

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	4
ソリューションの概要: TrustSec、ISE、および pxGrid を搭載した WSA	6
Cisco Web Security Appliance (WSA)	6
Cisco TrustSec	7
Cisco Identity Services Engine (ISE)	7
Cisco pxGrid	7
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	10
Cisco WSA のインストール	12
WSA システム ウィザード	12
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	17
WSA 証明書信頼ストアへの CA ルート証明書の追加	18
WSA 信頼ストアへの CA ルート証明書の追加	18
CA 署名付き WSA クライアント証明書の設定	18
WSA 秘密キーおよび CSR 要求の作成	18
WSA からの WSA 秘密キーおよび CSR 要求の作成(代替策)	20
WSA での ISE サービスの設定	22
プライマリ pxGrid ノード証明書のアップロード	23
セカンダリ pxGrid ノードの証明書のアップロード	24
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	24
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	24
WSA の証明書と秘密キーのアップロード	25
テストの実行	25
登録済み pxGrid クライアントとしての WSA の確認	27
WSA ポリシー	28
WSA での識別プロファイルの作成	28
WSA アクセス ポリシーの作成	29
WSA の復号化アプリケーション ポリシーの作成	32
アプリケーションの復号化	34
ルート公開キー/秘密キー ペアの取得	36
クライアントのテスト	38

ユーザレポート.....	40
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.....	44
WSA の自己署名証明書の作成.....	44
ISE 自己署名識別証明書および ISE pxGrid の設定.....	45
WSA と ISE pxGrid ノードの設定.....	47
クライアントのテスト.....	52
使用例のシナリオ.....	54
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.....	54
ISE 動的タグ、認可プロファイル、および認可ポリシー.....	56
動的タグ.....	56
許可プロファイルと CWA 用のダウンロード可能な ACL.....	57
許可ポリシー.....	58
従業員.....	59
識別プロファイルと Web アクセス ポリシー.....	59
テスト.....	62
ゲスト.....	68
識別プロファイルと Web アクセス ポリシー.....	68
テスト.....	70
請負業者.....	76
識別プロファイルと Web アクセス ポリシー.....	76
テスト.....	77
トラブルシューティング.....	85
RESTful ISE ノードの障害.....	85
ISE pxGrid クライアントの接続の問題.....	85
WSA 仮想 での CPU RAM 使用率が 100%.....	85
付録.....	86
Internet Explorer のプロキシ設定.....	86
CWA の ACL 設定の切り替えとリダイレクト.....	87
リダイレクト ACL.....	87
CWA スイッチの設定.....	87
参考資料.....	88

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、認証レール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 の認証レール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ることで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トチャンプライアンス 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、ポストチャ、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/適用することによ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、ポストチャステータス、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。

