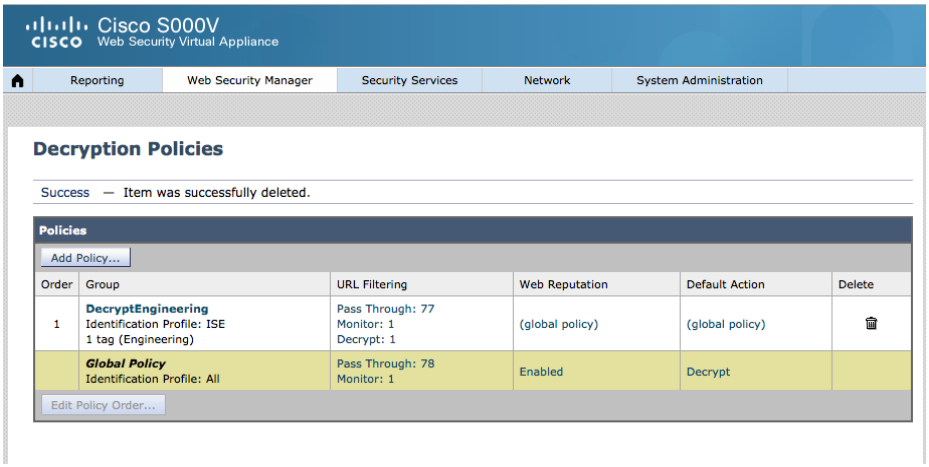
ステップ 3 完了したら、[完了（Done）] > [送信（Submit）] を選択します。

ステップ 4 [URL フィルタリング（URL Filtering）] から、[グローバル ポリシー（Global Policy）] > [パススルー（Pass-through）] に移動し、[すべて選択（Select All）] および [復号化（Decript）] で [ソーシャル ネットワーキング（Social Networking）] を選択します。



ステップ 5 [送信（Submit）] > [確定する（Commit）] をクリックします（2 回）。

ステップ 6 次が表示されます。



アプリケーションの復号化

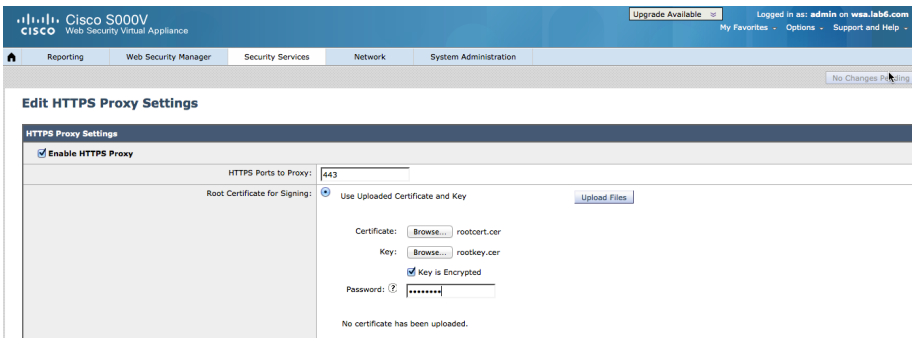
HTTPS プロキシを有効にし、暗号化された Web サイトを復号化できるようにします。次に、ルート公開/秘密キーのペアをアップロードする例を示します。下位の CA テンプレートを使用して CA の署名付き証明書をアップロードするオプションもあります。エンジニアリング SGT が割り当てられているユーザをブロックするため、後でこれを Web アクセス ポリシー内に使用します。

ステップ 1 [セキュリティ サービス（Security Services）] > [プロキシ設定（Proxy Settings）] > [HTTPS プロキシ（HTTPS Proxy）] に移動します。

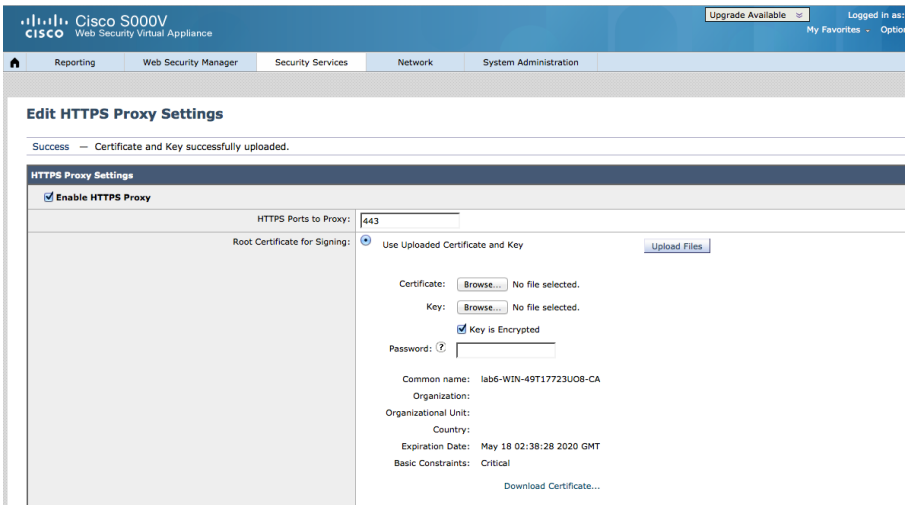
ステップ 2 [設定の有効化および編集（Enable and Edit Settings）] > [プロキシ契約に署名する（Sign Proxy Agreement）] をクリックします。

ステップ 3 [復号化オプション（Decryption Options）] > [エンドユーザの確認応答を復号化:（Decrypt for End-User Acknowledgement）] > [有効（Enable）] > [エンドユーザの確認応答ページを表示するために復号化を有効化（Enable decryption for display of the end-user acknowledge page）]

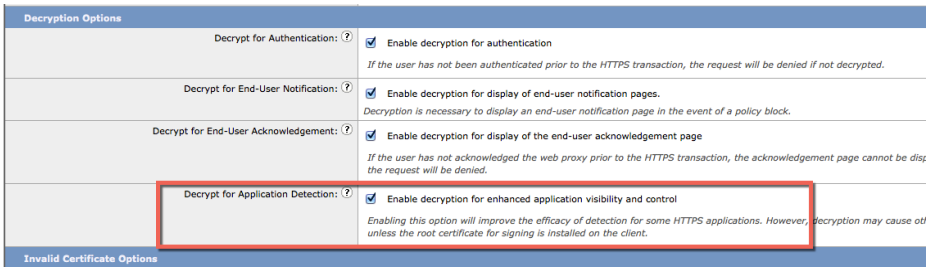
ステップ 4 [セキュリティ サービス（Security Services）] > [アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）] で次に示すように [ルート証明書/秘密キーのペア（Obtaining Root/private key）] からルート証明書と公開/秘密キーのペアを選択し、パスワードを入力します。



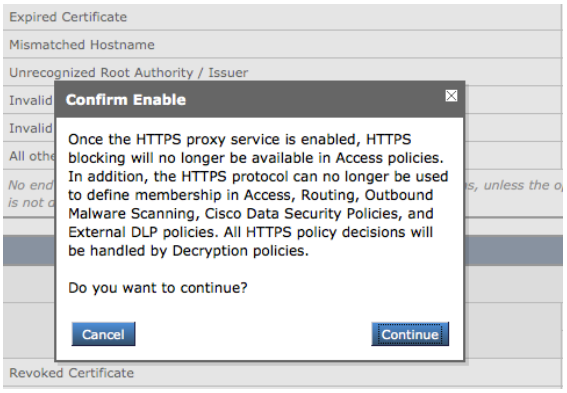
ステップ 5 [ファイルのアップロード（Upload Files）] を選択し、ファイルが正常にアップロードされたことを確認します。



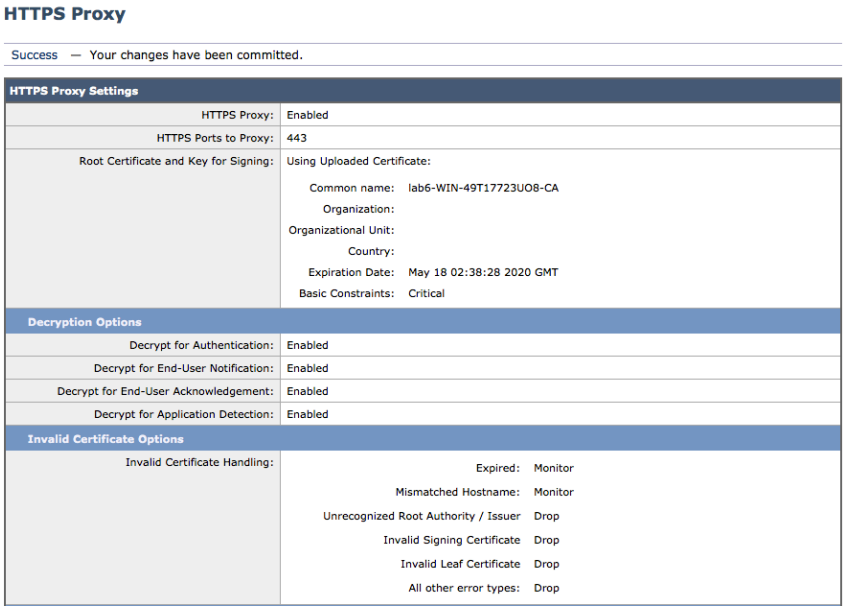
ステップ 6 [アプリケーション検出のために復号化(Decrypt for Application Detection)] で、[高度なアプリケーション可視性のために復号化を有効にする...(Enable decryption for enhanced application visibility…)] を選択します。



ステップ 7 [送信(Submit)] をクリックして次が表示されたら、[続行(Continue)] をクリックします。

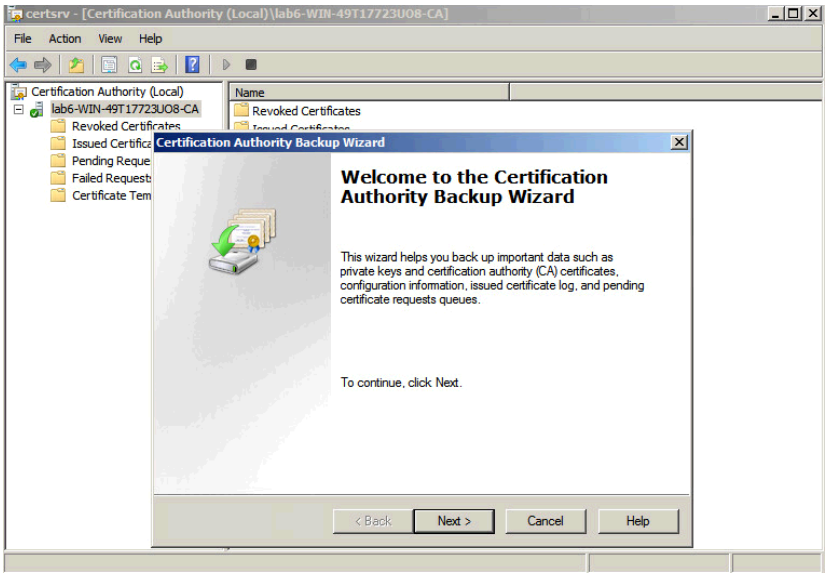


ステップ 8 [変更を送信(Submit Changes)] > [確定する(Commit)] を 2 回クリックします。
ステップ 9 次が表示されます。

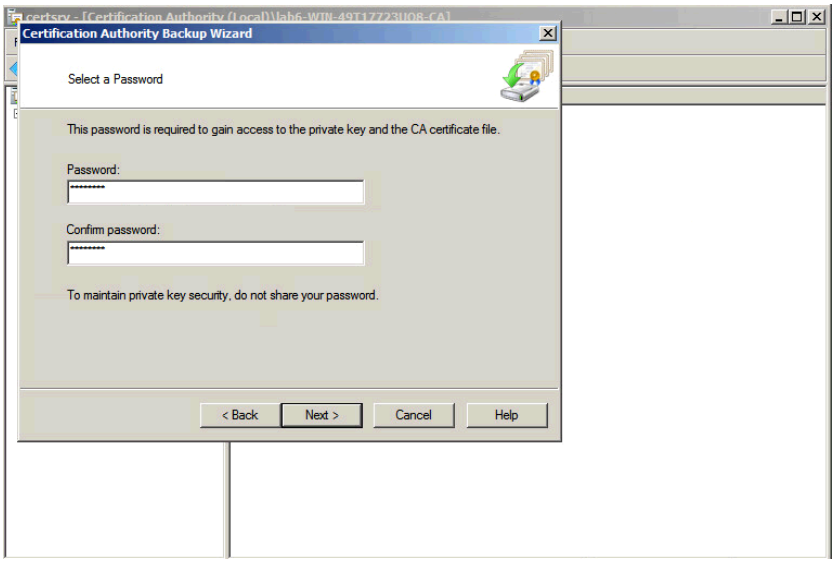


ルート公開キー/秘密キー ペアの取得

ステップ 1 秘密キーを使用して ルート CA をバックアップします。
[CA 機関（CA Authority）] で [PC] を右クリックし、[すべてのタスク（All Tasks）] > [CA をバックアップ（Backup CA）] を選択します。



ステップ 2 [次へ（Next）] を選択します。
ステップ 3 秘密キー、CA 証明書、およびバックアップ場所を選択し、パスワードを入力します。



ステップ 4 [次へ（Next）] を選択します。

ステップ 5 CA が .P12 ファイルとして保存されます。P12 ファイル証明書から秘密/公開キーをエクスポートするには、次のように openssl を使用します。

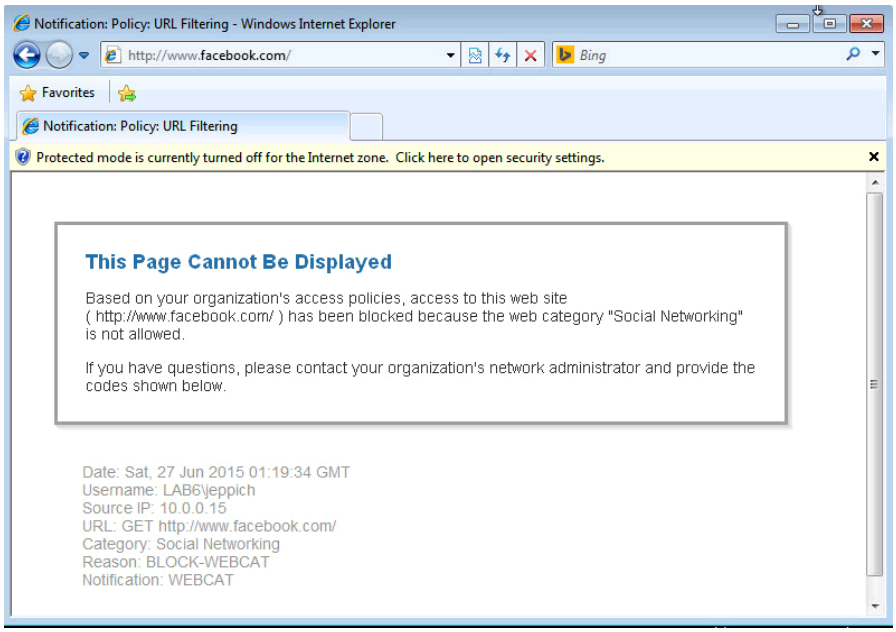
```
openssl pkcs12 -in lab6-WIN-49T17723UO8-CA.p12 -nocerts -out rootkey.cer
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

openssl pkcs12 -in lab6-WIN-49T17723UO8-CA.p12 -clcerts -nokeys -out rootcert.cer
Enter Import Password:
MAC verified OK
```

注: CA バックアップ証明書のエクスポート時に指定したパスワードがインポートと PEM のパスフレーズになります。

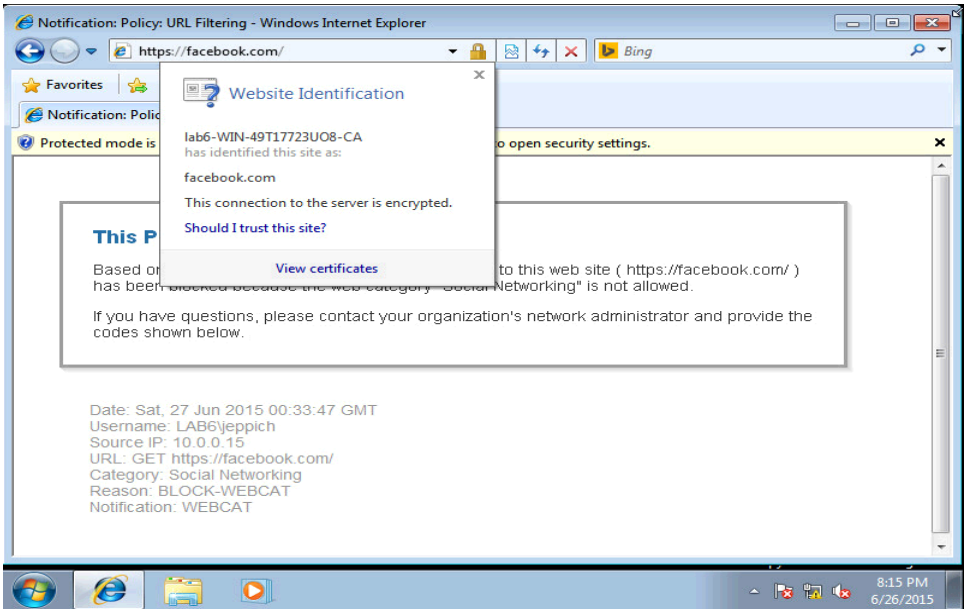
クライアントのテスト

エンドユーザは、最初のポリシー Web アクセスに基づいて認証され、エンジニアリング SGT が割り当てられ、帯域幅がモニタされます。明示的にプロキシが使用されているクライアント PC で、ユーザがブラウザに https://facebook.com と入力します。Internet Explorer のプロキシ設定については「付録」を参照してください。

ステップ 1 ユーザが Facebook にアクセスしようとして www.facebook.com を入力すると、そのアクセスが拒否されます。

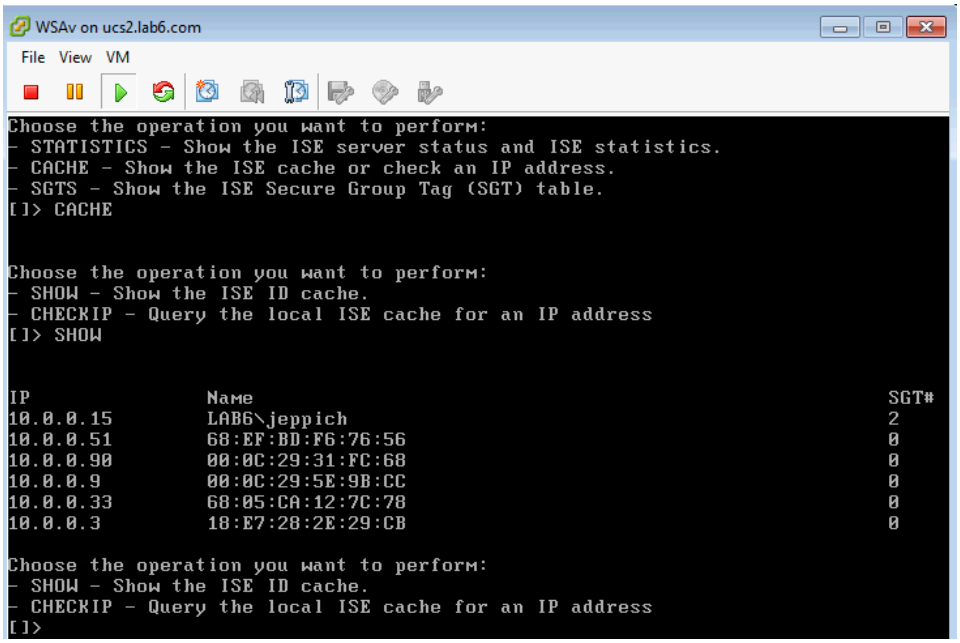


ステップ 2 ユーザが https://facebook.com と入力しても、アクセスは拒否されます。



ステップ 3 仮想 WSAで、次のように入力します。

```
isedata
CACHE
SHOW
```



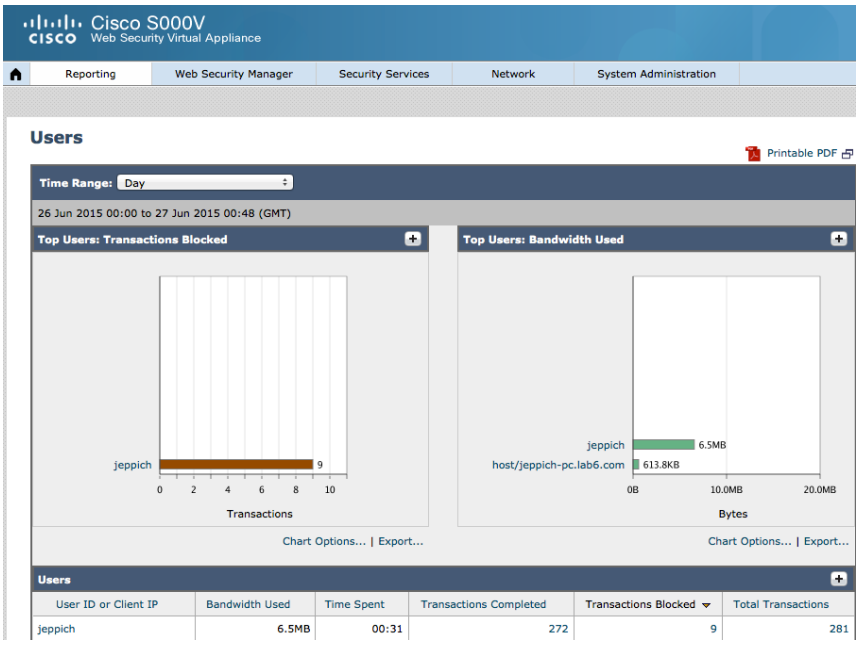
認証済みユーザの SG-IP のマッピングに注意してください。

isedata により、ダウンロードされたタグでの ISE の動作に関する統計情報が表示され、IP-SGT ユーザ名のマッピングが表示されます。

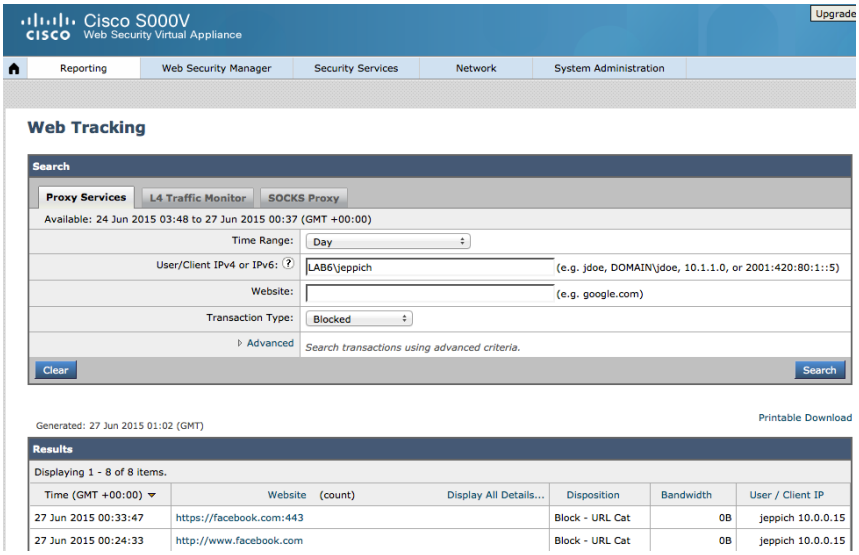
ユーザ レポート

WSA のレポート機能は、Web サイトにアクセスし、Web の使用状況をモニタし、ブロックされた Web トランザクションに関する詳細情報を提供することで、エンドユーザのトラフィック パターンを把握できるようにします。また、レポートには特定の URL からエンドユーザの IP アドレスへのトレースも含まれており、Web トランザクションの詳細情報を提供します。