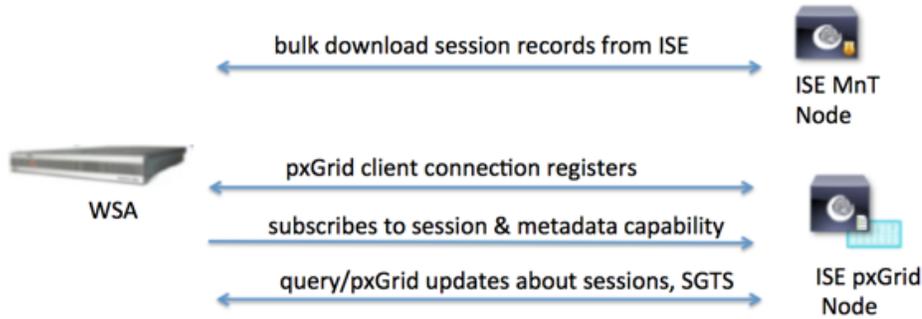
```
session (ip=192.168.1.14, Audit Session Id=0A0301030000001E00FEBAD7, User Name=jsmith, Domain=lab4.com, Calling station id=00:0C:29:77:A8:C7, Session state= STARTED, Epsstatus=null, Security Group=Engineering, Endpoint Profile=Microsoft-Workstation, NAS IP=192.168.1.2, NAS Port=GigabitEthernet1/0/9, 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=jepich,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。

Clients | Live Log

License Warning | ise14ppan | admin | Logout | Feedback

System | Identity Management | Network Resources | Device Portal Management | **pxGrid Services** | Feed Service | pxGrid Identity Mapping

Enable Auto-Registration | Disable Auto-Registration | View By Capability

Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-ise14smnt		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
ise-mnt-ise14smnt		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-admin-ise14pmnt		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
ise-mnt-ise14pmnt		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-admin-ise14ppan		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ironport.example.com-pxgrid_client	pxGrid Connection from WSA	Capabilities(0 Pub, 2 Sub)	Online	Session	View

Capability Detail | 1 - 2 of 2 | Show 25 per page | Page 1 of 1

Capability Name	Capability Version	Messaging Role	Message Filter
<input type="radio"/> SessionDirectory	1.0	Sub	
<input type="radio"/> TrustSecMetaData	1.0	Sub	

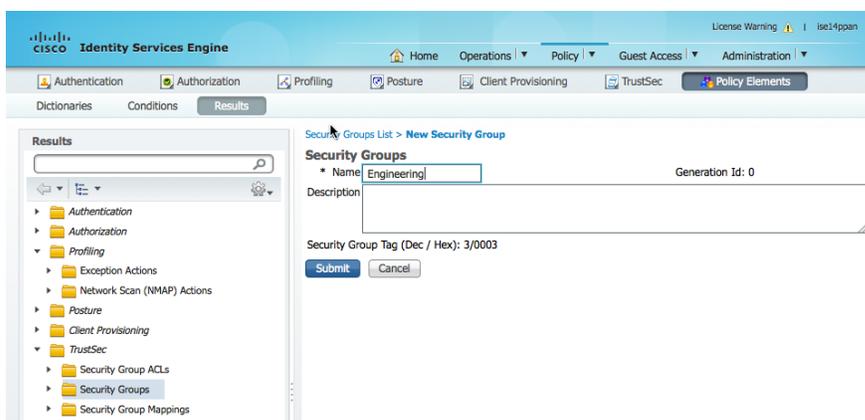
wsa.lab6.com-test_client | pxGrid Connection from WSA | Capabilities(0 Pub, 0 Sub) | Offline | Session | [View](#)

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ーと、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)]



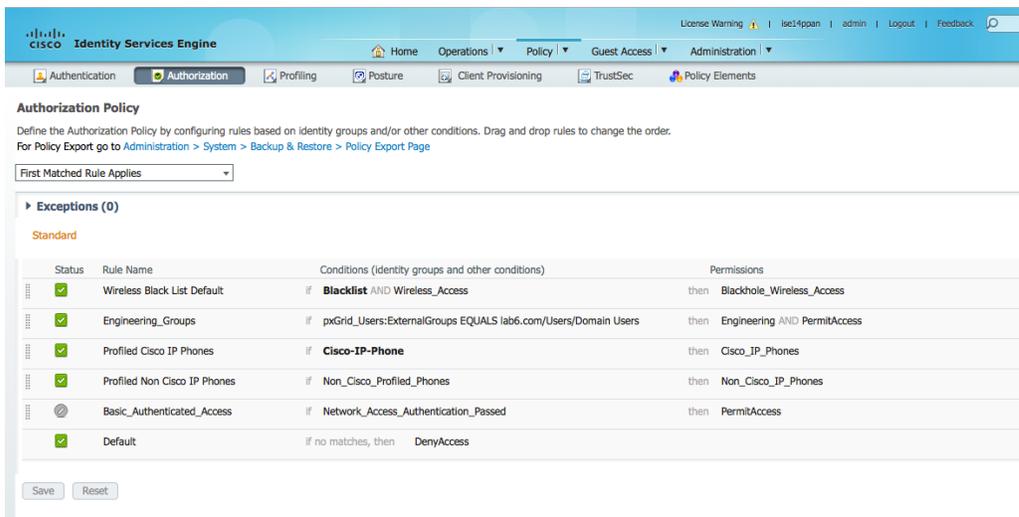
ステップ 2 許可ポリシーを作成し、SGT 許可プロファイルをポリシーに割り当てます。

[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



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Engineering_Groups	if pxGrid_Users:ExternalGroups EQUALS lab6.com/Users/Domain Users	then Engineering AND PermitAccess
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
<input type="checkbox"/>	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then PermitAccess
<input checked="" type="checkbox"/>	Default	if no matches, then DenyAccess	

Save Reset

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。

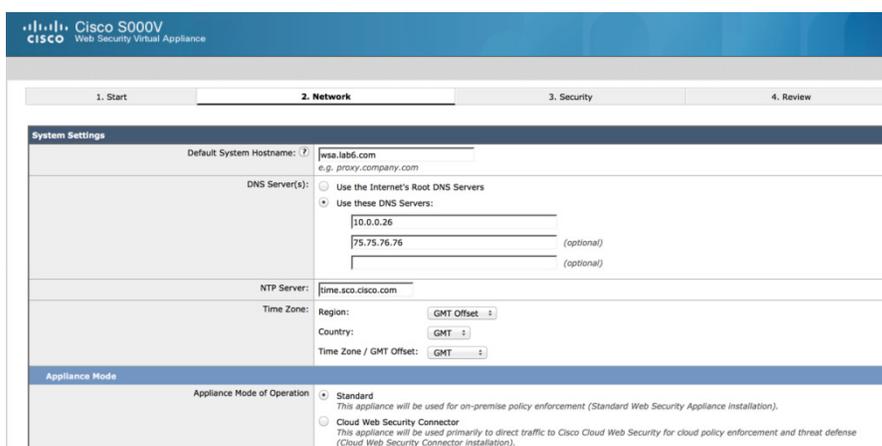
WSA システム ウィザード

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。

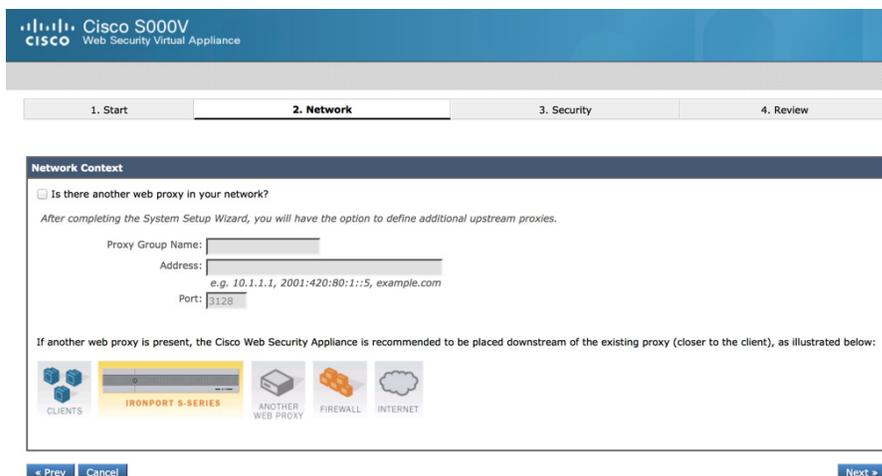


The screenshot shows the 'System Settings' section of the Cisco S000V Web Security Virtual Appliance installation wizard. The '2. Network' step is active. The 'System Settings' section includes:

- Default System Hostname:
- DNS Server(s):
 - Use the Internet's Root DNS Servers
 - Use these DNS Servers:
 - (optional)
 - (optional)
- NTP Server:
- Time Zone:
 - Region:
 - Country:
 - Time Zone / GMT Offset:
- Appliance Mode of Operation:
 - Standard (This appliance will be used for on-premise policy enforcement (Standard Web Security Appliance installation).)
 - Cloud Web Security Connector (This appliance will be used primarily to direct traffic to Cisco Cloud Web Security for cloud policy enforcement and threat defense (Cloud Web Security Connector installation).)

ステップ 3 [次へ (Next)] を選択します。

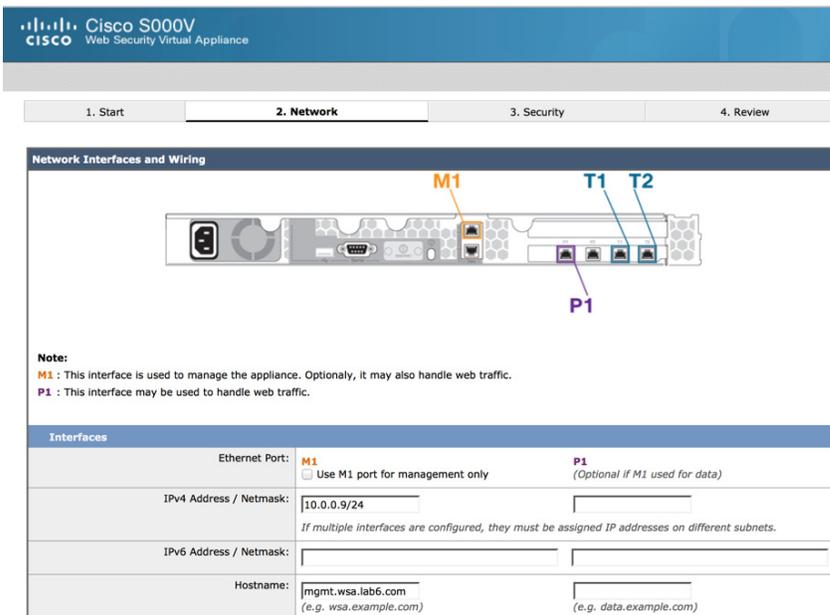
ステップ 4 ネットワーク内に他の Web プロキシがない場合は、[次へ (Next)] を選択します。



The screenshot shows the 'Network Context' section of the Cisco S000V Web Security Virtual Appliance installation wizard. The '2. Network' step is active. The 'Network Context' section includes:

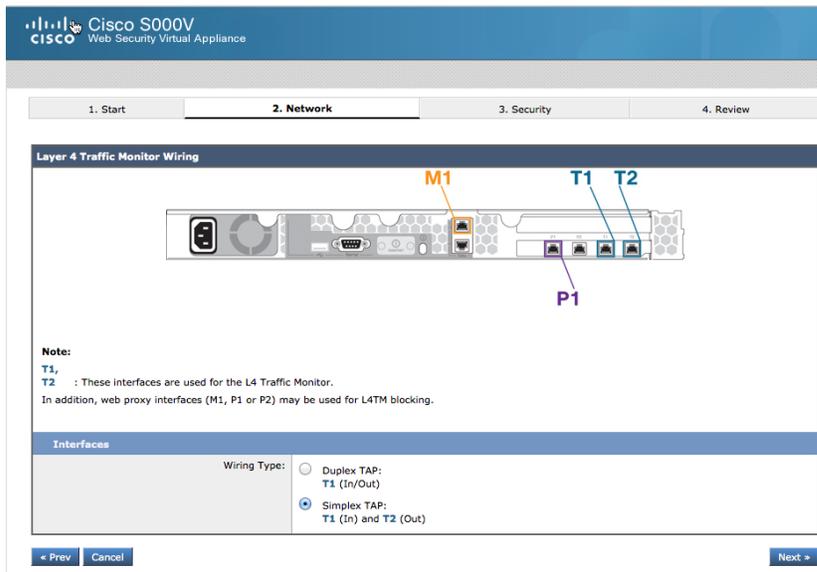
- Is there another web proxy in your network?