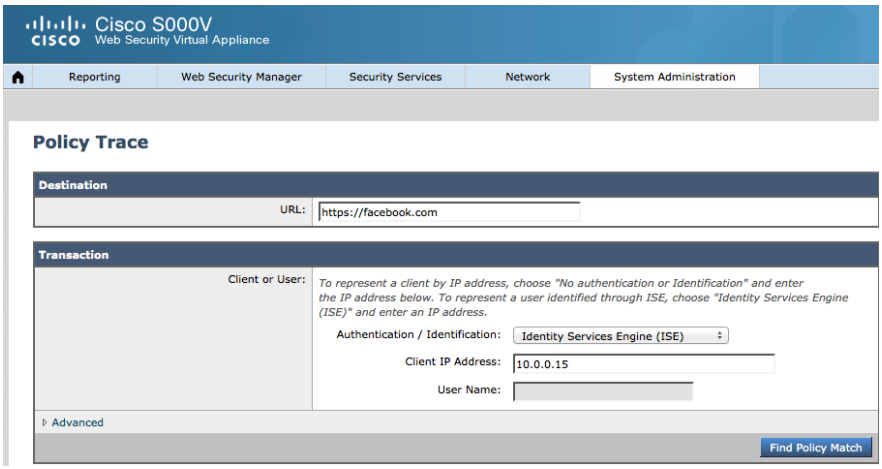
ステップ 1 [レポート(Reporting)] > [ユーザ(Users)] を選択します。このユーザには、ブロックされたトランザクションがいくつかあります。



ステップ 2 レポートで [ブロックされたトランザクション（Transactions Blocked）] を選択し、ブロックされた Facebook のトランザクションの詳細なトランザクションに注目します。

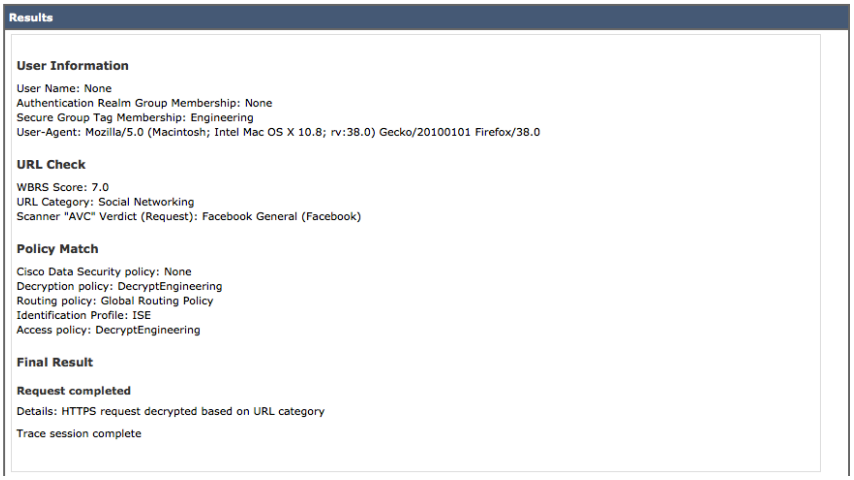


ステップ 3 また、[システム管理（System Administration）] で [ポリシー トレース（Policy Trace）] を選択し、[認証/識別（Authentication/Identification）] に Identity Services Engine（ISE）を選択して、クライアント IP アドレスを入力します。

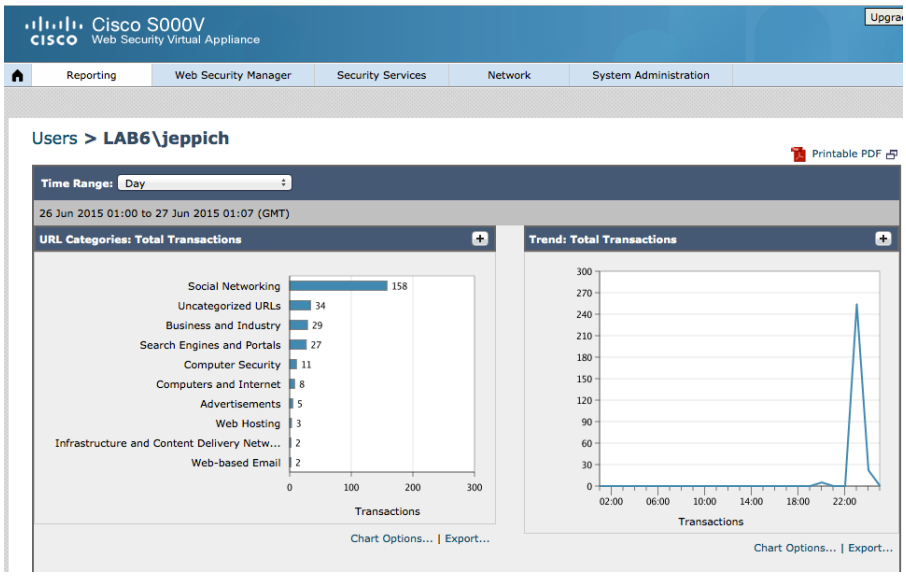


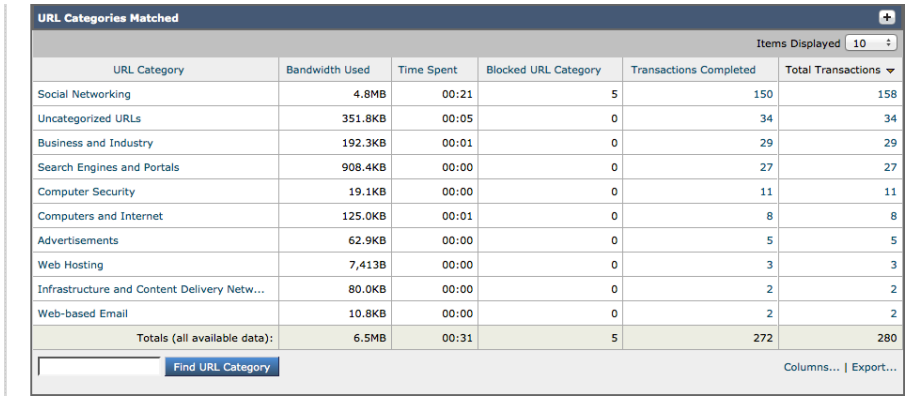
次のポリシー トレースが表示されます。

復号化ポリシーとアクセス ポリシーに注意してください。



ステップ 4 ユーザ レポート全体に、WSA に一致したアクセス ポリシーが表示されます。





Domains Matched

Items Displayed 10

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
akamaihd.net	4.5MB	00:10	117	0	117
facebook.com	323.4KB	00:10	33	8	41
10.0.0.26	351.8KB	00:05	34	0	34
doubleverify.com	109.0KB	00:00	10	0	10
live.com	196.7KB	00:00	10	0	10
omniroot.com	21.9KB	00:00	9	0	9
yimg.com	591.2KB	00:00	8	0	8
digicert.com	7,352B	00:00	6	0	6
yahoo.com	128.6KB	00:00	6	0	6
google.com	10,130B	00:00	5	0	5

Find Domain or IP

Columns... | Export...

Applications Matched

Application	Application Type	Bandwidth Used	Transactions Completed	Other Blocked Transactions	Total Transactions
Facebook General	Facebook	4.8MB	150	0	153
Outlook.com	Webmail	88.5KB	5	0	5
Windows Update	Software Updates	672B	1	0	1
Totals (all available data):	--	4.9MB	156	0	159

Advanced Malware Protection Threats Detected

No data was found in the selected time range

Malware Threats Detected

No data was found in the selected time range

Policies Matched

Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions
DefaultGroup	Decryption	3.1MB	111	0	111
Engineering	Access	367.5KB	65	9	74
Engineering	Decryption	2.0MB	61	0	61
ExemptEngineering	Decryption	1.0MB	28	0	28
DefaultGroup	Access	54.5KB	6	0	6
DecryptEngineering	Decryption	5,201B	1	0	1
Totals (all available data):	--	6.5MB	272	9	281

Find Policy Name

Columns... | Export...

ISE スタンドアロン環境での自己署名証明書を使用した WSA と ISE pxGrid ノードの設定

自己署名証明書を使用した ISE スタンドアロン環境は POC 環境で使用される場合があります。WSA の自己署名証明書は、openssl と keytool があるシステム、通常は Linux システムに作成されます。このドキュメントでは、WSA の秘密キーと CSR 要求を生成し、証明書に自己署名するために MAC が使用されています。

ISE 自己署名証明書は ISE からエクスポートされ、WSA 信頼ストアにインポートされます。ISE スタンドアロン環境では、ISE 識別証明書は、すべての ISE ノードに役立つ自己署名証明書です。この証明書は ISE システム ストアからエクスポートされ、ISE 信頼システム ストアにインポートされます。ISE 識別証明書はエクスポートされると、WSA 信頼証明書ストアにインポートされます。

WSA 自己署名証明書はエクスポートされると、ISE 信頼システム証明書ストアにインポートされます。WSA 自己署名証明書は、WSA 信頼ストアにもインポートされます。自己署名証明書はデフォルトでは信頼されていないため、WSA 信頼ストアにインポートする必要があります。そうしないと、WSA は初期一括セッション レコード情報をダウンロードできず、ISE pxGrid ノードに接続できません。

WSA 復号化ポリシーで使用される HTTPS プロキシ証明書に同じ WSA 自己署名証明書を使用することもできます。

WSA の自己署名証明書の作成

自己署名証明書の公開/キー ペアが作成、生成されます。WSA 自己署名証明書は、WSA と ISE+pxGrid ノードの信頼システム ストアにアップロードされます。この証明書は、HTTPS プロキシ設定にも使用されます。

ステップ 1 WSA の秘密キーを作成します。

```
openssl genrsa -out wsa_self.key 4096
Generating RSA private key, 4096 bit long modulus
.++
........++
e is 65537 (0x10001)
```

ステップ 2 WSA の CSR 要求を秘密キーから生成します。

```
openssl req -new -key wsa_self.key -out wsa_self.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:cisco123
An optional company name []:
```

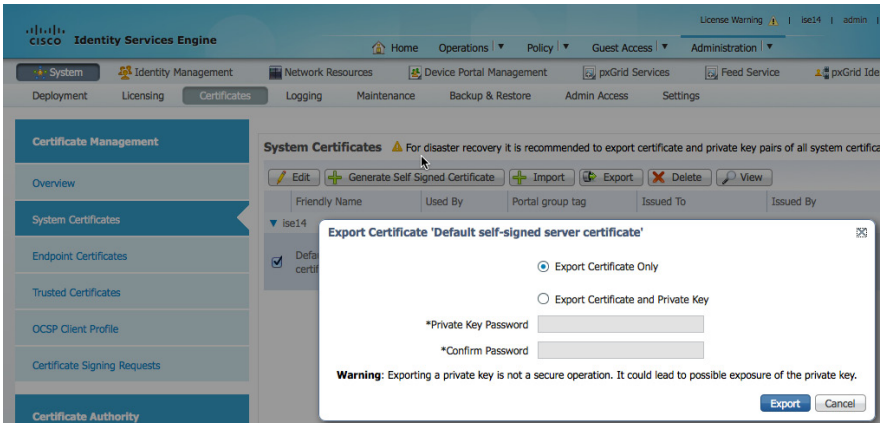
ステップ 3 次を入力し、WSA 証明書に自己署名します。

```
openssl req -x509 -days 365 -key wsa_self.key -in wsa_self.csr -out wsa_self.cer
```

ISE 自己署名識別証明書および ISE pxGrid の設定

ステップ 1 ISE 識別証明書をシステム信頼ストアにエクスポートします。
[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）] > [ISE 識別証明書（ISE Identity Certificate）] を選択 > [エクスポート（Export）] > [証明書のみをエクスポート（Export Certificate Only）]

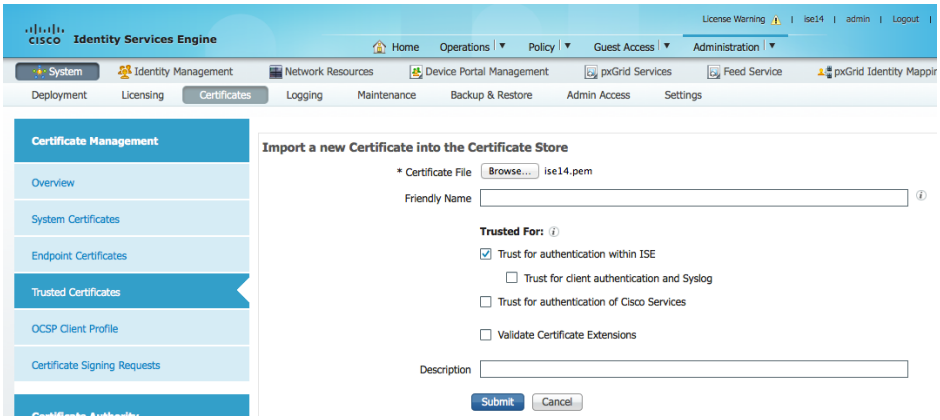
注：秘密キーは不要です。



ステップ 2 defaultsignedservercerti.pem ファイルを保存します。このファイル名は変更することもできます。

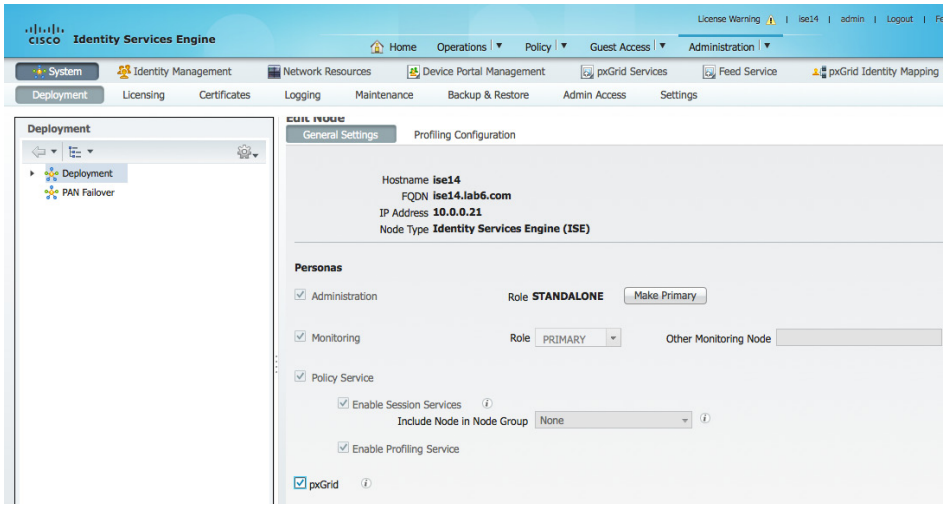
ステップ 3 [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）] > [証明書ファイル（Certificate file）] を選択し、PEM ファイルを選択してアップロードします。

注：[ISE 内での認証について信頼（Trust for Authentication within iSE）] がオンになっていることを確認します。



ステップ 4 [Submit（送信）] をクリックします。

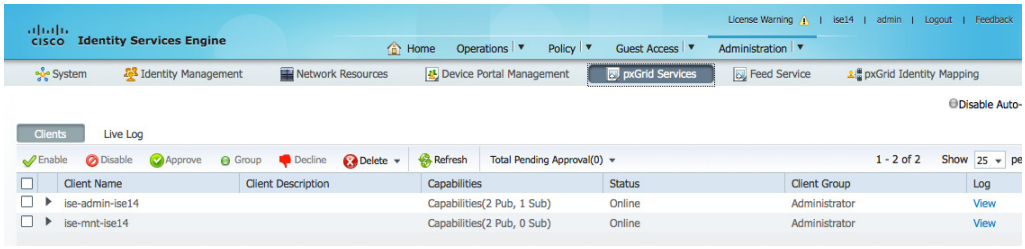
ステップ 5 [管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択し、ISE ノードを選択して [pxGrid] をオンにします。



ステップ 6 [保存（Save）] をクリックします。

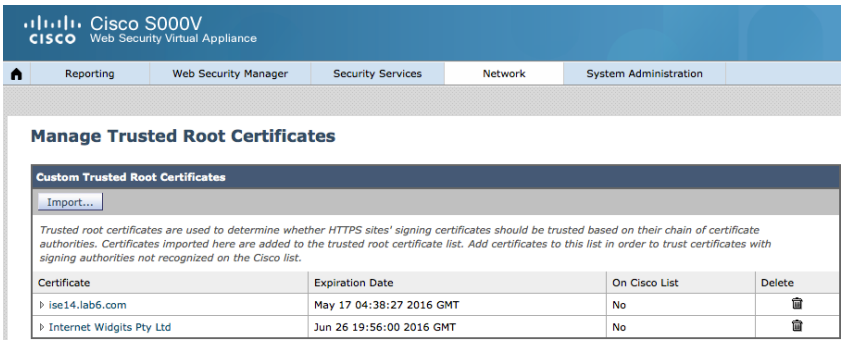
ステップ 7 [管理（Administration）] > [pxGrid サービス（pxGrid Services）] を選択します。ISE 公開ノードが表示されていることを確認します。

注：pxGrid サービスの初期化に 1 分ほどかかる場合があります。

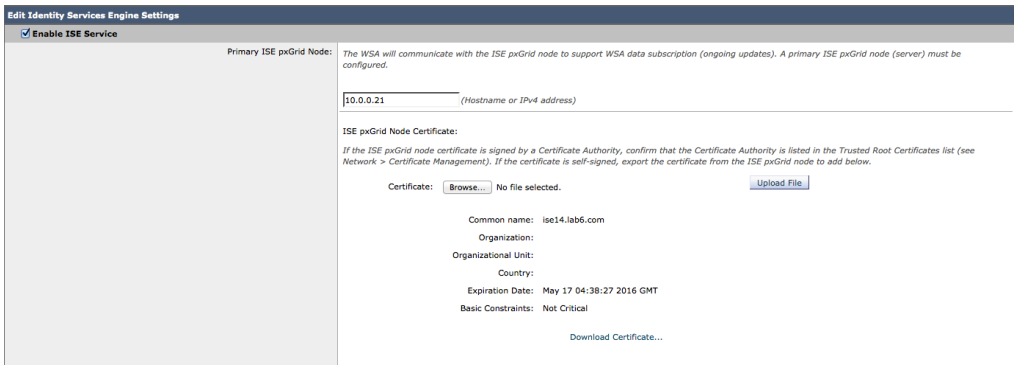


WSA と ISE pxGrid ノードの設定

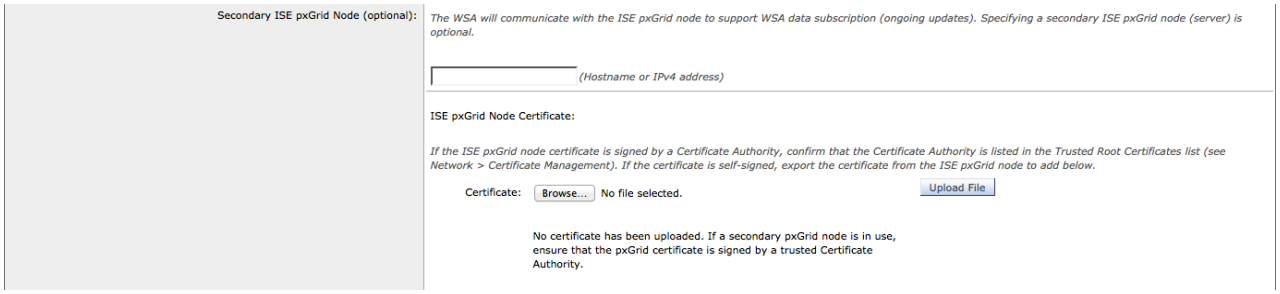
ステップ 1 WSA 信頼ストアに WSA 自己署名証明書と ISE 自己署名識別証明書をアップロードします。
[ネットワーク（Network）] > [証明書の管理（Certificate Management）] > [信頼できるルート証明書の管理（Manage Trusted Root Certificates）] > [ファイルをインポートして送信（Import the files and submit）] > [変更を確定（Commit Changes）]（2 回）を選択します。



ステップ 2 ISE 識別証明書 PEM ファイルを WSA にアップロードします。
[ネットワーク（Network）] > [識別サービス（Identification Services）] > [Identity Services Engine] > [ISE サービスを有効化（Enable ISE Service）] を選択し、ISE+pxGrid IP アドレスまたは FQDN を入力して ISE 識別証明書をアップロードします。