After completing the System Setup Wizard, you will have the option to define additional upstream proxies.
- Proxy Group Name:
- Address:
- Port:
- If another web proxy is present, the Cisco Web Security Appliance is recommended to be placed downstream of the existing proxy (closer to the client), as illustrated below:
- Diagram illustrating network topology: CLIENTS -> IRONPORT S-SERIES -> ANOTHER WEB PROXY -> FIREWALL -> INTERNET

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。

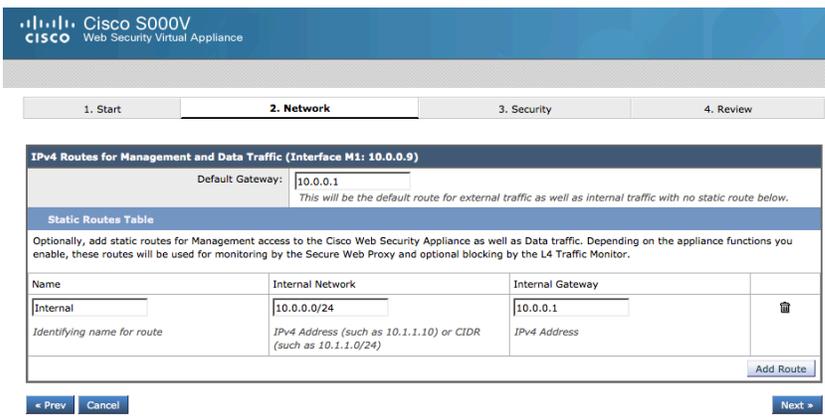


ステップ 6 [次へ (Next)] をクリックします。

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。

Cisco S000V
Web Security Virtual Appliance

1. Start **2. Network** 3. Security 4. Review

IPv4 Routes for Management and Data Traffic (Interface M1: 10.0.0.9)

Default Gateway:
This will be the default route for external traffic as well as internal traffic with no static route below.

Static Routes Table

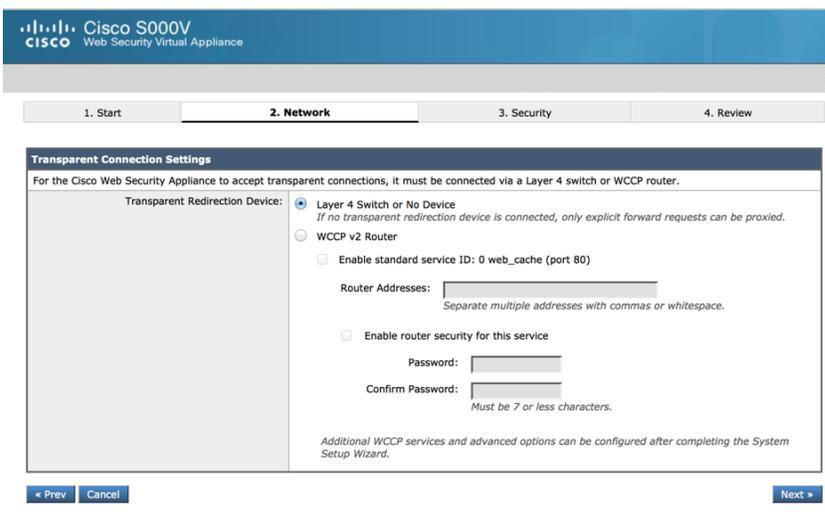
Optionally, add static routes for Management access to the Cisco Web Security Appliance as well as Data traffic. Depending on the appliance functions you enable, these routes will be used for monitoring by the Secure Web Proxy and optional blocking by the L4 Traffic Monitor.

Name	Internal Network	Internal Gateway	
<input type="text" value="Internal"/>	<input type="text" value="10.0.0.0/24"/>	<input type="text" value="10.0.0.1"/>	

Identifying name for route *IPv4 Address (such as 10.1.1.10) or CIDR (such as 10.1.1.0/24)* *IPv4 Address*

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。



Cisco S000V
Web Security Virtual Appliance

1. Start **2. Network** 3. Security 4. Review

Transparent Connection Settings

For the Cisco Web Security Appliance to accept transparent connections, it must be connected via a Layer 4 switch or WCCP router.

Transparent Redirection Device:

- Layer 4 Switch or No Device
If no transparent redirection device is connected, only explicit forward requests can be proxied.
- WCCP v2 Router
 - Enable standard service ID: 0 web_cache (port 80)
Router Addresses:
Separate multiple addresses with commas or whitespace.
 - Enable router security for this service
Password:
Confirm Password:
Must be 7 or less characters.

Additional WCCP services and advanced options can be configured after completing the System Setup Wizard.

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。

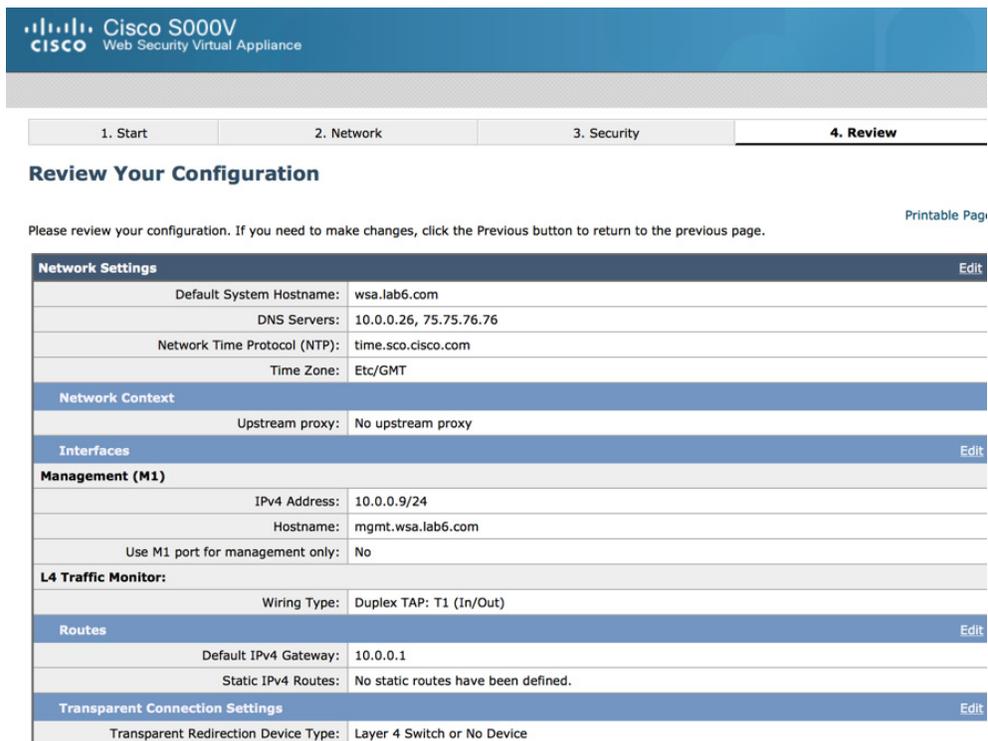
The screenshot shows the 'Administrative Settings' section of the Cisco S000V configuration interface. The progress bar at the top indicates that '2. Network' is the current step. The form includes fields for 'Administrator Password' (with a confirmation field), 'Email system alerts to' (with an example email address), 'Send Email via SMTP Relay Host (optional)' (with a host and port field), and 'AutoSupport' (checked). Below this is the 'SensorBase Network Participation' section, where 'Network Participation' is checked, and the 'Standard - Full URL information' option is selected.

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。

The screenshot shows the 'Security Settings' section of the Cisco S000V configuration interface. The progress bar at the top indicates that '3. Security' is the current step. The form includes several sections: 'Global Policy Default Action' (radio buttons for 'Monitor all traffic' and 'Block all traffic'), 'L4 Traffic Monitor' (radio buttons for 'Monitor only' and 'Block'), 'Acceptable Use Controls' (checked), 'Reputation Filtering' (checked), 'Malware and Spyware Scanning' (checked for Webroot, McAfee, and Sophos), and 'Cisco Data Security Filtering' (checked).

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。



The screenshot shows the configuration review page for a Cisco S000V Web Security Virtual Appliance. The page is titled "Review Your Configuration" and includes a progress bar with four steps: 1. Start, 2. Network, 3. Security, and 4. Review (highlighted). Below the progress bar, there is a "Printable Page" link and a message: "Please review your configuration. If you need to make changes, click the Previous button to return to the previous page." The configuration is organized into several sections, each with an "Edit" link:

- Network Settings**:
 - Default System Hostname: wsa.lab6.com
 - DNS Servers: 10.0.0.26, 75.75.76.76
 - Network Time Protocol (NTP): time.sco.cisco.com
 - Time Zone: Etc/GMT
- Network Context**:
 - Upstream proxy: No upstream proxy
- Interfaces**:
 - Management (M1)**:
 - IPv4 Address: 10.0.0.9/24
 - Hostname: mgmt.wsa.lab6.com
 - Use M1 port for management only: No
 - L4 Traffic Monitor**:
 - Wiring Type: Duplex TAP: T1 (In/Out)
- Routes**:
 - Default IPv4 Gateway: 10.0.0.1
 - Static IPv4 Routes: No static routes have been defined.