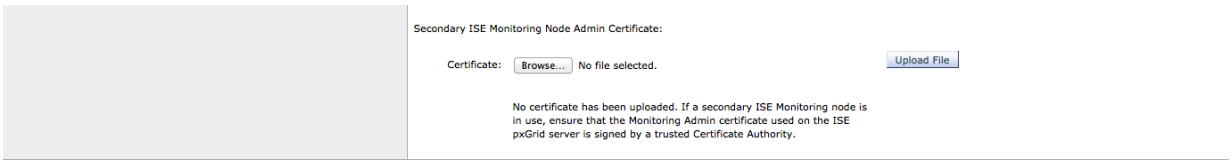


ステップ 3 [セカンダリ ISE+pxGrid ノード（Secondary ISE+pxGrid Node）] は空白のままにします。

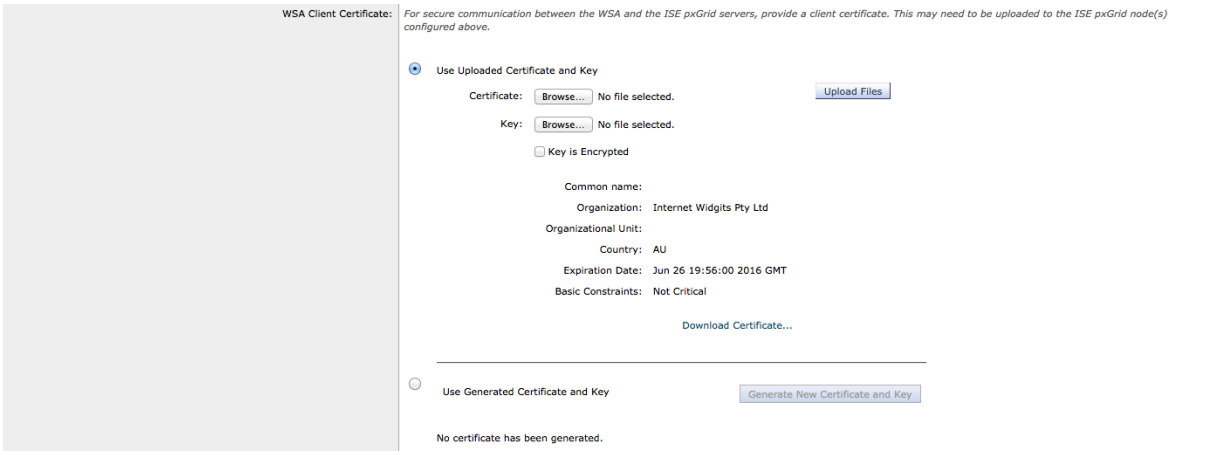


ステップ 4 ISE 識別証明書を MNT ノード証明書としてアップロードします。

ステップ 5 セカンダリ MNT ノードは空白のままにします。



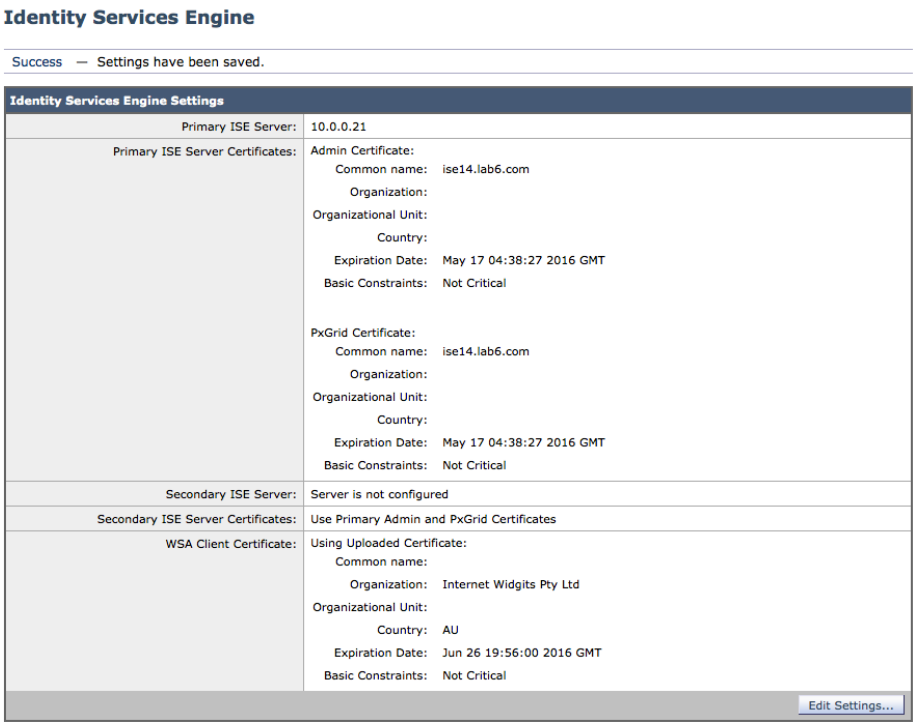
ステップ 6 WSA 自己署名公開証明書と自己署名秘密キーの両方を WSA にアップロードします。



ステップ 7 [ISE サーバとの通信をテスト(Test Communication with ISE server)] > [テスト開始(Start Test)]

```
Checking DNS resolution of ISE pxGrid Node hostname(s)...
Success: Resolved '10.0.0.21' address: 10.0.0.21

Validating WSA client certificate...
Success: Certificate validation successful

Validating ISE PxGrid Node certificate(s) ...
Success: Certificate validation successful

Validating ISE Monitoring Node Admin certificate(s) ...
Success: Certificate validation successful

Checking connection to ISE PxGrid Node(s)...
Success: Connection to ISE PxGrid Node was successful.
Retrieved 3 SGTs from: 10.0.0.21

Checking connection to ISE Monitoring Node (REST server(s)...
Success: Connection to ISE Monitoring Node was successful.
REST Host contacted: ise14.lab6.com

Test completed successfully.
```

ステップ 8 次が表示されます。

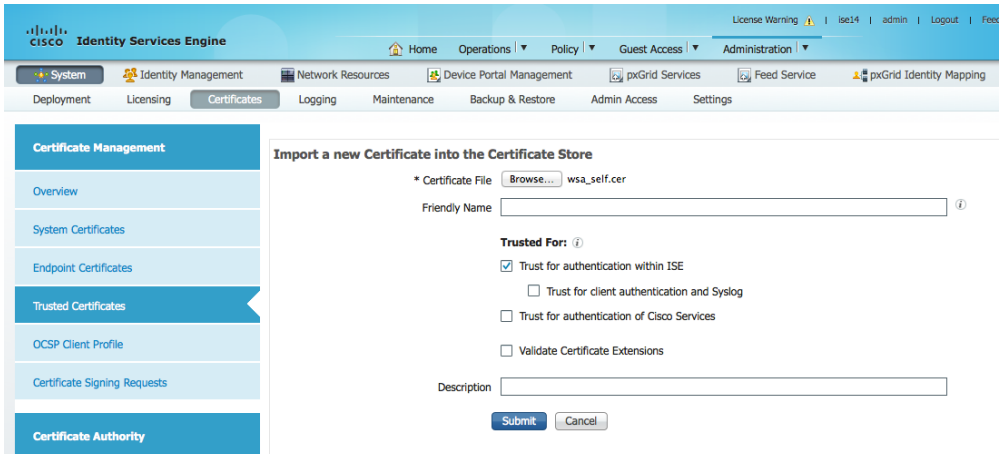


ステップ 9 変更を 2 回確定します。

ステップ 10 ISE 信頼ストアに wsa_self.cer をアップロードします。

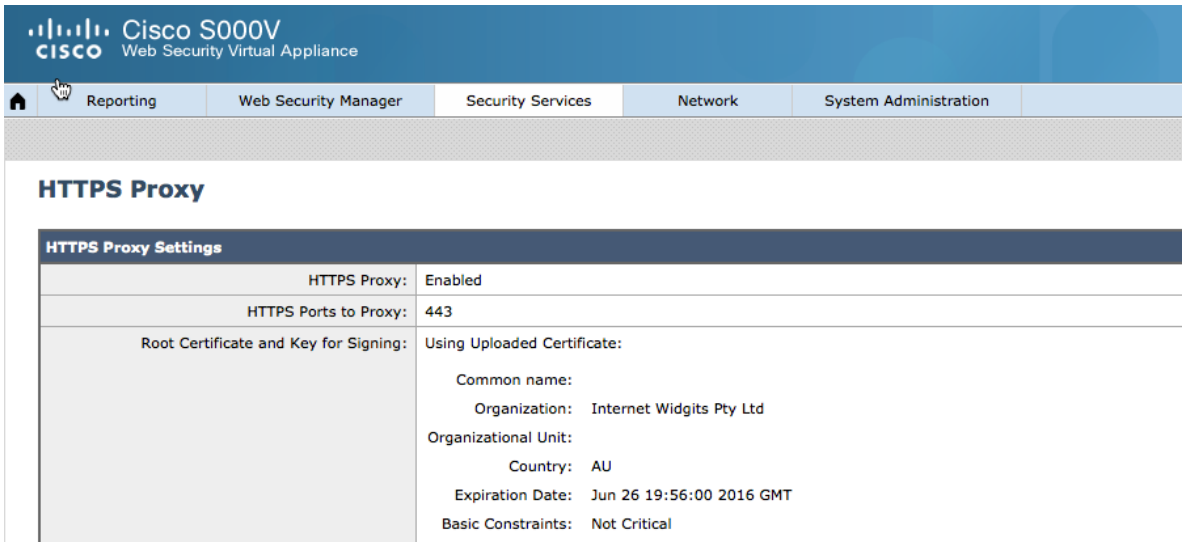
[管理(Administration)] > [証明書(Certificates)] > [証明書の管理(Certificate Management)] > [信頼できる証明書(Trusted Certificates)] を選択し、wsa_self1.cer ファイルをアップロードします。

注:ISE 内での認証の信頼を有効にします。

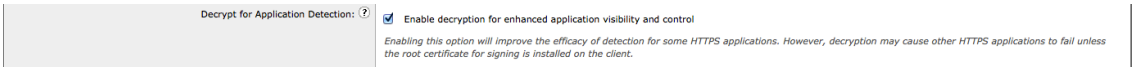


ステップ 11 同じ WSA 自己署名証明書を HTTPS プロキシに使用します。

[セキュリティ サービス(Security Services)] > [HTTP プロキシを有効化(Enable HTTP proxy)] を選択し、自己署名証明書から公開/秘密キーをアップロードします。

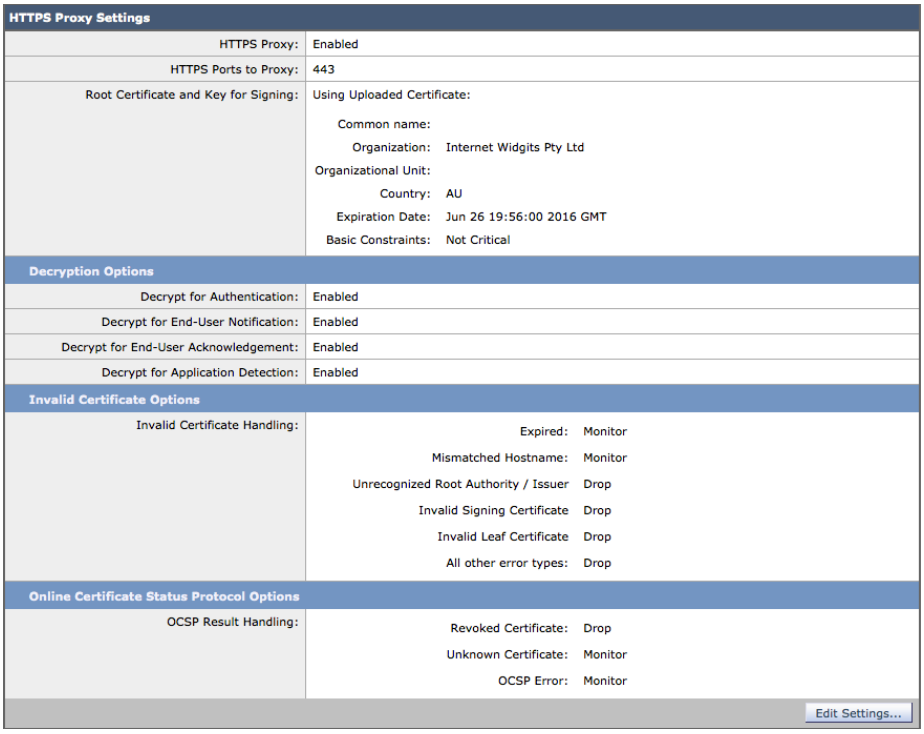


ステップ 12 高度な可視性とセキュリティ用に復号化を有効にします。



ステップ 13 [Submit(送信)] をクリックします。

ステップ 14 次が表示されます。

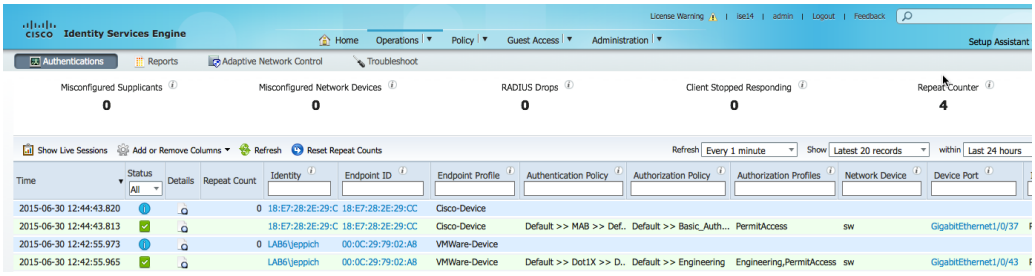


ステップ 15 変更を 2 回確定します。
ステップ 16「ISE を使用した動的セキュリティ タグの割り当て」、「WSA ポリシー」を参照してください。

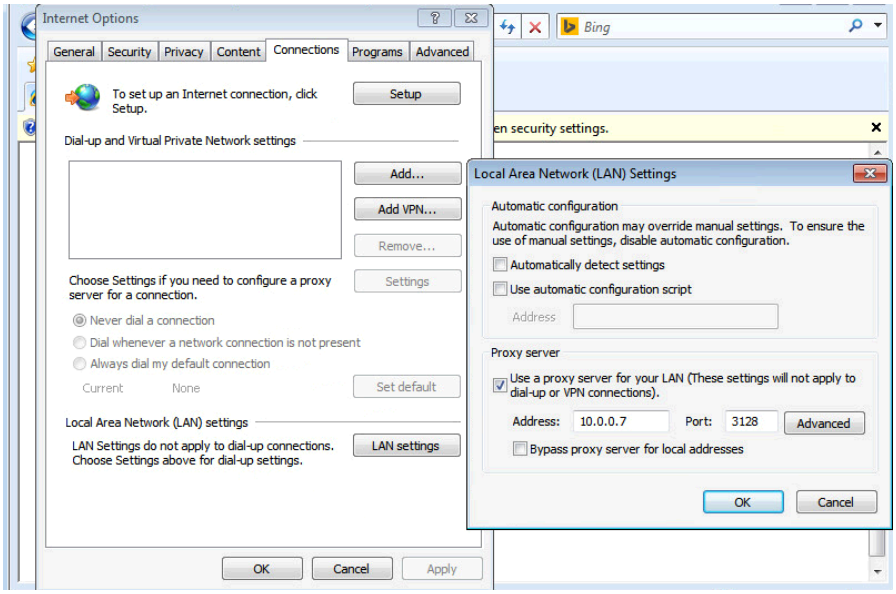
クライアントのテスト

これは、ユーザが正常にログインし、エンジニアリング セキュリティ グループ タグが割り当てられ、WSA によって Facebook アクセスを拒否する場合の使用例と同じです。

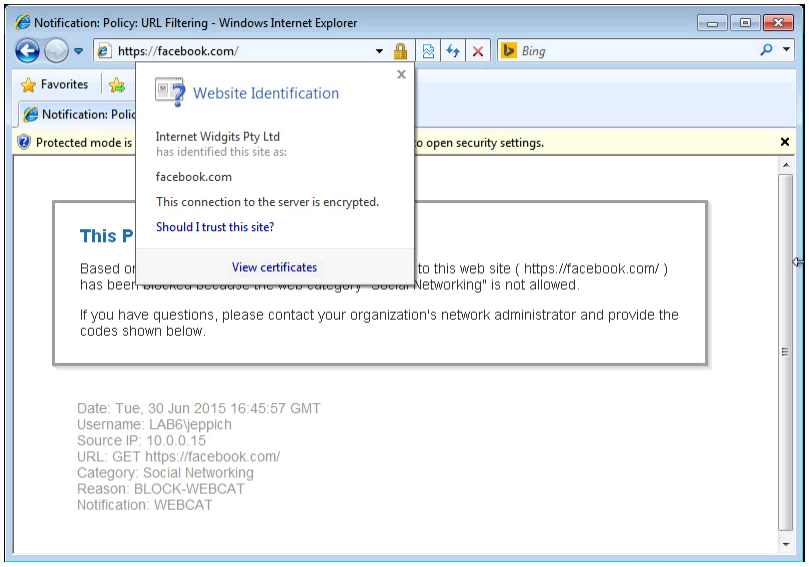
ステップ 1 エンドユーザが正常にログインすると、エンジニアリング SGT が割り当てられます。



ステップ 2 ユーザがプロキシ情報を入力します。



ステップ 3 ユーザが https://facebook.com にアクセスし、そのアクセスが拒否されます。



使用例のシナリオ

ここでは、従業員、請負業者、およびゲストに関する組織の内部 Web セキュリティ ポリシーの使用例を示します。それぞれに、組織の Web セキュリティ ポリシーを表すセキュリティ グループ タグが付与されます。

- 組織の従業員は、Box.com へのアクセスが許可され、Facebook へのアクセスは拒否されます。また、Netflix などのストリーミング メディアに関する帯域幅制限が適用されます。組織の従業員には従業員 SGT が割り当てられます。
- ゲストはスポンサー付きのゲスト ポータルを経由します。このデフォルトのスポンサー ポータルは、ゲストおよび請負業者アイデンティティ グループに所属する ISE 内部ユーザに使用されます。ゲストの組織のセキュリティ Web セキュリティでは、Facebook アクセスを許可し、Box.com アクセスを拒否します。ゲスト SGT は、組織のゲスト ユーザに割り当てられます。
- 請負業者はゲストと同じ Web セキュリティ ポリシーが提供されます。

また、ISE は中央 Web 認証（CWA）用に設定する必要があります。Web トラフィックを ISE にリダイレクトするように、追加の ACL をスイッチに設定する必要があります。ISE にリダイレクトされるように、CWA 用の許可プロファイルが初期のゲストおよび請負業者アクセス用に作成されます。

注：ISE 互換性マトリックス（http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/compatibility/ise_sdt.html）を参照し、ISE がお使いのスイッチをサポートしていることを確認してください。

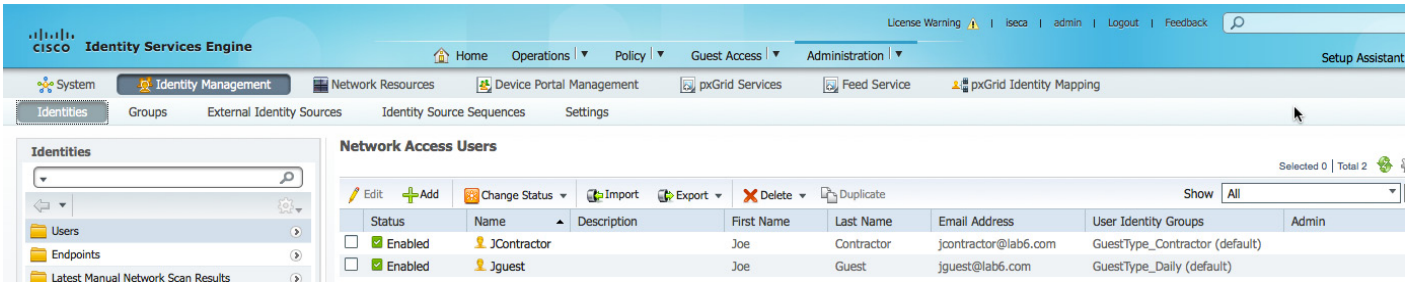
個別の識別プロファイルと Web アクセス ポリシーが、従業員およびゲスト用に定義され、請負業者は WSA で定義されます。

ISE 内部ユーザおよびデフォルトのスポンサー ゲスト ポータル

ISE 内部ユーザはスポンサー ゲスト ポータル用に設定されます。

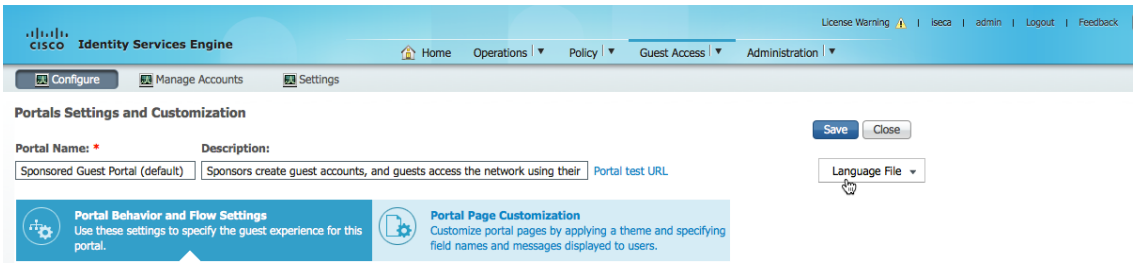
ステップ 1 [管理者（Administrator）] > [ユーザ（Users）] を選択し、下にユーザとアイデンティティ グループを追加します。