- Transparent Connection Settings**:
 - Transparent Redirection Device Type: Layer 4 Switch or No Device

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。

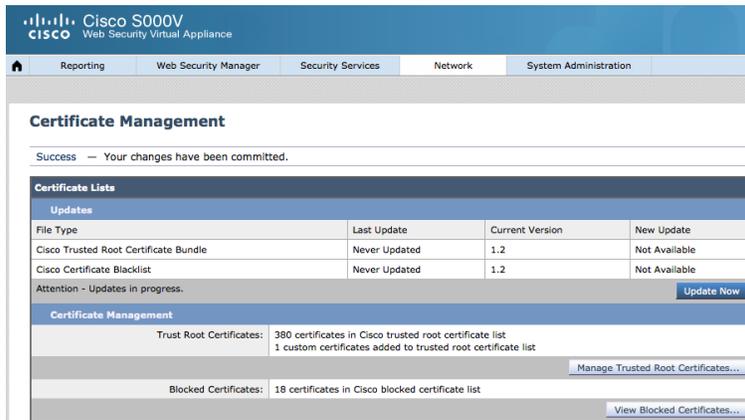
CA ルート証明書が pxGrid プライマリ ノードと pxGrid セカンダリ ノードから WSA にアップロードされます。pxGrid のノードは、管理者ノードを問い合わせ、動作可能なノードを確認します。デフォルトでは、プライマリ pxGrid ノードがアクティブで、セカンダリ pxGrid ノードが非アクティブになります。完全な PPAN 障害が発生し、SPAN がアクティブになった場合、プライマリ pxGrid ノードは SPAN をアクティブな PPAN と見なします。

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 wsal.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 wsal.key -out wsal.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。

Microsoft Active Directory Certificate Services – lab6-WIN-49T17723U08-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
M5LlJofmDFsDk8ZogFzRHRet0At3xuy5GYIPVT0TkK7
rDAAcYpOGa1+7bgXNoRjueA32XP3pOb5ap6Hrt54I
2O7dbnNGd9bbiEkzbOKM7y9AvHj8BEHr8fcfx+Mbv
AZ/X/wpsmnlO1E9IC88FrjcejHAvh5TGAw5FMKAhyl
8/x29MNHAguykoXHSqIPMIEOC7IH9K3GmRI85HOF!
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

pxGrid

Additional Attributes:

Attributes:

Submit >

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。

Microsoft Active Directory Certificate Services – lab6-WIN-49T17723U08-CA

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

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。

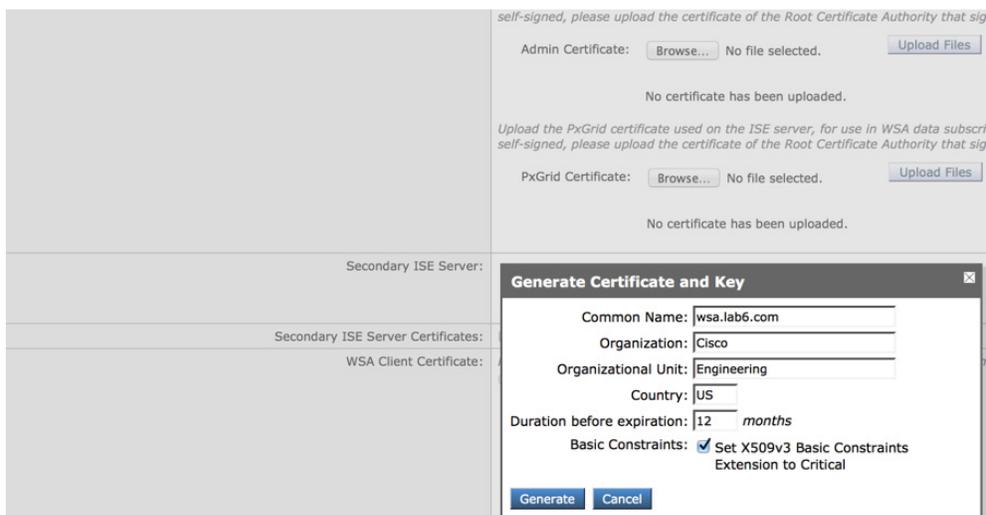
WSA からの WSA 秘密キーおよび CSR 要求の作成(代替策)

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。

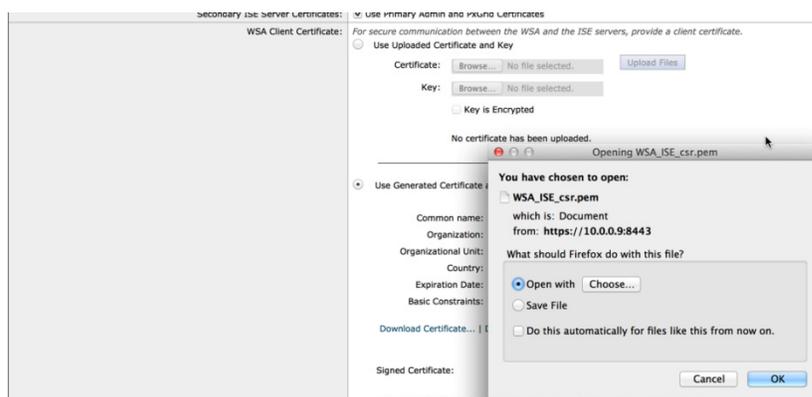


ステップ 2 次の手順で、CSR 要求が生成されます。情報を入力してください。

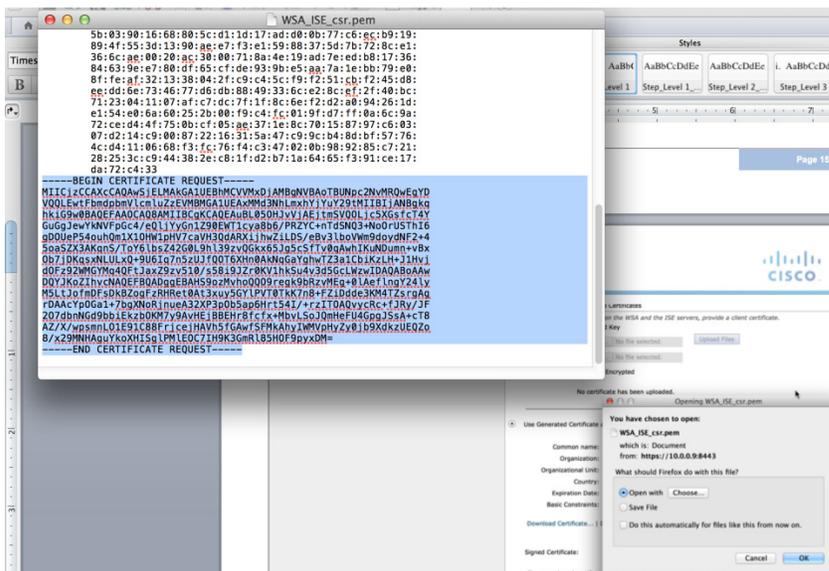


ステップ 3 [生成(Generate)] を選択し、証明書とキーが正常に生成されていることを確認します。

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。

Microsoft Active Directory Certificate Services – lab6-WIN-49T17723U08-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
M5LJofmDFsDk8ZogFzRHRet0At3xuy5GYIPVOT0TKK7
rDAACyPOGa1+7bgXNoRjueA32XP3pOb5ap6Hrt541
Z07dbnNGd9bEkbOKM7y9AvHEjBBEhRfCfx+Mbv
AZ/X/wpsmL01E91C88FjceJHAVh5FGAw5FMkAhyI
8/x29MHAguykXIH5ipMfOC7H9K3GmRl85HOF
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

pxGrid

Additional Attributes:

Attributes:

Submit >

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。

Microsoft Active Directory Certificate Services – lab6-WIN-49T17723U08-CA

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

[Download certificate](#)

[Download certificate chain](#)

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。

Use Generated Certificate and Key

Certificate: No file selected.

Key: No file selected.

Key is Encrypted

No certificate has been uploaded.

Use Generated Certificate and Key

Common name: wsa.lab6.com
 Organization: Cisco
 Organizational Unit: Engineering
 Country: US
 Expiration Date: Jun 22 21:38:55 2016 GMT
 Basic Constraints: Critical

[Download Certificate...](#) | [Download Certificate Signing Request...](#)

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate: wsa.cer

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。

Cisco S000V
Web Security Virtual Appliance

Reporting Web Security Manager Security Services Network System Administration

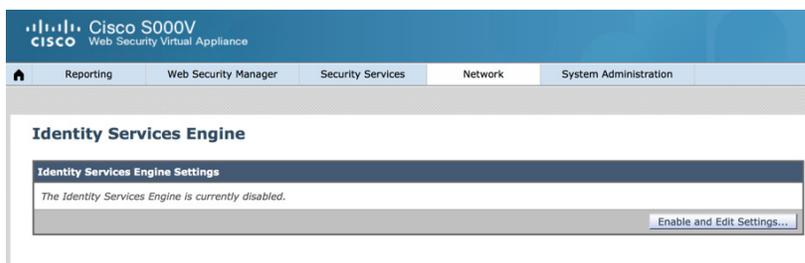
Edit Log Subscription

Log Subscription	
Log Type:	Access Logs
Log Name:	accesslogs <small>(will be used to name the log directory)</small>
Rollover by File Size:	10G Maximum <small>(Add a trailing K or M to indicate size units)</small>
Rollover by Time:	None
Log Style:	<input checked="" type="radio"/> Squid <input type="radio"/> Apache <input type="radio"/> Squid Details
Custom Fields (optional):	%m Custom Fields Reference
File Name:	aclog
Log Compression:	<input type="checkbox"/> Enable
Log Exclusions (Optional):	<input type="text"/> <small>(Enter the HTTP status codes of transactions that should not be included in the Access Log)</small>
Retrieval Method:	<input checked="" type="radio"/> FTP on mgmt.wsa.lab6.com Maximum Number of Files: 10 <input type="radio"/> FTP on Remote Server

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。

Secondary ISE pxGrid Node (optional): The WSA will communicate with the ISE pxGrid node to support WSA data subscription (ongoing updates). Specifying a secondary ISE pxGrid node (server) is optional.