ステップ 2 ユーザごとに [送信（Submit）] を選択します。

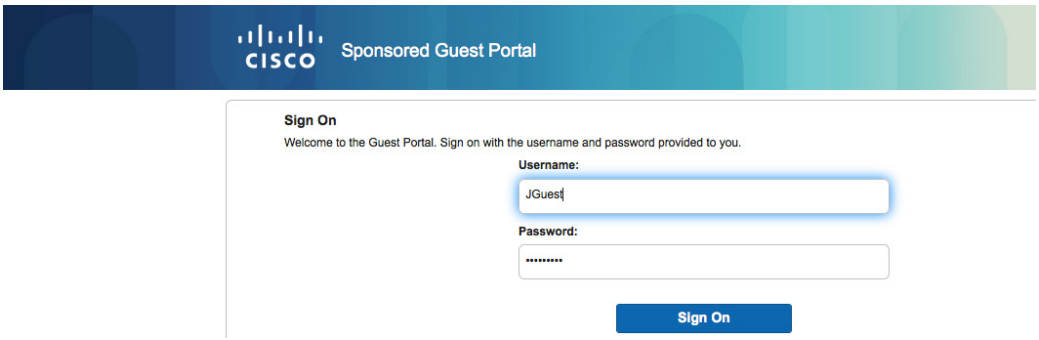


ステップ 3 [ゲスト アクセス(Guest Access)] > [ゲスト ポータル(Guest Portals)] > [スポンサー ゲスト(Sponsor Guest)] を選択し、デフォルトを保持します。

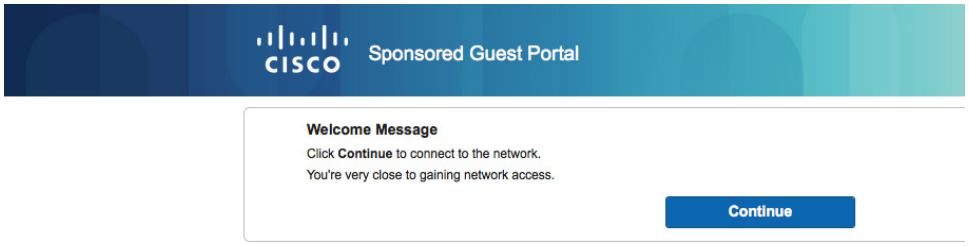
ステップ 4 [ポータル テストの URL(Portal Test URL)] を選択し、ユーザ名を入力して、ISE 内部ユーザをテストします。



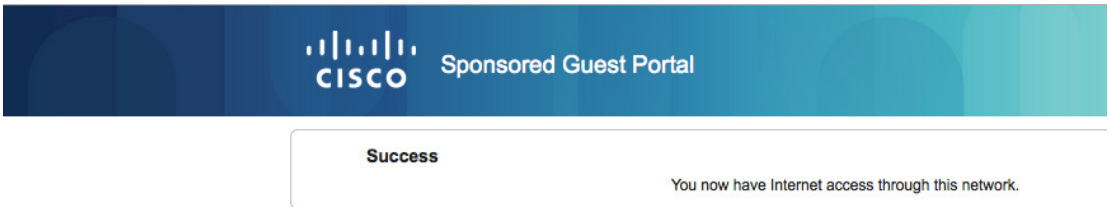
ステップ 5 ユーザ クレデンシャルを入力し、サインインします。



ステップ 6 [サインオン(Sign On)] をクリックします。

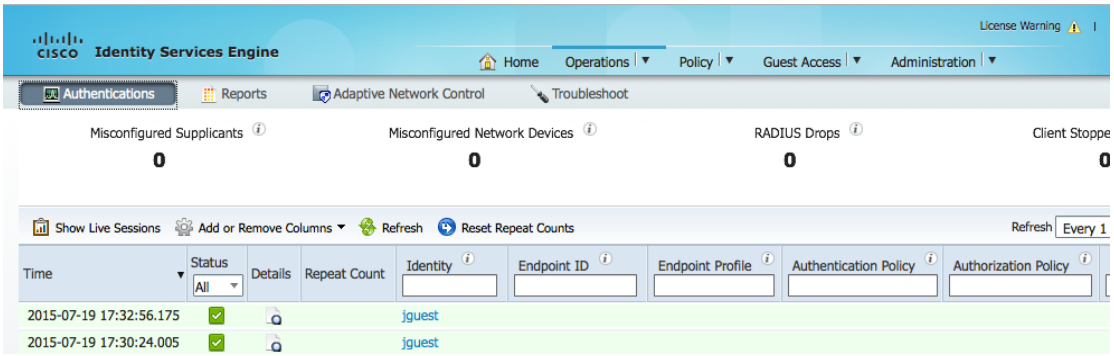


ステップ 7 [Continue(続行)] をクリックします。



ユーザ クレデンシャルのテストが正常に実行されたことを確認します。

ステップ 8 [操作（Operations）] > [認証（Authentications）] を選択します。



ステップ 9 JContractor と同じテスト手順に従います。

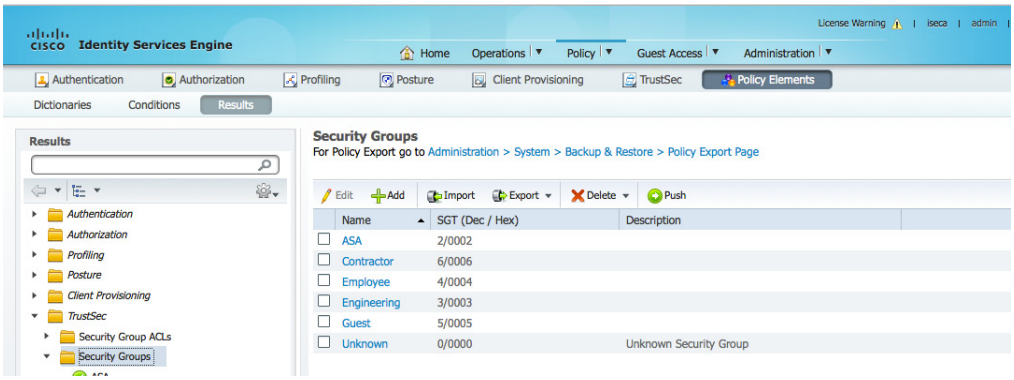
ISE 動的タグ、認可プロファイル、および認可ポリシー

従業員、請負業者、およびゲスト用のセキュリティ グループ タグを作成します。CWA 用の許可プロファイルが作成され、許可ポリシー内の有線 MAB 条件に追加されます。セキュリティ タグの条件ルールおよび関連付けられているセキュリティ グループ タグが許可ポリシーにも適用されます。

動的タグ

従業員、ゲストおよび請負業者の動的タグを作成します。

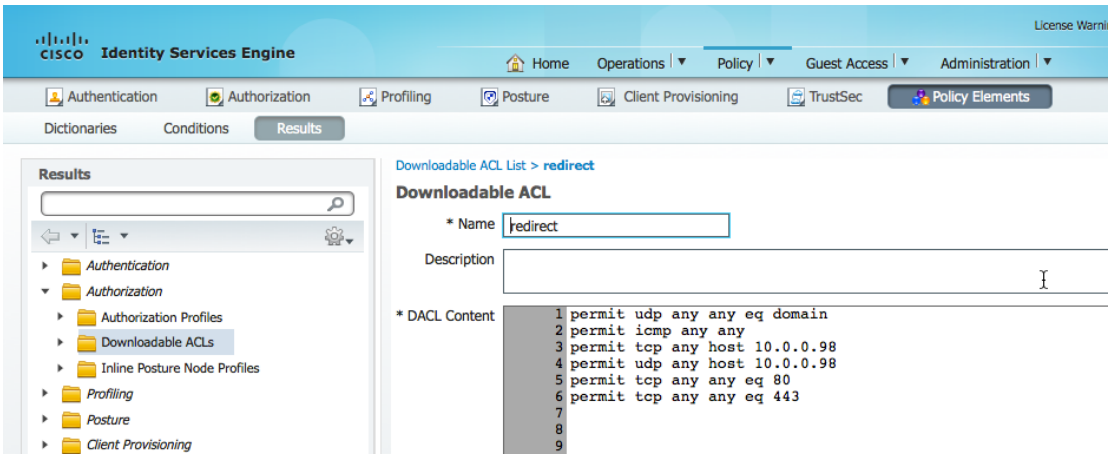
ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [TrustSec] > [セキュリティ グループ）] で従業員、ゲスト、および請負業者用のタグを追加し、送信します。



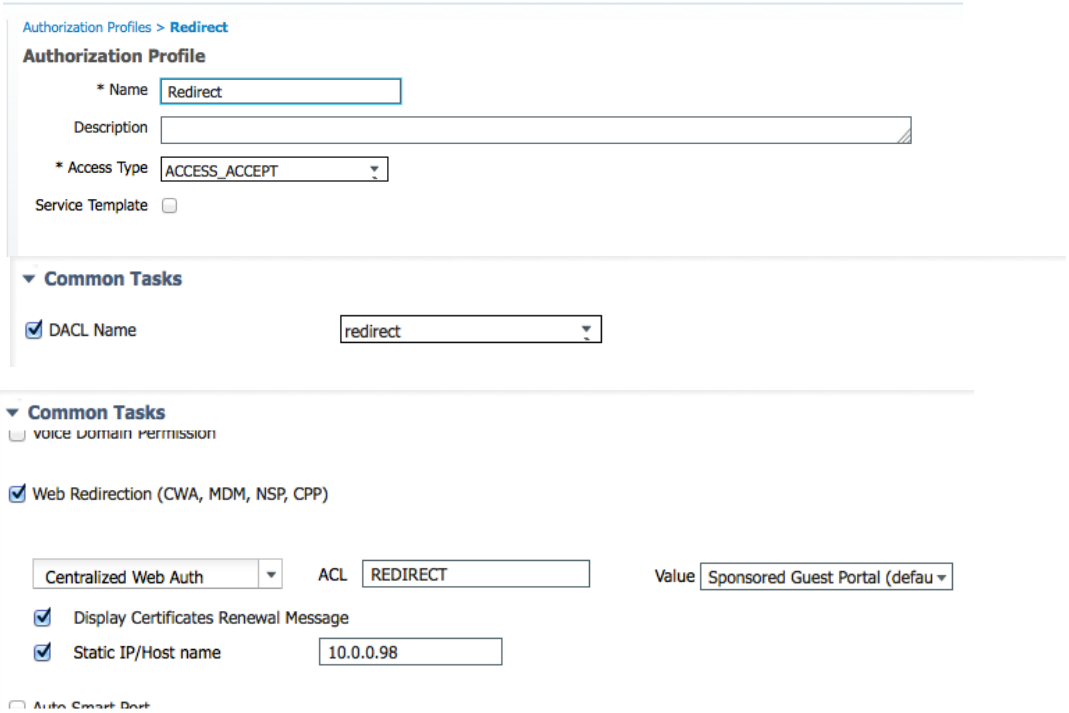
許可プロファイルと CWA 用のダウンロード可能な ACL

ダウンロード可能な DACL がスイッチにプッシュ ダウンされ、ISE へのリダイレクションを許可します。この「リダイレクト」DACL が CWA 用の許可プロファイルに挿入されます。

ステップ 1 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [ダウンロード可能な ACL（Downloadable ACL）] を選択し、DACL のコンテンツを追加して送信します。



ステップ 2 [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [許可プロファイル（Authorization Profiles）] > [名前（Name）] を選択してリダイレクト DACL とリダイレクト スイッチ ACL を追加し、[スポンサー ゲスト ポータル（Sponsored Guest Portal）] を選択します。スタティック IP アドレスは、スタンドアロン ISE 展開の ISE ノードのアドレス、または分散 ISE ノードの ISE PSN ノードのアドレスであり、必須ではありません。

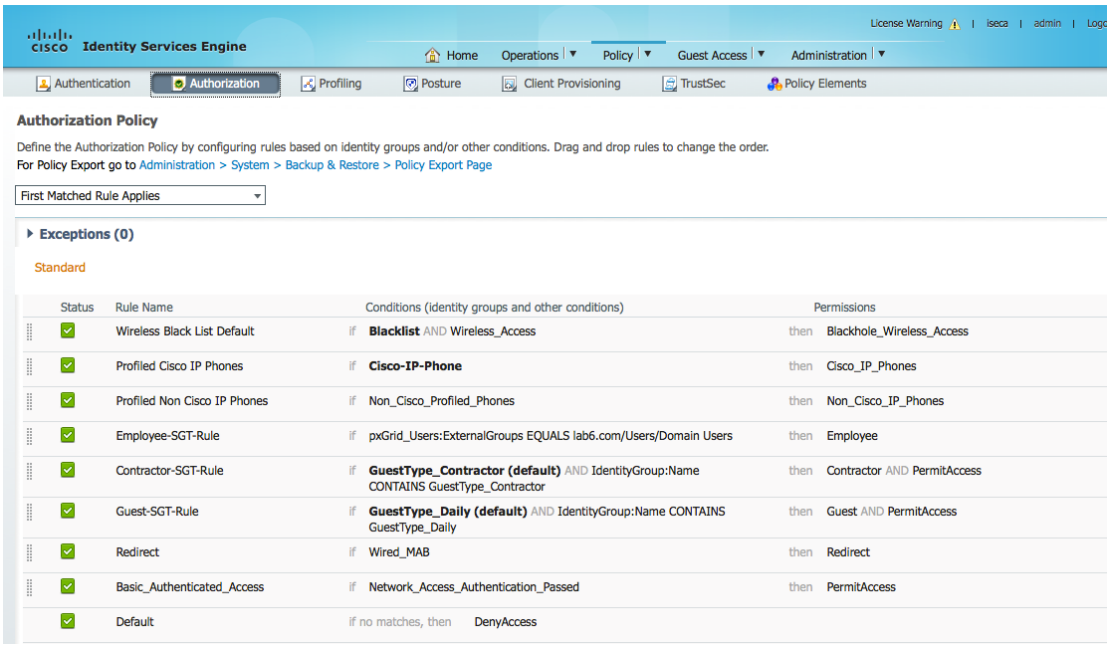


許可ポリシー

許可ポリシーは、従業員、請負業者、ゲストの SGT および有線 MAB ルールを含むように更新されています。

ステップ 1 [ポリシー（Policy）] > [認証（Authorization）] を選択し、従業員 SGT ルール、請負業者 SGT ルール、およびゲスト SGT ルールを追加します。

[従業員 SGT ルール（Employee SGT Rule）]：	ExternalGroup/Domain/Users：Employee SGT
[請負業者 SGT ルール（Contractor SGT Rule）]：	アイデンティティ グループ：GuestType_Contractor（デフォルト） アイデンティティ グループ：名前には GuestType_Contractor が含まれています。 Contractor SGT および Permit Access
[ゲスト SGT ルール（Guest SGT Rule）]：	アイデンティティ グループ：GuestType_Daily（デフォルト） アイデンティティ グループ：名前には GuestType_Daily が含まれています。 Guest SGT および Permit Access



ステップ 2 CWA リダイレクト ルールを追加します。
[リダイレクト ルール（Redirect Rule）] > [ライブラリからの有線 MAB 条件（Wired MAB condition from library）] > [許可プロファイルをリダイレクト（Redirect authorization profile）]

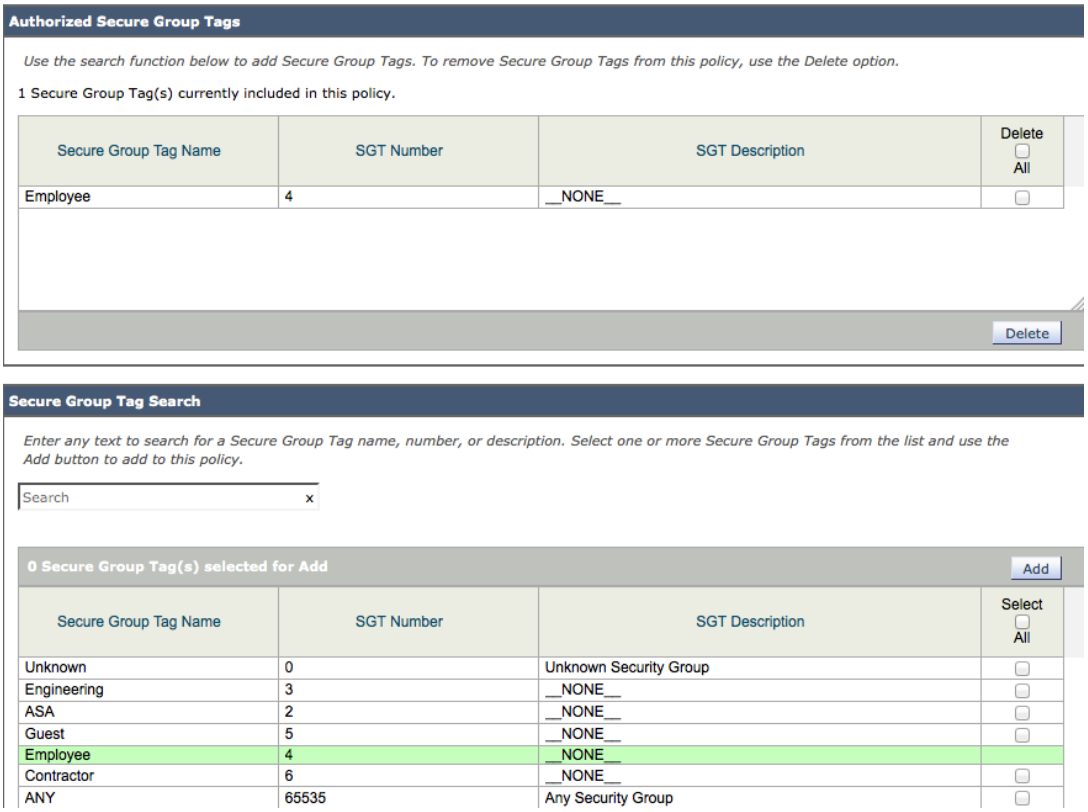
ステップ 3 [保存（Save）] を選択します。

従業員

従業員 WSA 識別プロファイルと Web アクセス ポリシーが作成されます。Web アクセス ポリシーでは、Box.com アクセスを許可し、Facebook アクセスを拒否します。

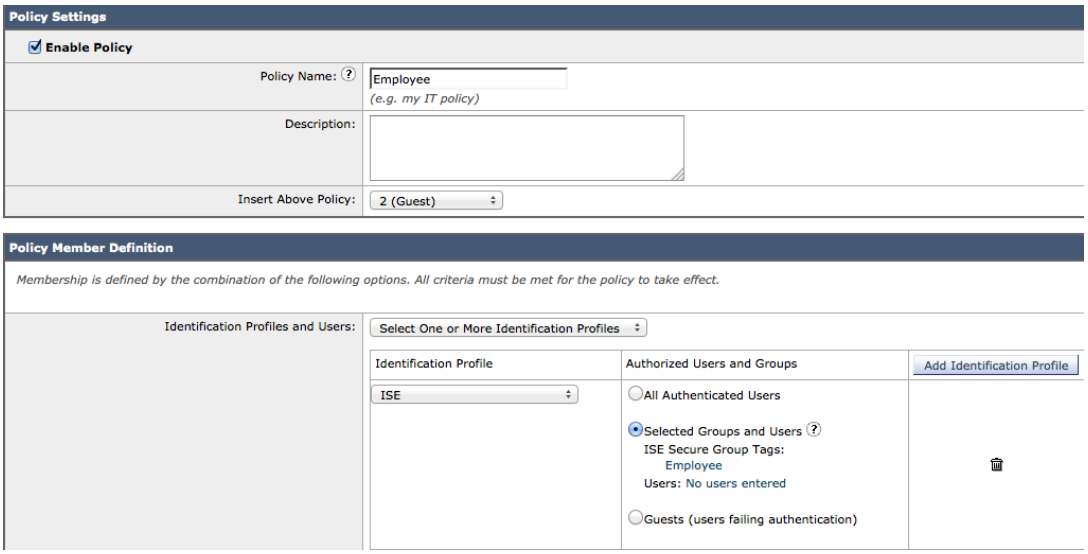
識別プロファイルと Web アクセス ポリシー

ステップ 1 [Web セキュリティ マネージャ(Web Security Manager)] > [Web ポリシー(Web Policies)] > [Web アクセス ポリシー(Web Access Policies)] を選択し、[セキュリティ グループ タグ:ユーザの入力なし(Secure Group Tags; No Users Entered)] をクリックして従業員識別プロファイルを作成し、[セキュリティ グループ タグ名(Security Group Tag Name)] で [従業員(Employee)] を選択します。



ステップ 2 [完了(Done)] をクリックします。

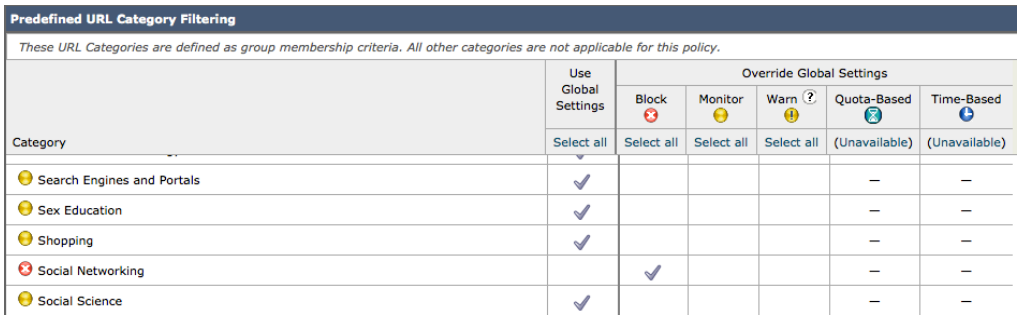
ステップ 3 次が表示されます。



ステップ 4 [送信(Submit)] をクリックし、[変更を確定(Commit Changes)] を 2 回クリックします。
ステップ 5 [URL フィルタリング(URL Filtering)] で [モニタリング(Monitoring)] をクリックします。
ステップ 6 デフォルトでは、ファイル転送サービスは [モニタリング(Monitoring)] に設定され、Box.com アクセスが許可されます。

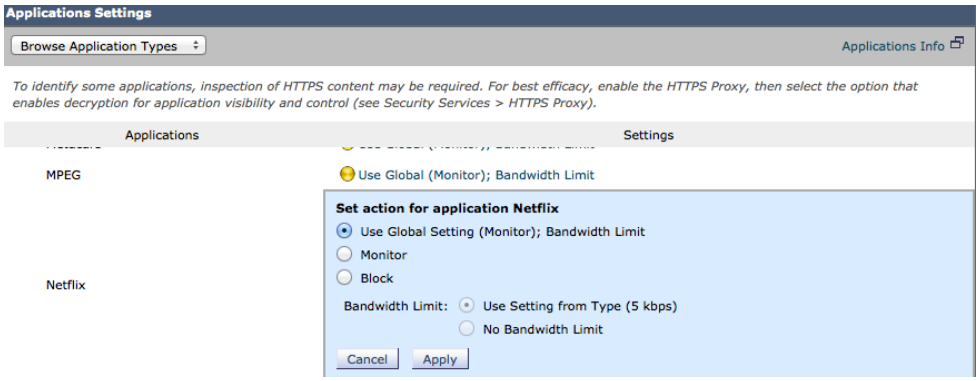
注: www.box.com のカスタム定義の URL カテゴリも、[セキュリティ(Security)] > [カスタム カテゴリ(Custom categories)] で作成されている可能性があります。この場合は、URL カテゴリの下に表示されます。

ステップ 7 Facebook については [ソーシャル ネットワーキング(Social Networking)] に [ブロック(Block)] を選択します。
ステップ 8 [送信(Submit)] をクリックし、[変更を確定(Commit Changes)] を 2 回クリックします。



ステップ 9 [アプリケーション(Applications)] で、[モニタリング(Monitoring)] > [編集(Edit)] > [アプリケーションの設定(Application Settings)] > [アプリケーションのカスタム設定を定義(Define Applications Custom Settings)] を選択します。
ステップ 10 [メディア(Media)] で、[帯域幅制限なし(No Bandwidth Limit)] をクリックし、帯域幅制限を設定して [適用(Apply)] をクリックします。これですべてのメディア タイプに適用されます。

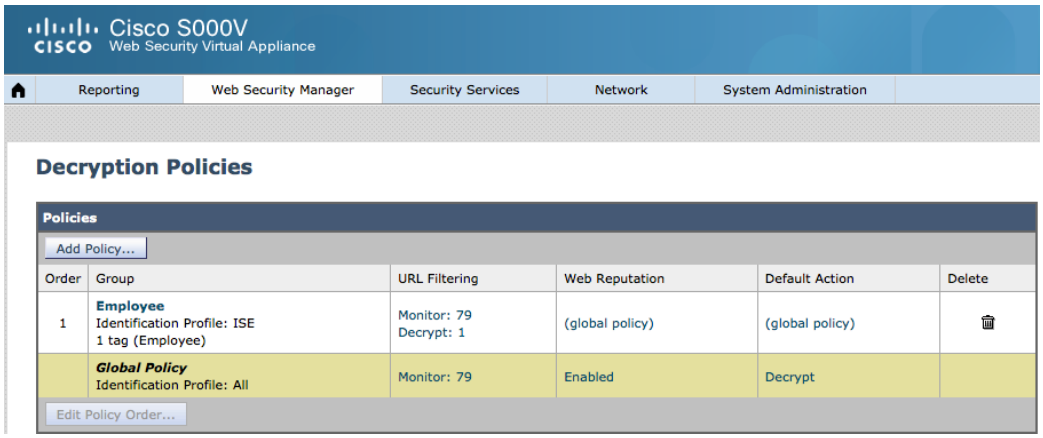
ステップ 11 [メディア（Media）] をクリックし、[Netflix] が選択されていることを確認します。



ステップ 12 [送信（Submit）] > [変更を確定（Commit Changes）] を 2 回クリックします。
ステップ 13 次が表示されます。

2	**Employee** Identification Profile: ISE 1 tag (Employee)	(global policy)	Block: 1 Monitor: 79	Block: 10 Monitor: 368 (Bandwidth Limit: 61)	(global policy)	(global policy)	🗑

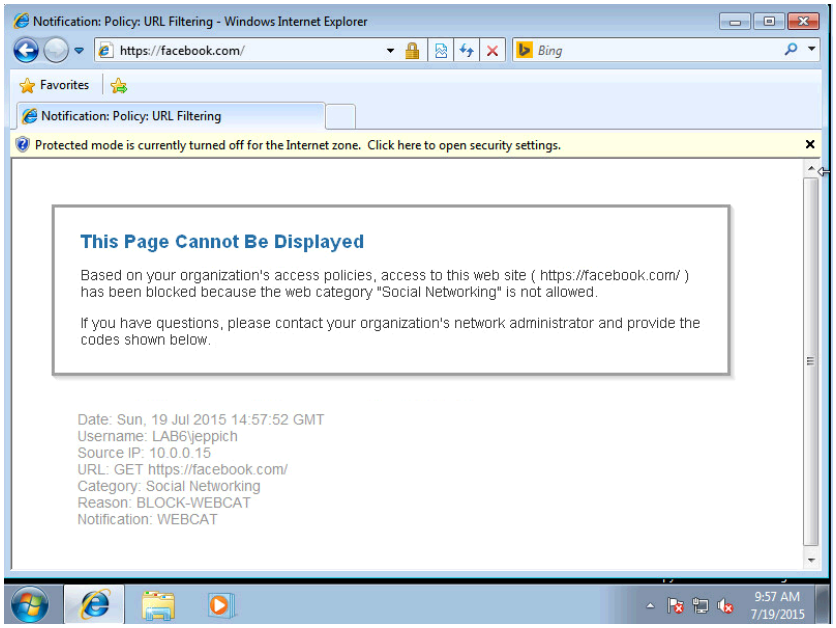
ステップ 14 従業員に Facebook の復号化ポリシーが作成されます。「**アプリケーションの復号化**」を参照してください。



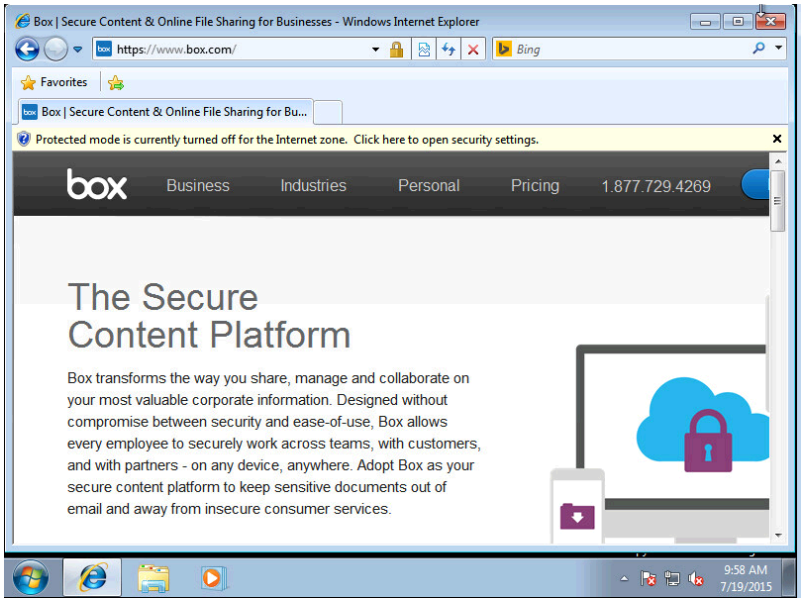
テスト

従業員が正常に認証され、従業員セキュリティ グループ タグが付与され、Facebook アクセスが拒否されて box.com アクセスは許可され、Netflix アクセスは制限されます。

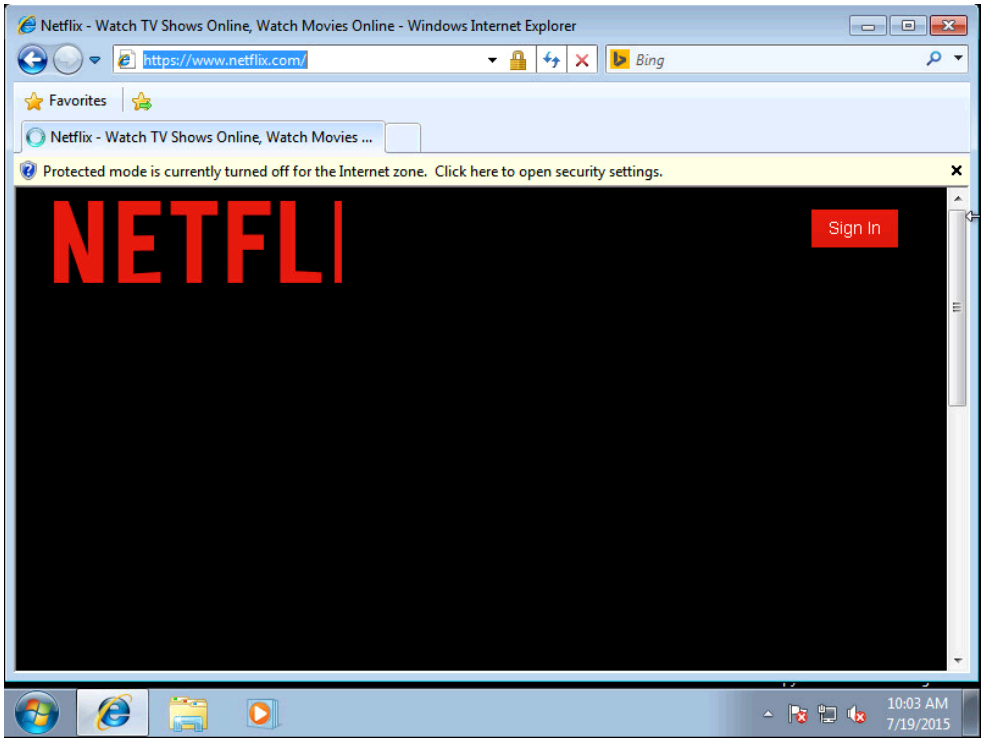
ステップ 1 従業員は、802.1X 経由で正常に認証され、従業員セキュリティ グループ タグが付与され、Facebook アクセスは拒否されます。



ステップ 2 従業員は Box.com にアクセスできます



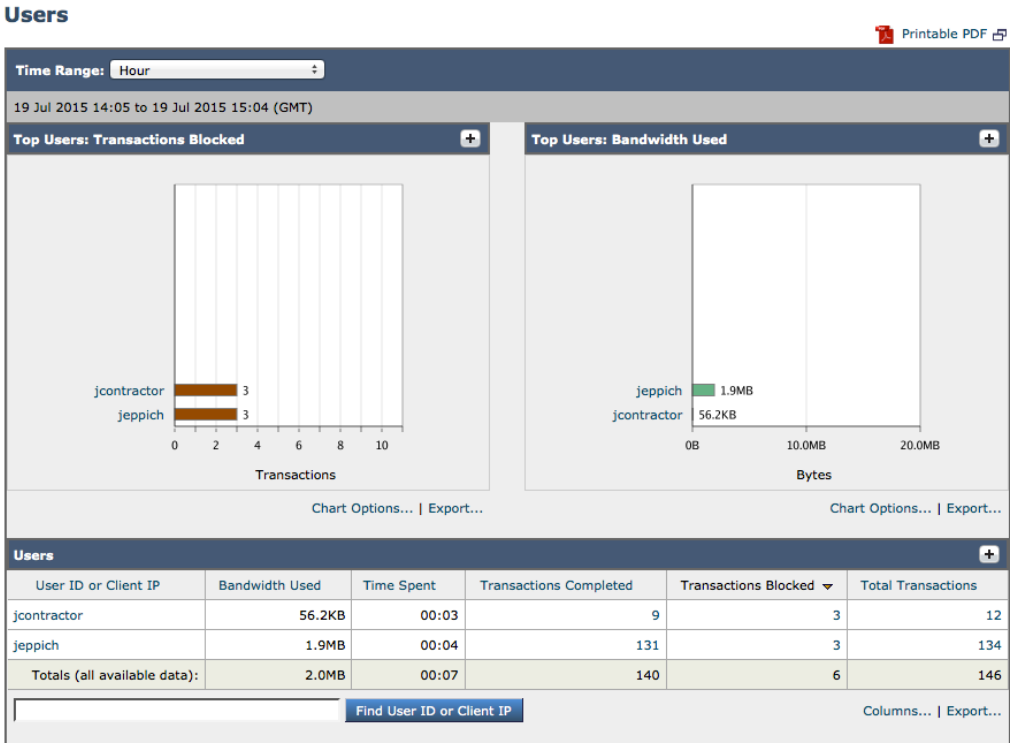
ステップ 3 従業員が Netflix にアクセスすると、ストリーミング メディアの帯域幅制限のために画面表示が低速になっていることがわかります。



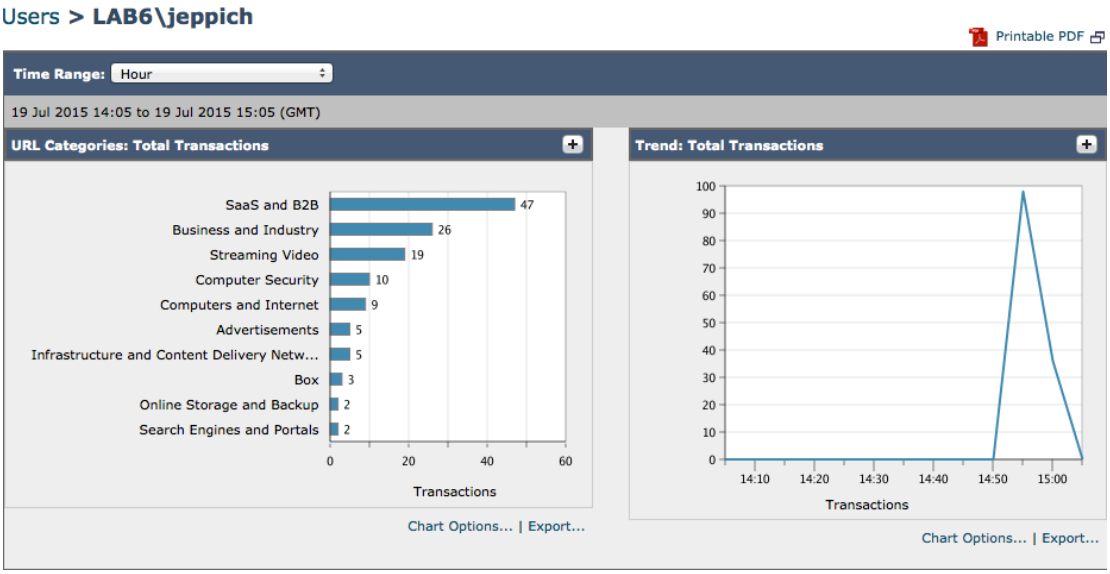
ステップ 4 employee LAB6\jeppich の SGT-IP マッピングを取得するように「ISEDATA」は WSA で動作します

```
- CACHE - Show the ISE cache or check an IP address.
- SGTS - Show the ISE Secure Group Tag (SGT) table.
[]> CACHE


Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[]> SHOW


IP              Name                                                  SGT#
10.0.0.15       LAB6\jeppich                                          4
10.0.0.98       00:0C:29:35:48:2A                                     0
169.254.57.162  00:0C:29:C7:16:48                                     0
10.0.0.22       00:0C:29:CA:A3:8F                                     0
10.0.0.33       68:05:CA:12:7C:78                                     0
10.0.0.21       jcontractor                                           6
10.0.0.3        18:E7:28:2E:29:CC                                     0

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[]>
```

ステップ 5 [レポート(Reporting)] > [ユーザ レポート(Users Report)] を選択します。jeppich にはブロックされたトランザクションが 3 つあり、一部の帯域が使用されています。



ステップ 6 [jeppich] をクリックし、ドリル ダウンして、Box のトランザクション、ブロックされた Facebook アクセス、ストリーミング メディアの帯域幅、および一致した Web アクセス従業員ポリシーを表示します。



URL Categories Matched

Items Displayed 10

URL Category	Bandwidth Used	Time Spent	Blocked URL Category	Transactions Completed	Total Transactions
SaaS and B2B	921.1KB	00:00	0	47	47
Business and Industry	123.7KB	00:00	0	26	26
Streaming Video	734.6KB	00:02	0	19	19
Computer Security	13.8KB	00:00	0	10	10
Computers and Internet	49.7KB	00:00	0	9	9
Advertisements	7,559B	00:00	0	5	5
Infrastructure and Content Delivery Netw...	4,218B	00:00	0	4	5
Box	26.0KB	00:00	0	3	3
Online Storage and Backup	4,297B	00:00	0	2	2
Search Engines and Portals	55.2KB	00:00	0	2	2
Totals (all available data):	1.9MB	00:04	2	131	134

Find URL Category

Columns... | Export...

Applications Matched

Application	Application Type	Bandwidth Used	Transactions Completed	Other Blocked Transactions	Total Transactions
Box.net	File Sharing	947.8KB	48	0	48
Netflix	Media	734.6KB	19	0	19
Google Analytics	Internet Utilities	16.5KB	4	0	4
Facebook General	Facebook	0B	0	2	2
LinkedIn General	LinkedIn	1,909B	1	0	1
Windows Update	Software Updates	676B	1	0	1
Totals (all available data):	--	1.7MB	73	2	75

Find Application

Columns... | Export...

Advanced Malware Protection Threats Detected

No data was found in the selected time range

Malware Threats Detected

No data was found in the selected time range

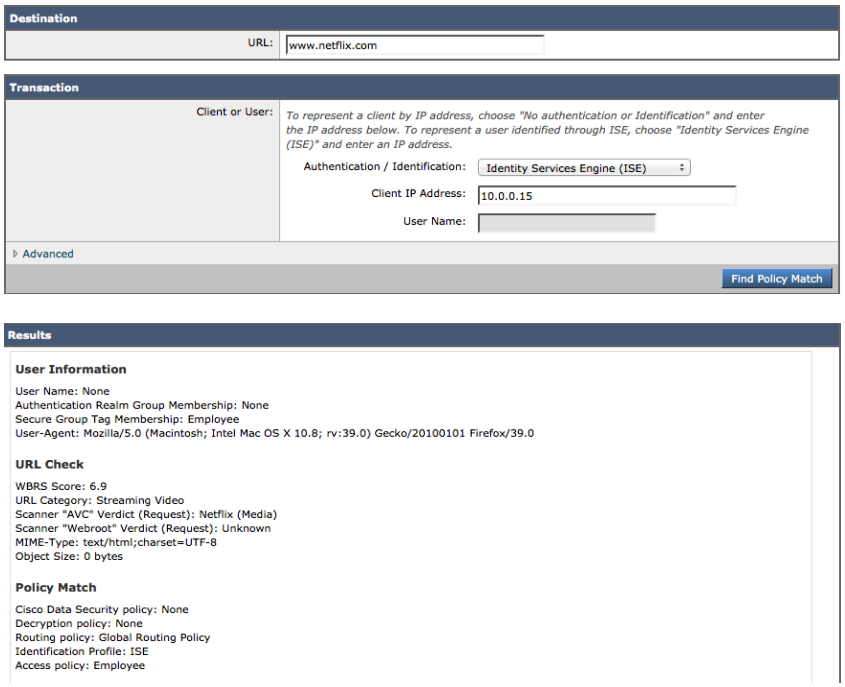
Policies Matched

Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions
Employee	Access	1.3MB	118	3	121
Employee	Decryption	676.7KB	13	0	13
Totals (all available data):	--	1.9MB	131	3	134

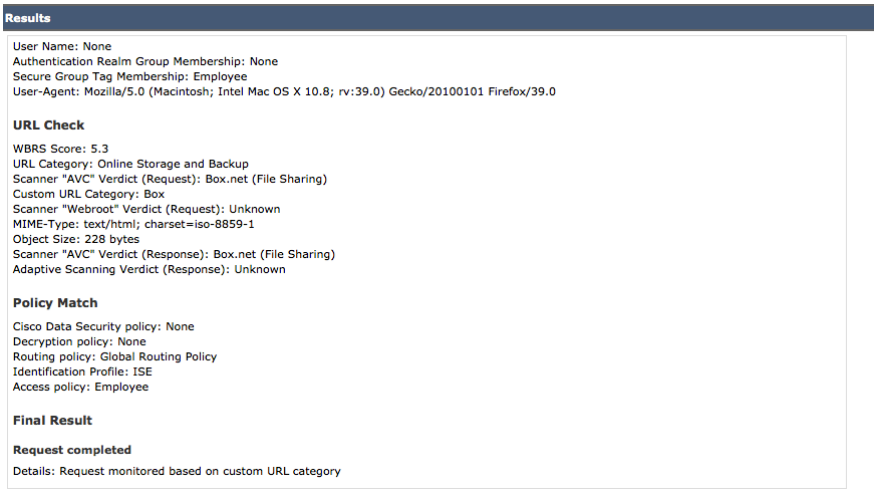
Find Policy Name

Columns... | Export...

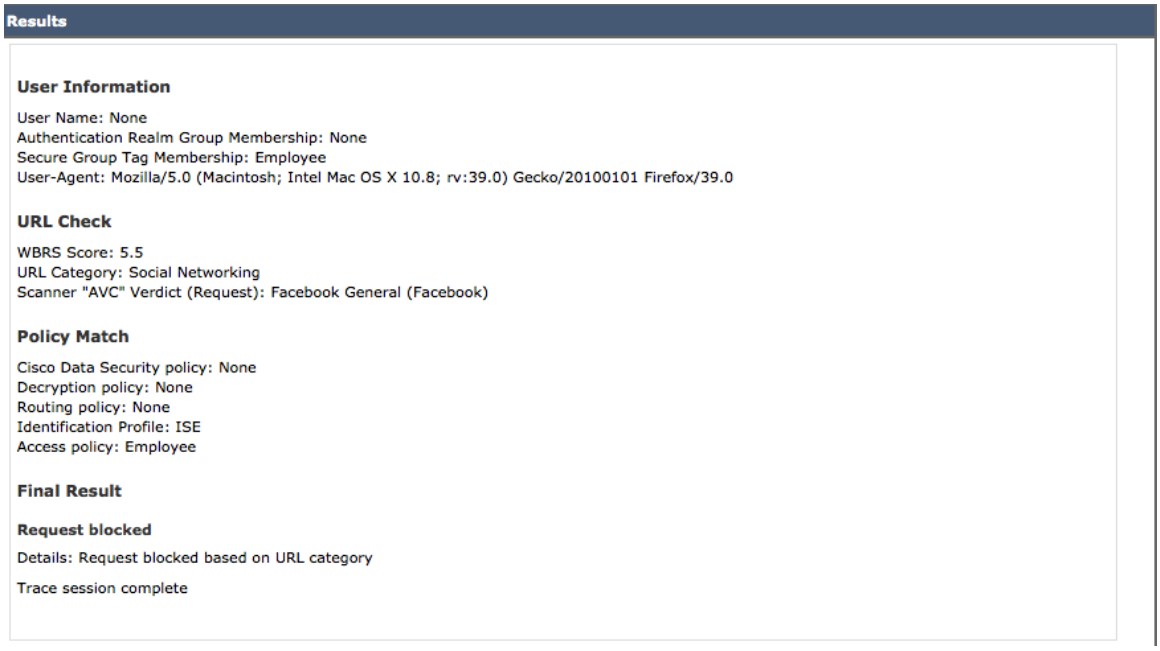
ステップ 7 [システム管理者（System Administrator）] > [ポリシー トレース（Policy Trace）] を選択します。Netflix のポリシー トレースと従業員の照合 Web アクセス ポリシーに注意してください。



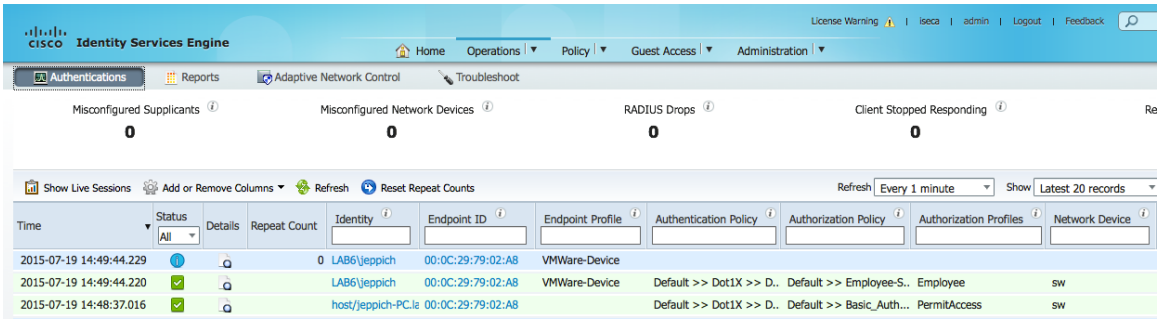
ステップ 8 Box のポリシー トレースと従業員の照合 Web アクセス ポリシーに注意してください。



ステップ 9 Facebook のポリシートレースと従業員の一致 Web アクセス ポリシー、およびブロックされたトランザクションに注意してください。



ステップ 10 [操作(Operations)] > [認証(Authentications)] を選択し、認証済みユーザと従業員セキュリティ グループ タグの割り当てを表示します。

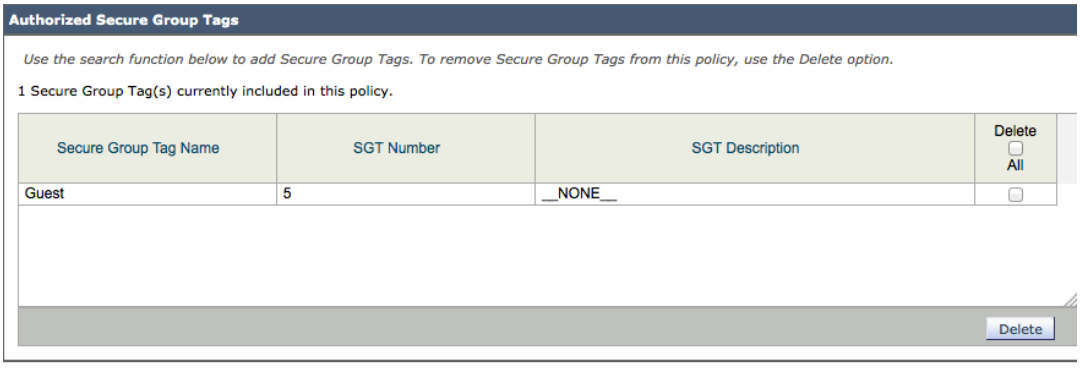


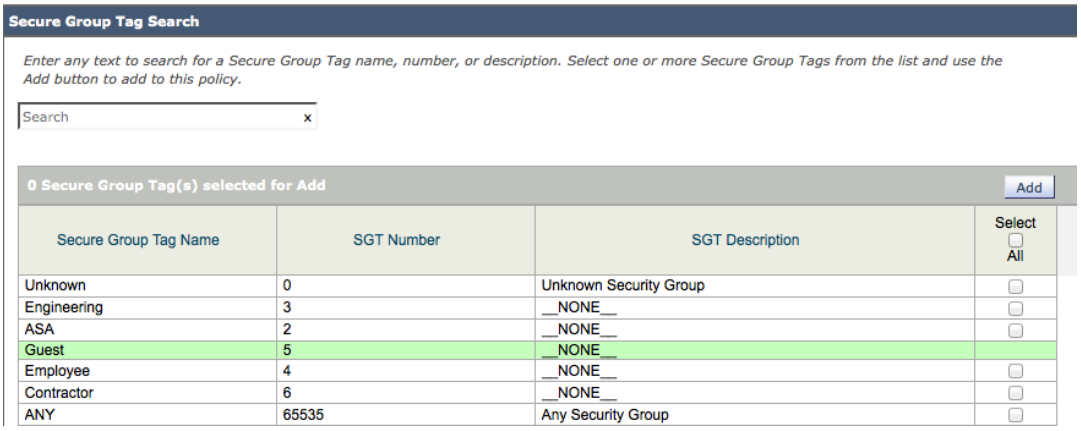
ゲスト

ゲスト用の WSA 識別プロファイルと Web アクセス ポリシーが作成されます。この Web アクセス ポリシーでは、Box アクセスを拒否し、Facebook アクセスを許可します。

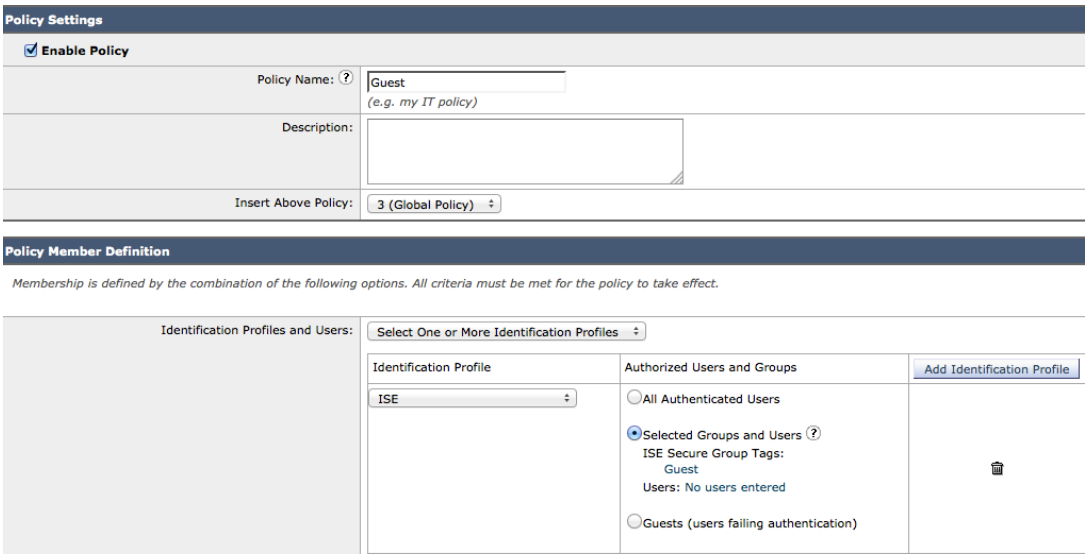
識別プロファイルと Web アクセス ポリシー

ステップ 1 [Web セキュリティ マネージャ(Web Security Manager)] > [Web ポリシー(Web Policies)] > [Web アクセス ポリシー(Web Access Policies)] を選択し、[セキュリティ グループ タグ:ユーザの入力なし(Secure Group Tags; No Users Entered)] をクリックしてゲスト識別プロファイルを作成し、[セキュリティ グループ タグ名(Security Group Tag Name)] で [ゲスト(Guest)] を選択します。





ステップ 2 [完了(Done)] をクリックします。
ステップ 3 次が表示されます。



ステップ 4 [送信(Submit)] をクリックし、[変更を確定(Commit Changes)] を 2 回クリックします。
ステップ 5 [URL フィルタリング(URL Filtering)] で [モニタリング(Monitoring)] をクリックします。
ステップ 6 ファイル転送サービスをブロックします。

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Use Global Settings	Override Global Settings: Block	Monitor	Warn	Quota-Based	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Education	✓				–	–
Entertainment	✓				–	–
Extreme	✓				–	–
Fashion	✓				–	–
File Transfer Services		✓			–	–
Filter Avoidance	✓				–	–

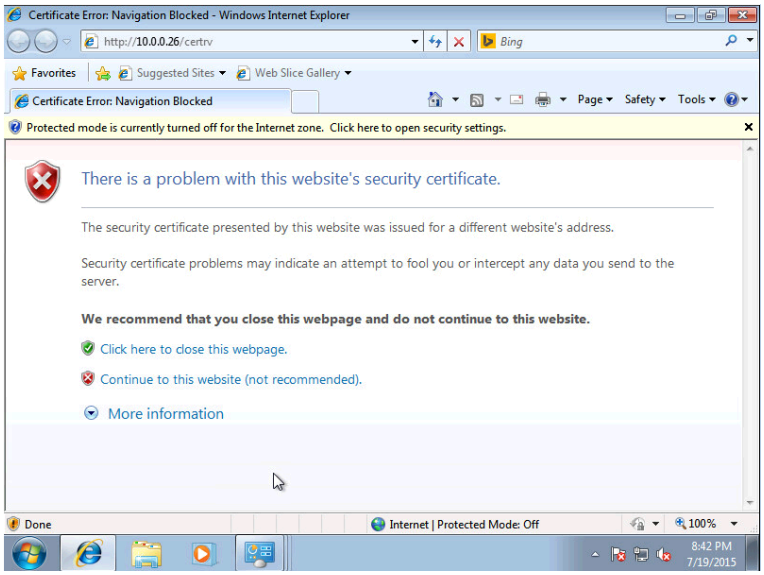
ステップ 7 Box の URL ポリシーを [モニタリング(Monitoring)] または [許可(Allow)] に設定します。
ステップ 8 [送信(Submit)] をクリックし、[変更を確定(Commit Changes)] を 2 回クリックします。

テスト

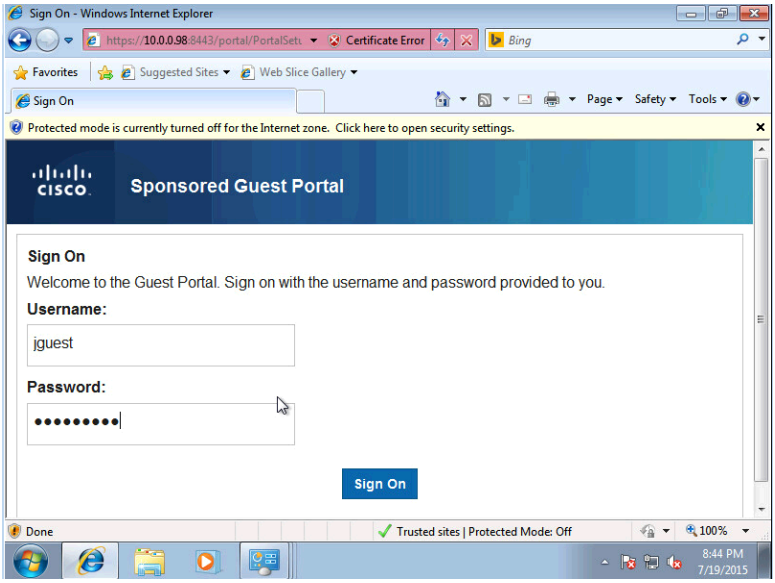
ゲスト ユーザがブラウザを開いて社内 Web サーバにアクセスすると、スポンサー ゲスト ポータルにリダイレクトされます。

注: 証明書エラーのメッセージには、ISE ノードのリダイレクトに FQDN が使用されていないことが示されます。その代わりに IP アドレスが使用されたことで、下記のメッセージが表示されます。また 10.0.0.26 は ISE リダイレクションに使用された社内 Web サーバです。http://1.1.1.1 を使用するほうが適切です。これは、「付録」のプロキシ設定に示されています。

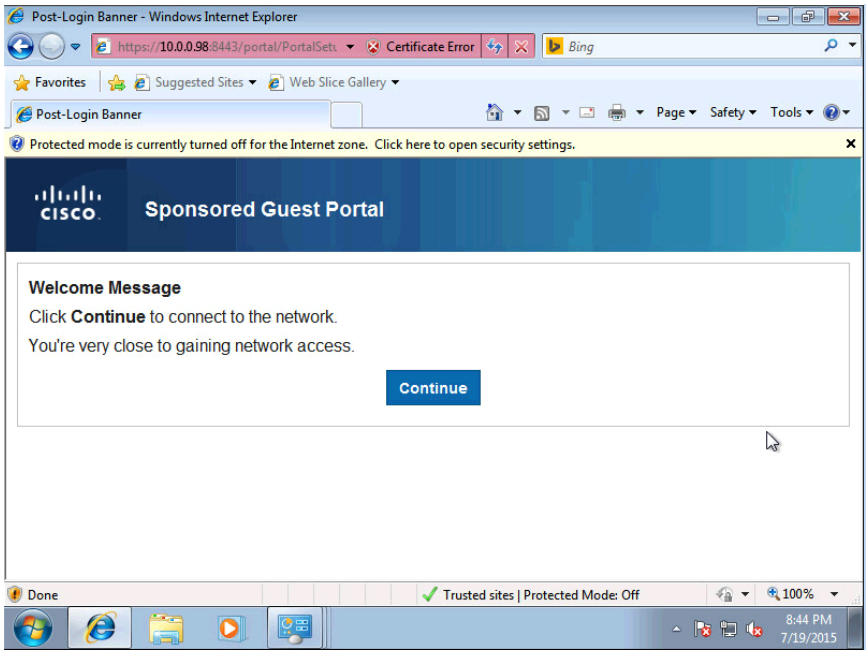
ステップ 1 ゲスト ユーザは、http://10.0.0.26/certsrv にアクセスすると ISE にリダイレクトされます。



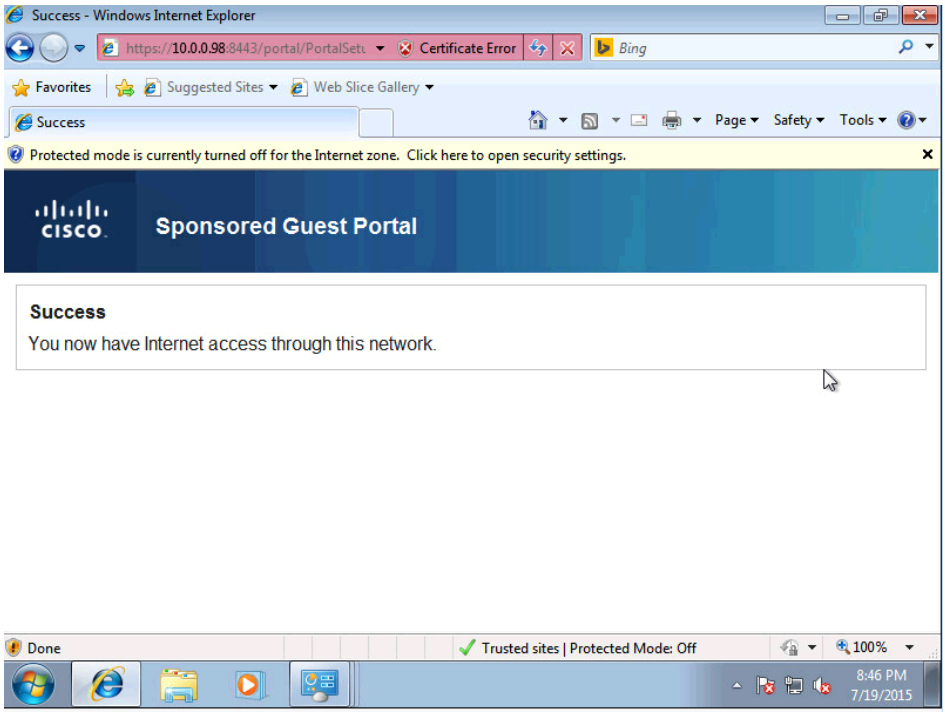
ステップ 2 ゲスト ユーザはクレデンシャルを入力してからサインオンします。



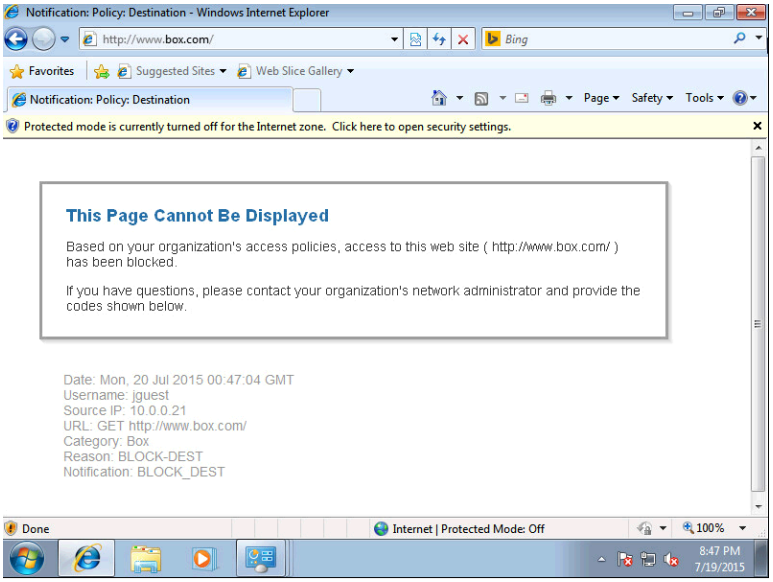
ステップ 3 [続行（Continue）] を選択します



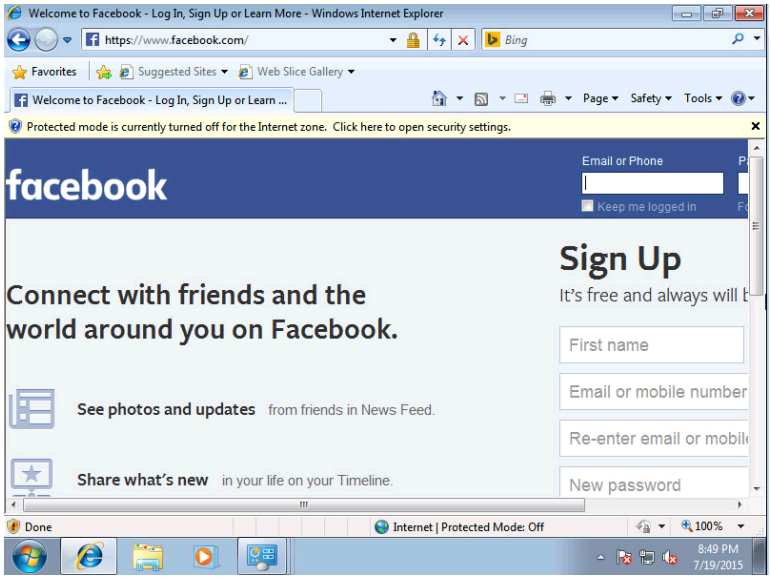
ステップ 4 Jguest に正常にログインしました。



ステップ 5 Box.com が拒否されました



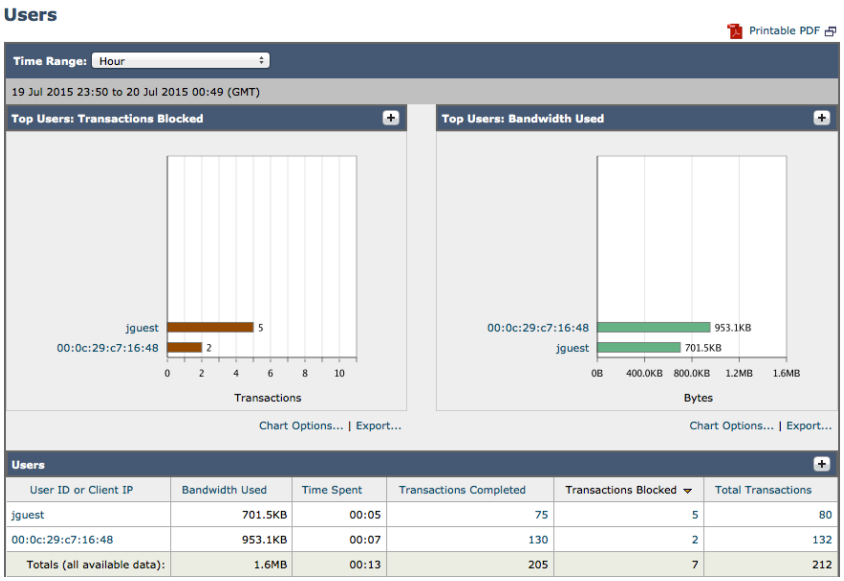
ステップ 6 Facebook が許可されました



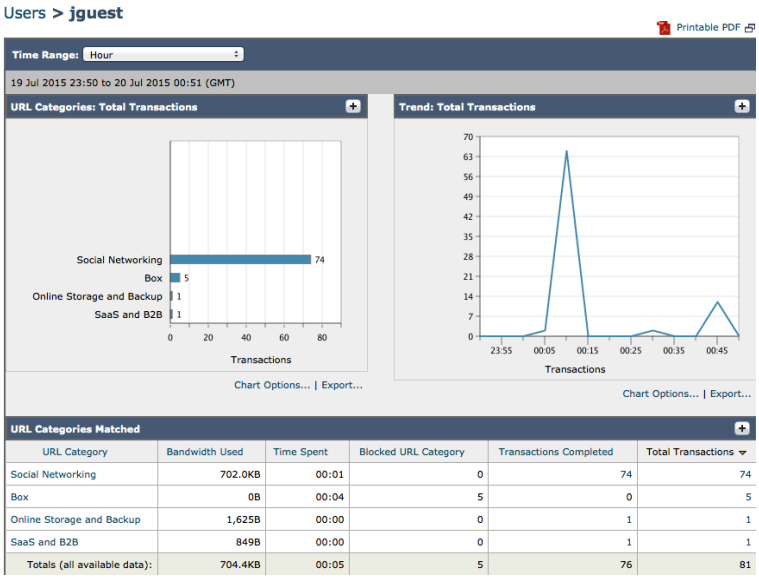
ステップ 7 ゲストの SGT-IP マッピングに注意します。

```
- CACHE - Show the ISE cache or check an IP address.
- SGTS - Show the ISE Secure Group Tag (SGT) table.
[]> CACHE


Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[]> SHOW


IP              Name                                                SGT#
10.0.0.15       LAB6\jeppich                                        4
10.0.0.98       00:0C:29:35:48:2A                                   0
169.254.57.162  00:0C:29:C7:16:48                                   0
10.0.0.22       00:0C:29:CA:A3:8F                                   0
10.0.0.33       68:05:CA:12:7C:78                                   0
10.0.0.21       jguest                                              5
10.0.0.3        18:E7:28:2E:29:CC                                   0

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[]>
```

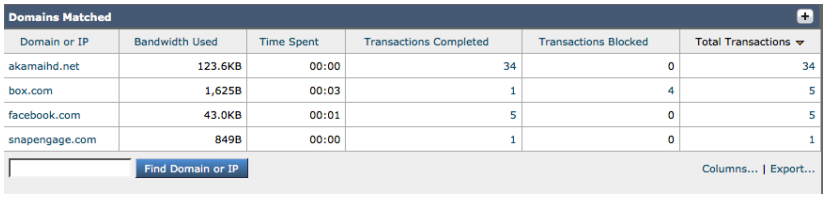
ステップ 8 jguest のユーザ レポートに注意します。このユーザには 2 つのブロックされたトランザクションがあります。



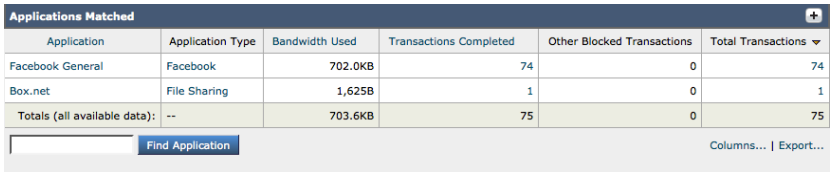
ステップ 9 jguest をクリックし、Box のブロックされたトランザクションを表示します。



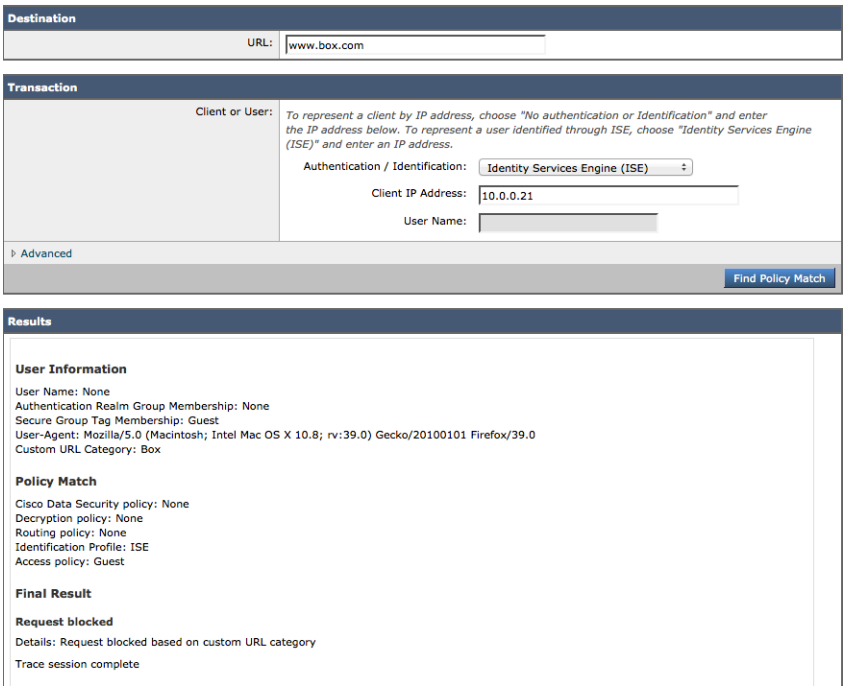
ステップ 10 jguest は、Box へのアクセスを拒否され、Facebook へのアクセスは許可されています。



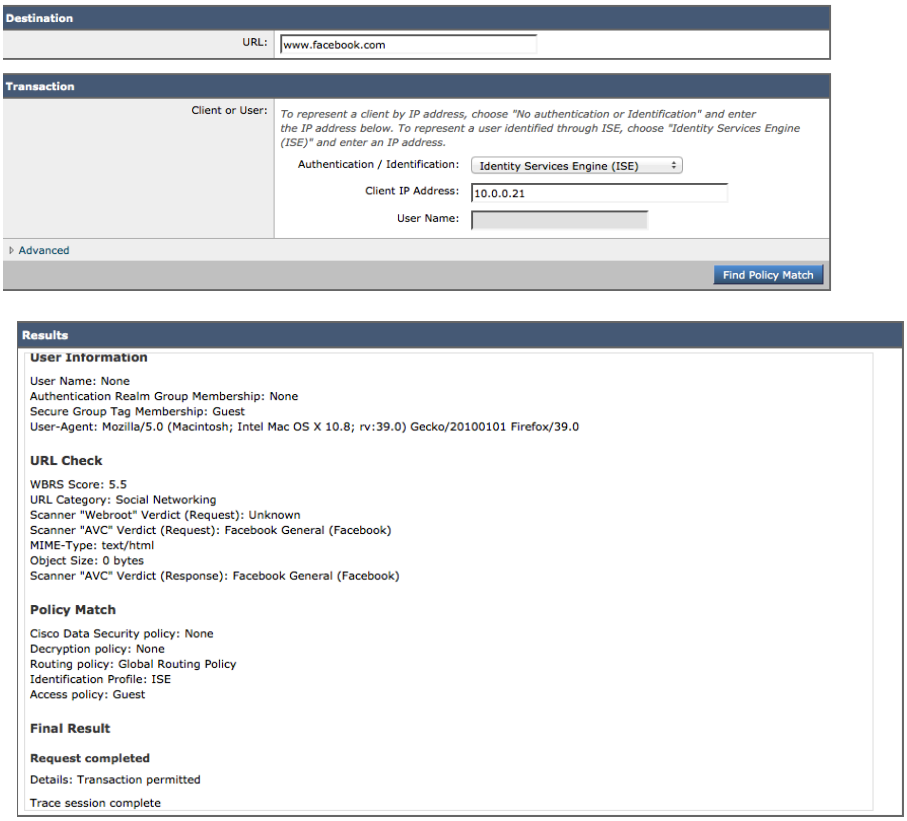
ステップ 11 アプリケーションを一致させることで可視性が向上します。



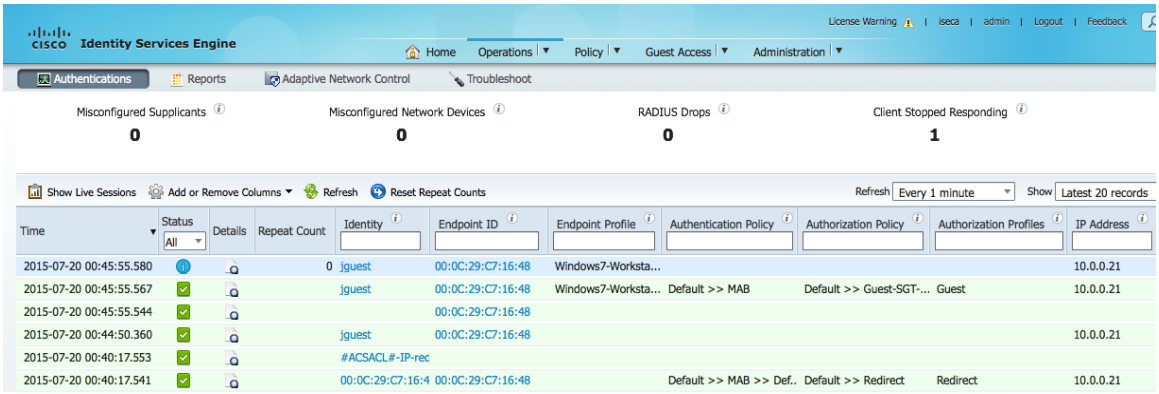
ステップ 12 [管理者（Administrator）] > [ポリシー トレース（Policy Trace）] を選択し、Box のポリシー トレースを確認します。



ステップ 13 Facebook のポリシー トレースも確認します。



ステップ 14 [操作（Operations）] > [認証（Authentication）] を選択し、ゲスト セキュリティ グループ タグが jguest に適用されていることに注意します。

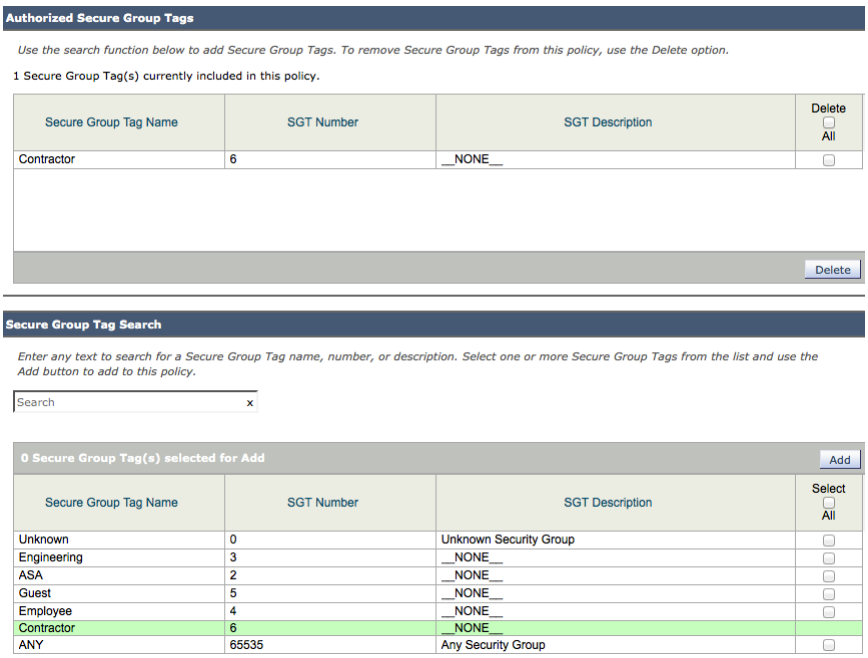


請負業者

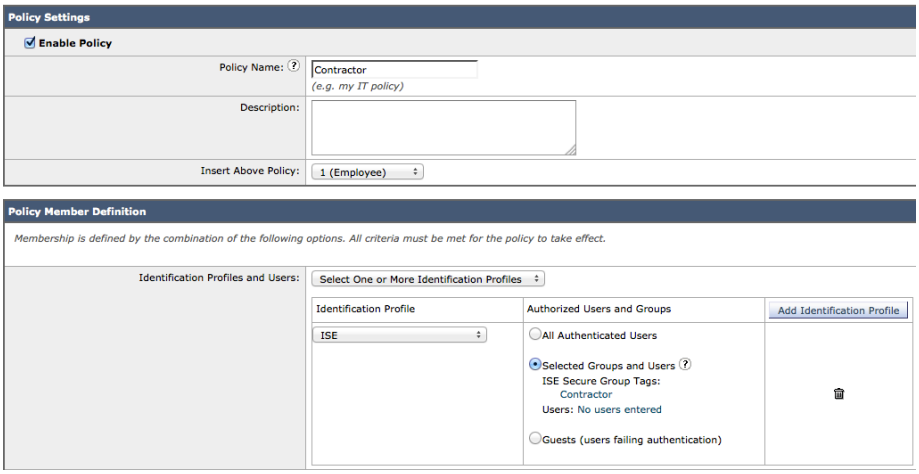
請負業者識別プロファイルと請負業者用の Web アクセス ポリシーが作成されます。この Web アクセス ポリシーでは、Box アクセスを拒否し、Facebook アクセスを許可します。

識別プロファイルと Web アクセス ポリシー

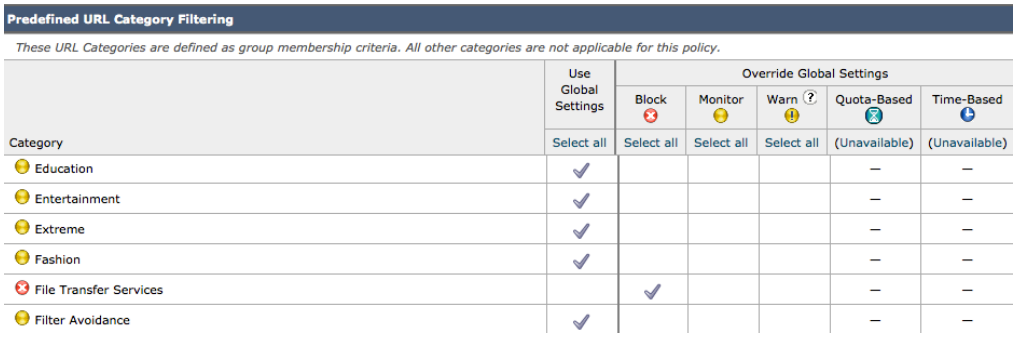
ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [Web ポリシー（Web Policies）] > [Web アクセス ポリシー（Web Access Policies）] を選択し、[セキュリティ グループ タグ：ユーザの入力なし（Secure Group Tags; No Users Entered）] をクリックしてゲスト識別プロファイルを作成し、[セキュリティ グループ タグ名（Security Group Tag Name）] で [ゲスト（Guest）] を選択します。



ステップ 2 [完了（Done）] をクリックします。
ステップ 3 次が表示されます。



ステップ 4 [送信（Submit）] をクリックし、[変更を確定（Commit Changes）] を 2 回クリックします。
ステップ 5 [URL フィルタリング（URL Filtering）] で [モニタリング（Monitoring）] をクリックします。
ステップ 6 ファイル転送サービスをブロックします。

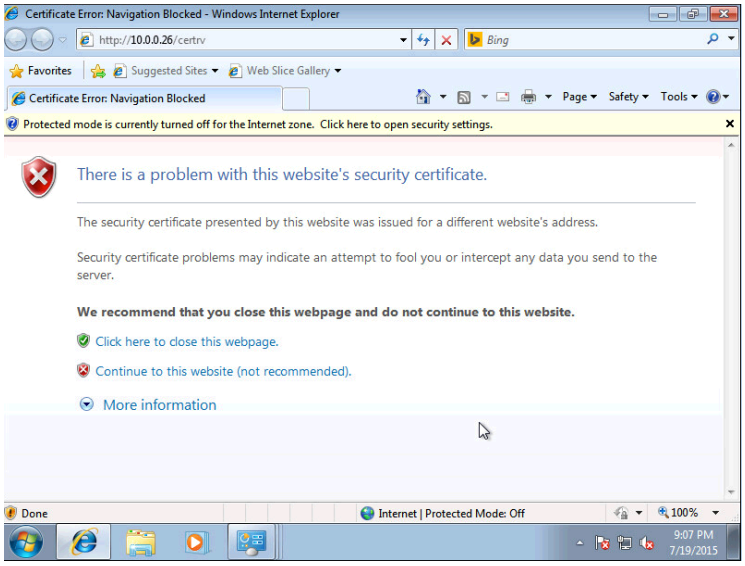


ステップ 7 [送信（Submit）] をクリックし、[変更を確定（Commit Changes）] を 2 回クリックします。

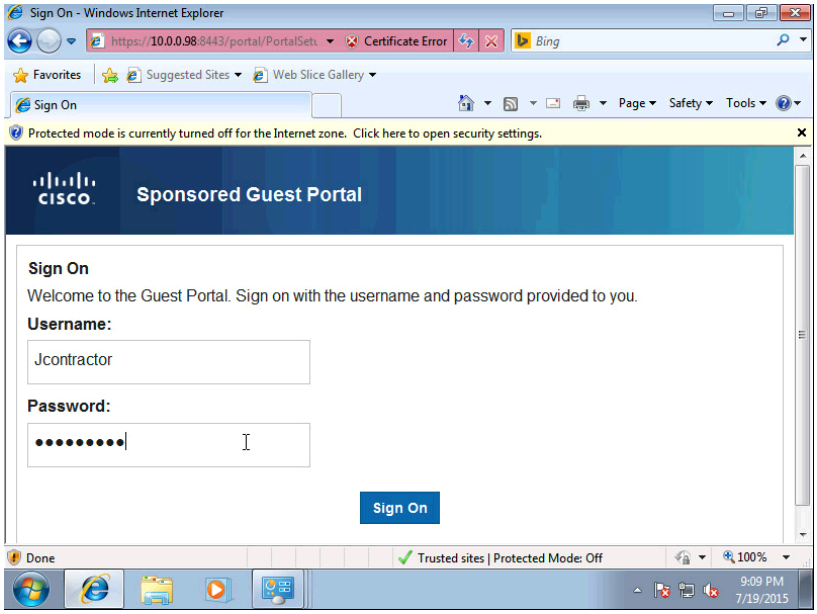
テスト

ステップ 1 請負業者がブラウザを開き、Web サイトにアクセスします。

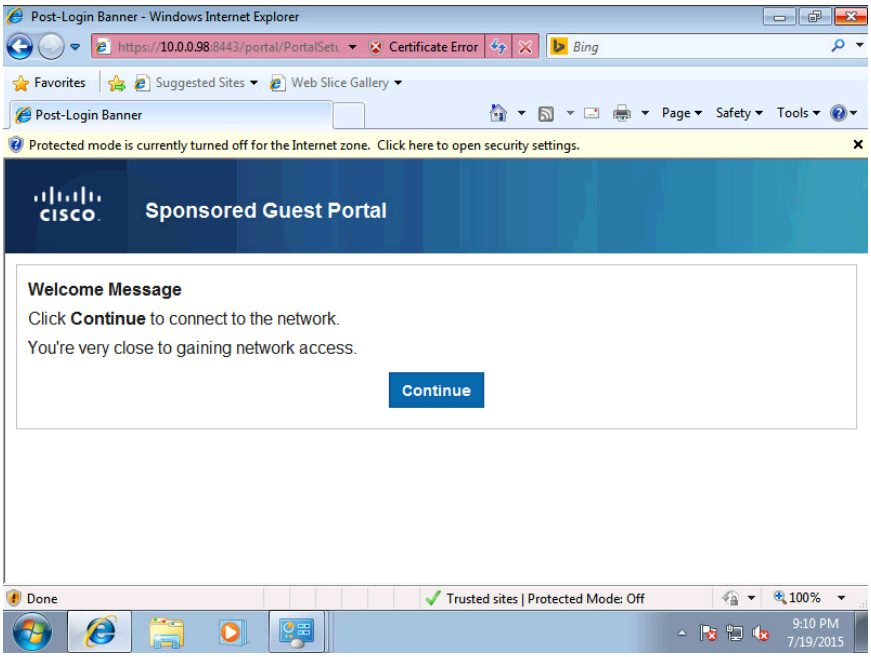
注：証明書のエラー メッセージは、URL がサーバの IP アドレスであったことが原因です。FQDN を使用していれば、このエラー メッセージは表示されません。



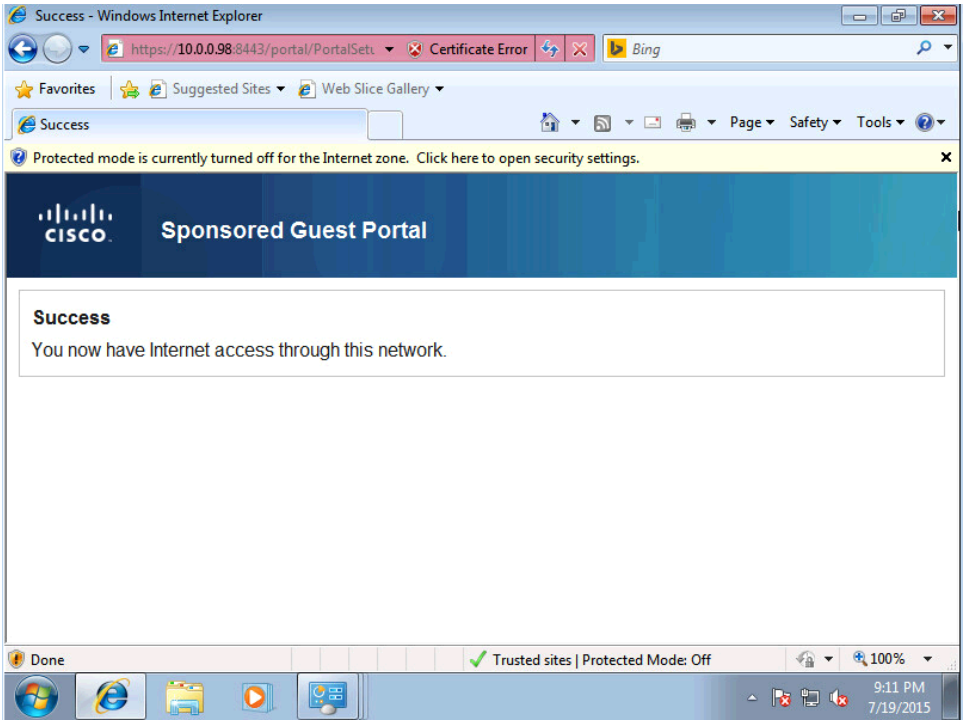
ステップ 2 請負業者が ISE の内部ユーザとして定義していたクレデンシャルを入力します。



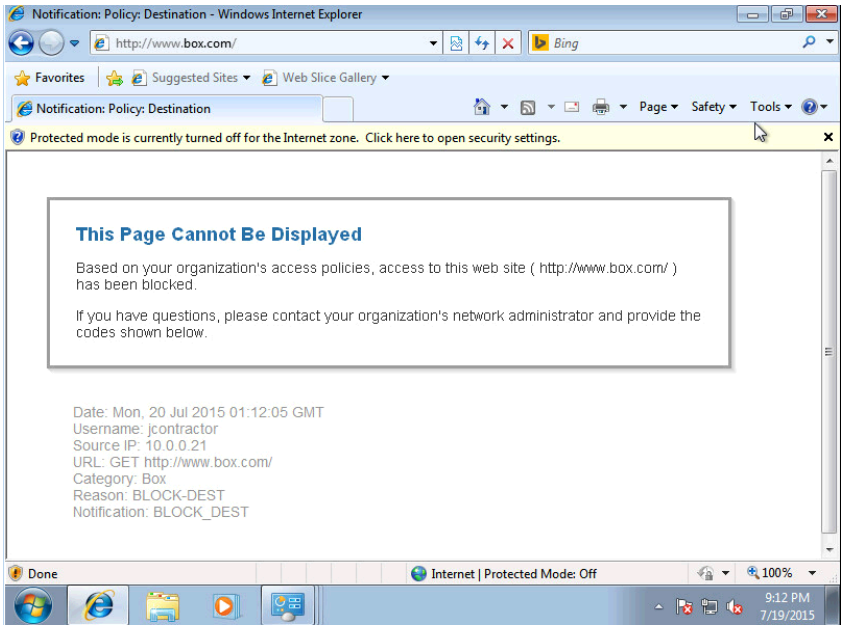
ステップ 3 請負業者が [続行(Continue)] を選択します。



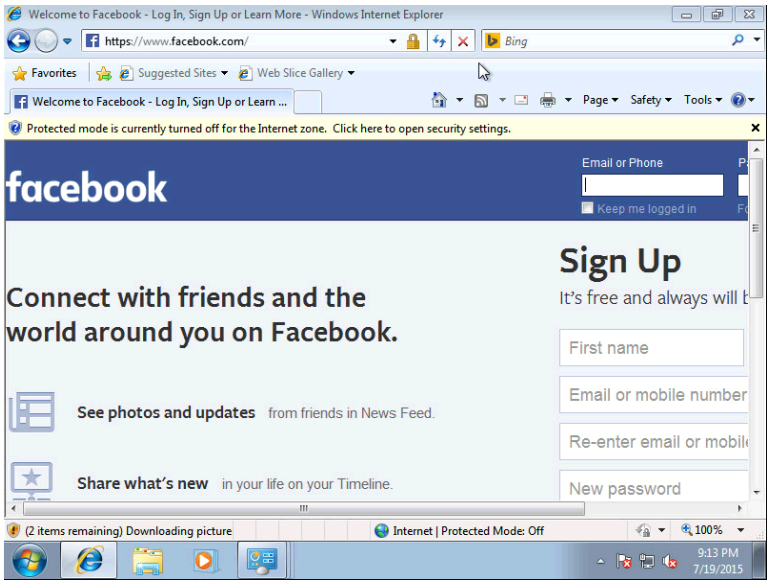
ステップ 4 請負業者がスポンサー ゲスト ポータルに正常にログインしました。



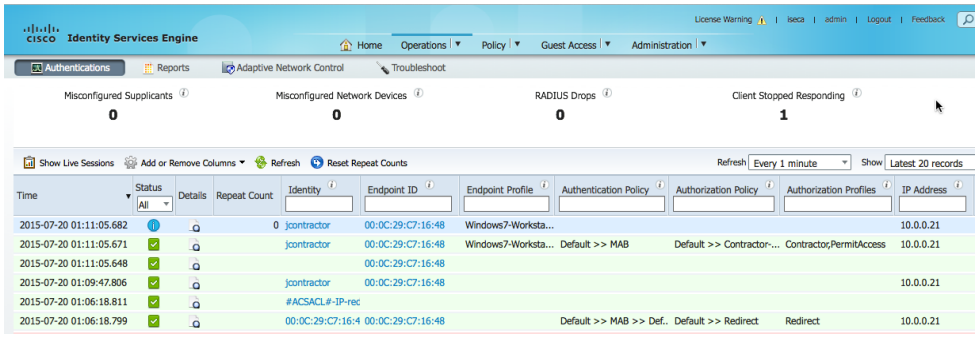
ステップ 5 請負業者が Box.com にアクセスし、拒否されます。



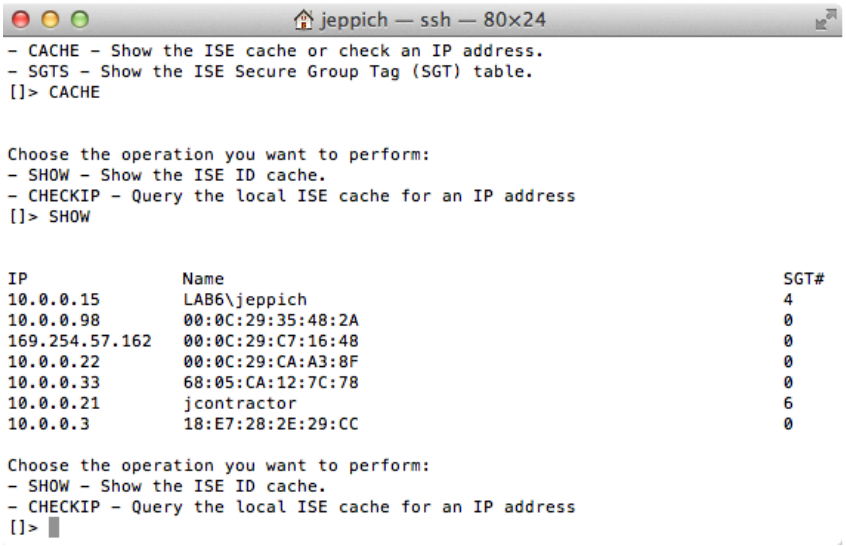
ステップ 6 請負業者が Facebook にアクセスします。



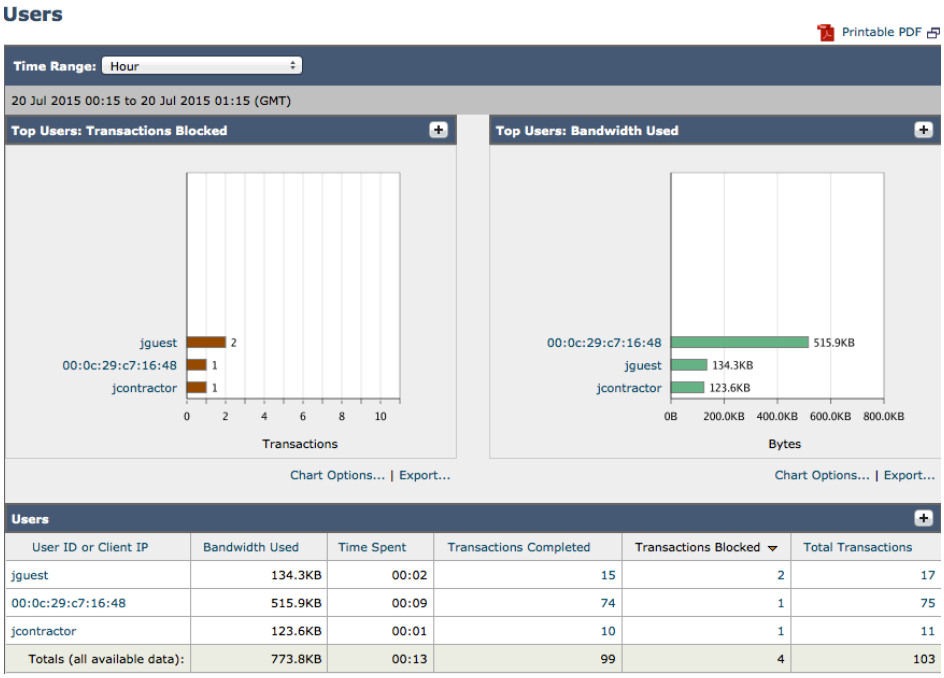
ステップ 7 [ISE 内の操作ビュー（Operations View in ISE）] を選択し、jcontractor に請負業者 SGT が割り当てられていることを表示します。



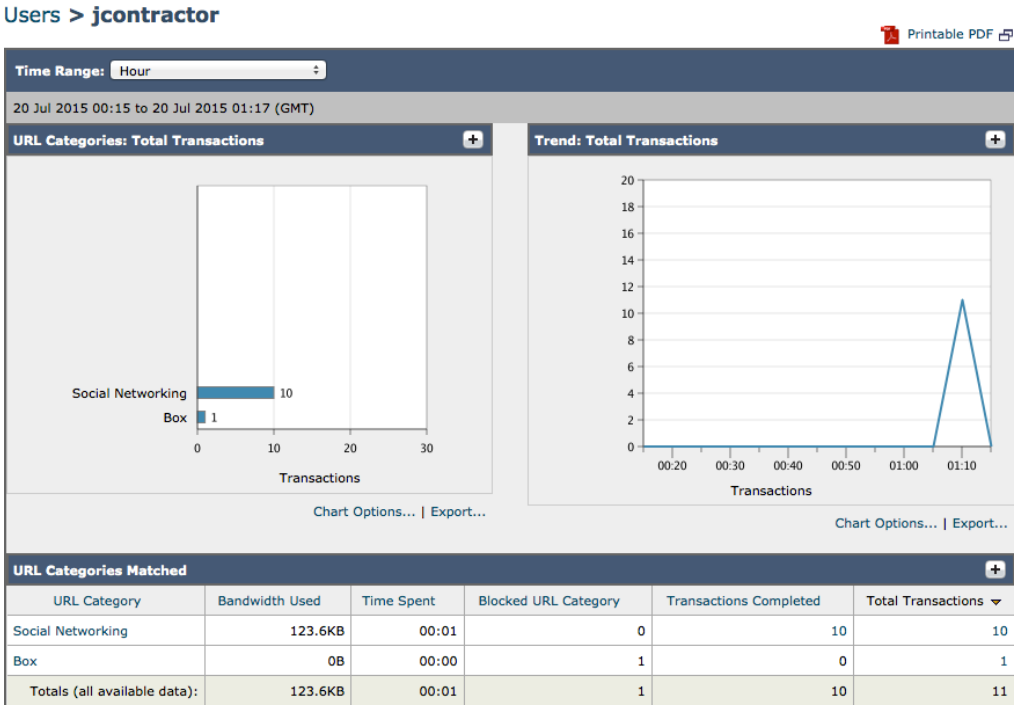
ステップ 8 jcontractor の IP-SGT マッピングを表示するには、WSA コンソールで「isedata」と入力します



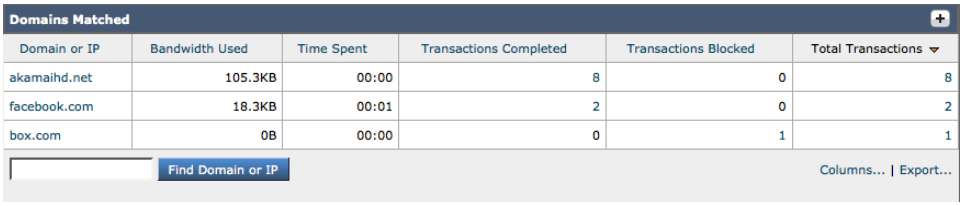
ステップ 9 WSA GUI で [レポート（Reports）] > [ユーザ（Users）] を選択し、ブロックされたトランザクションの概要を表示します。



ステップ 10 jcontractor を選択し、ブロックされたトランザクションを表示します。



ステップ 11 box.com がブロックされ、Facebook は許可されていたことに注意してください。

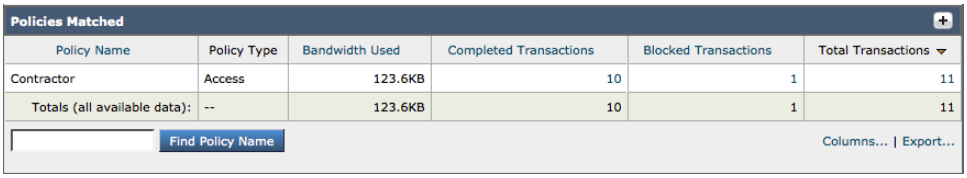


Domains Matched

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
akamaihd.net	105.3KB	00:00	8	0	8
facebook.com	18.3KB	00:01	2	0	2
box.com	0B	00:00	0	1	1

Find Domain or IP　Columns... | Export...

ステップ 12 次に、jcontractor の照合ポリシーを示します。

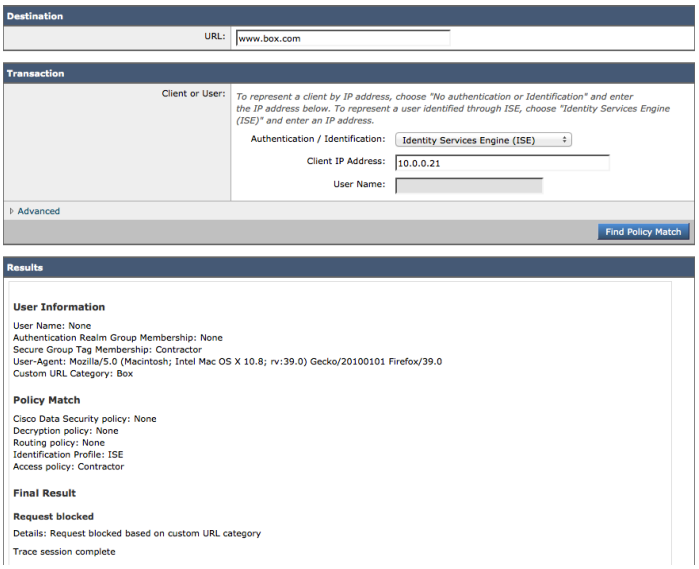


Policies Matched

Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions
Contractor	Access	123.6KB	10	1	11
Totals (all available data):	--	123.6KB	10	1	11

Find Policy Name　Columns... | Export...

ステップ 13 [管理者（Administrator）] > [ポリシー トレース（Policy Trace）] を選択し、Box の詳細情報の可視性を高めるように指定します。



Destination

URL: www.box.com

Transaction

Client or User: *To represent a client by IP address, choose "No authentication or Identification" and enter the IP address below. To represent a user identified through ISE, choose "Identity Services Engine (ISE)" and enter an IP address.*

Authentication / Identification: Identity Services Engine (ISE)

Client IP Address: 10.0.0.21

User Name:

Advanced

Find Policy Match

Results

User Information

User Name: None
Authentication Realm Group Membership: None
Secure Group Tag Membership: Contractor
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:39.0) Gecko/20100101 Firefox/39.0
Custom URL Category: Box

Policy Match

Cisco Data Security policy: None
Decryption policy: None
Routing policy: None
Identification Profile: ISE
Access policy: Contractor

Final Result

Request blocked

Details: Request blocked based on custom URL category

Trace session complete

ステップ 14 [管理者（Administrator）] > [ポリシー トレース（Policy Trace）] を選択し、Facebook の詳細情報の可視性を高めるように指定します。

Destination

URL: www.facebook.com

Transaction

Client or User: *To represent a client by IP address, choose "No authentication or Identification" and enter the IP address below. To represent a user identified through ISE, choose "Identity Services Engine (ISE)" and enter an IP address.*

Authentication / Identification: Identity Services Engine (ISE)

Client IP Address: 10.0.0.21

User Name:

Advanced

Find Policy Match

Results

User Information

User Name: None
Authentication Realm Group Membership: None
Secure Group Tag Membership: Contractor
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:39.0) Gecko/20100101 Firefox/39.0

URL Check

WBRS Score: 5.5
URL Category: Social Networking
Scanner "Webroot" Verdict (Request): Unknown
Scanner "AVC" Verdict (Request): Facebook General (Facebook)
MIME-Type: text/html
Object Size: 0 bytes
Scanner "AVC" Verdict (Response): Facebook General (Facebook)

Policy Match

Cisco Data Security policy: None
Decryption policy: None
Routing policy: Global Routing Policy
Identification Profile: ISE
Access policy: Contractor

Final Result

Request completed

Details: Transaction permitted

Trace session complete

トラブルシューティング

WSA と ISE pxGrid ノードの統合を設定する場合は、WSA では常に「tail ise_service_log」を使用してください。次が表示され、正常に接続されたことが確認できます。

```
Sat Jul 18 17:46:46 2015 Info: ISEBulkDownloader: Sessions:
   New:          4
   Updated:      0
   Dropped:      0   (out of date)
   Invalid:      2
```

RESTful ISE ノードの障害

- 解決策：「tail ise_service_log」を実行します。「ホスト名を解決できません（cannot resolve hostname）」エラーが表示された場合は、すべての ISE ノードと WSA で DNS が解決可能であることを確認します。
- 「ホスト名を解決できません（cannot resolve hostname）」エラーが引き続き表示され、WSA と ISE ノードで DNS が解決可能であれば、WSA pxGrid クライアント接続を削除し、WSA を再起動します。WSA 再起動後に、WSA が ISE pxGrid ノードの SessionDirectory と TrustsecMetadata 機能をサブスクライブしていたことが表示されることを確認します。「tail ise_service_log」を実行し、SGT タグのダウンロードが表示されることを確認します。引き続きエラーが表示される場合は、ISE pxGrid ノードを再起動する必要がある場合があります。
- CA 署名環境の場合は、WSA に ISE モニタリング ノードの管理者証明書として CA ルート証明書がインストールされていることを確認します。
- 自己署名証明書を実行している場合で、ISE スタンドアロン環境の場合は、WSA に ISE モニタリング ノードの管理者証明書として ISE 自己署名証明書がインストールされていることを確認します。
- WSA は初期ブート時に ISE RESTful API を使用して一括セッション レコードを ISE MnT ノードからダウンロードします。WSAは、ISE 管理者ノード証明書を使用して、利用可能な ISE MnT ノードに問い合わせます。

ISE pxGrid クライアントの接続の問題

- ISE スタンドアロン環境では、デフォルトで pxGrid ノードの自動登録は無効になっています。ISE 管理者が保留中の pxGrid クライアント要求を承認していることを確認すれば、これで問題ありません。自動登録を有効にするように変更し、要求の保留を回避するようにできます。

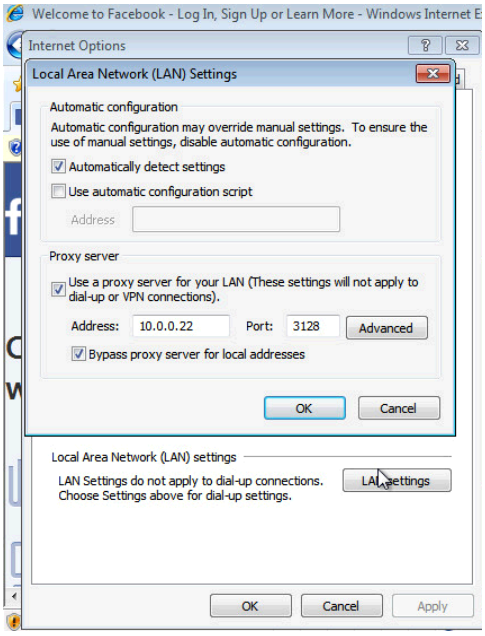
WSA 仮想 での CPU RAM 使用率が 100%

解決策：「tail ise_service_logs」を実行します。複数の WSA の再起動が発生した場合は、CPU は 2 倍に、RAM サイズは 8 GB に増加します。

付録

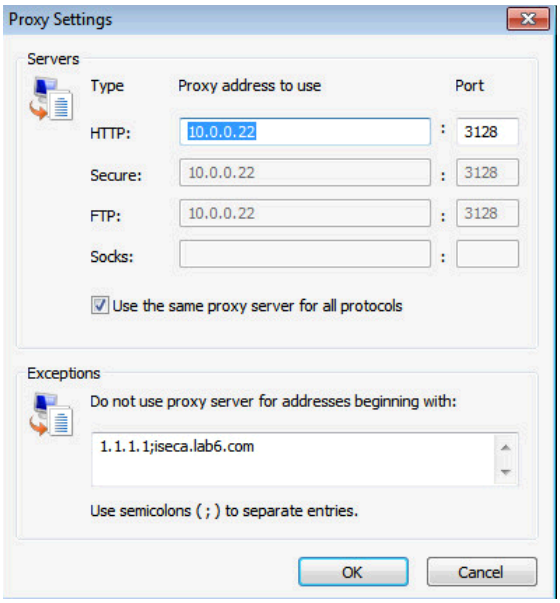
Internet Explorer のプロキシ設定

アドレスおよびポートは、WSA とポート番号を表します



次に、WSA プロキシ設定をバイパスし、CWA アクセス用の ISE ノードにリダイレクトできる例外を示します。1.1.1.1 は ISE ノード（iseca.lab.com）へのリダイレクトをトリガーする IP アドレスです。

注：これは、分散 ISE 展開での ISE PSN ノードの IP アドレスです



CWA の ACL設定の切り替えとリダイレクト

これにより、顧客の展開が保留されます。次に基本情報をハイライトします。このドキュメントでは、Catalyst 3850 スイッチを使用しています。

リダイレクト ACL

```
ip access-list extended REDIRECT
 deny   udp any any eq domain
 permit tcp any any eq www
 deny   ip any host 10.0.0.98      (Cisco ISE PSN node for a centralized ISE deployment or the ISE Node for a
                                    an ISE stand-alone deployment)
```

CWA スイッチの設定

追加設定については、http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_sw_cnfg.html を参照してください。

```
aaa server radius dynamic-author
 client 10.0.0.98 server-key {password}   (Cisco ISE PSN node for a centralized ISE deployment or the ISE Node
                                           for an ISE stand-alone deployment)
.
.
ip http server                             (Required for switch to redirect based on http traffic)
ip http secure-server                       (Required for switch to redirect on https traffic)
```

参考資料

分散 ISE 環境での pxGrid の設定方法:
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf

pxGrid での証明書の展開:自己署名証明書と、ISE pxGrid ノードおよび pxGrid クライアントを使用:
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-Self_signed_pxGridClient_selfsigned_pxGrid.pdf

px Grid での証明書の展開:CA 署名の ISE pxGrid ノードと CA 署名の pxGrid クライアントを使用:
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-Self_signed_pxGridClient_selfsigned_pxGrid.pdf