(Hostname or IPv4 address)

ISE pxGrid Node Certificate:

If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.

Certificate: No file selected.

Common name: lab6-WIN-49T17723U08-CA
 Organization:
 Organizational Unit:
 Country:
 Expiration Date: May 18 02:38:28 2020 GMT
 Basic Constraints: Critical

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。

ISE Monitoring Node Admin Certificates: The WSA will communicate with an ISE Monitoring node for WSA data initialization (bulk download). The ISE pxGrid node(s) configured above will provide a list of Monitoring nodes. However, additional certificates may need to be uploaded here to enable this communication.

If the ISE Monitoring Node Administration certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.

Primary ISE Monitoring Node Admin Certificate:

Certificate: No file selected.

Common name: ise14pmnt.lab6.com
 Organization:
 Organizational Unit:
 Country:
 Expiration Date: Jun 18 02:36:07 2017 GMT
 Basic Constraints: Not Critical

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。

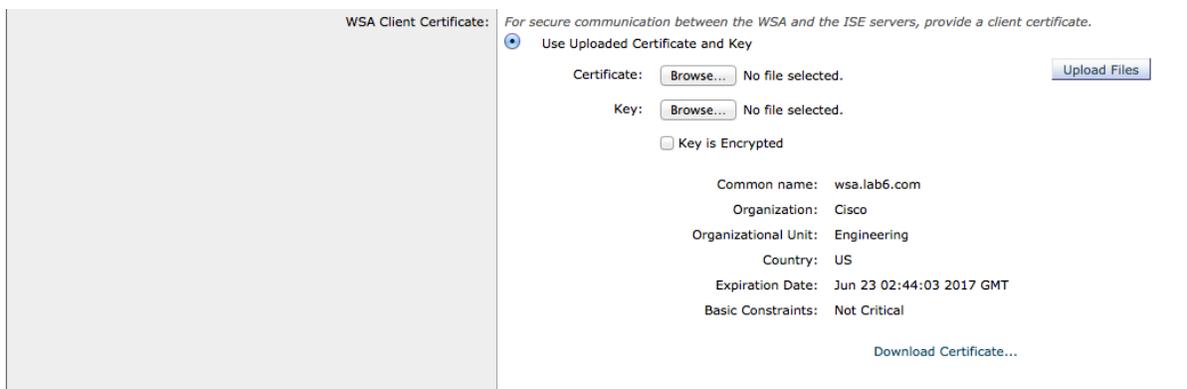
Secondary ISE Monitoring Node Admin Certificate:

Certificate: No file selected.

Common name: ise14smnt.lab6.com
 Organization:
 Organizational Unit:
 Country:
 Expiration Date: Jun 18 02:46:19 2017 GMT
 Basic Constraints: Not Critical

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。

Enable ISE Service

Primary ISE pxGrid Node: The WSA will communicate with the ISE pxGrid node to support WSA data subscription (ongoing updates). A primary ISE pxGrid node (server) must be configured.

10.0.0.93 (Hostname or IPv4 address)

ISE pxGrid Node Certificate:
If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.

Certificate: No file selected.

Common name: lab6-WIN-49T17723U08-CA
Organization:
Organizational Unit:
Country:
Expiration Date: May 18 02:38:28 2020 GMT
Basic Constraints: Critical

Secondary ISE pxGrid Node (optional): The WSA will communicate with the ISE pxGrid node to support WSA data subscription (ongoing updates). Specifying a secondary ISE pxGrid node (server) is optional.

10.0.0.95 (Hostname or IPv4 address)

ISE pxGrid Node Certificate:
If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.

Certificate: No file selected.

Common name: lab6-WIN-49T17723U08-CA
Organization:
Organizational Unit:
Country:
Expiration Date: May 18 02:38:28 2020 GMT
Basic Constraints: Critical

ISE Monitoring Node Admin Certificates: The WSA will communicate with an ISE Monitoring node for WSA data initialization (bulk download). The ISE pxGrid node(s) configured above will provide a list of Monitoring nodes. However, additional certificates may need to be uploaded here to enable this communication.

If the ISE Monitoring Node Administration certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.

Primary ISE Monitoring Node Admin Certificate:

Certificate: No file selected.

Common name: ise14pmt.lab6.com
Organization:
Organizational Unit:
Country:
Expiration Date: Jun 18 02:36:07 2017 GMT
Basic Constraints: Not Critical

Secondary ISE Monitoring Node Admin Certificate:

Certificate: No file selected.

Common name: ise14mnt.lab6.com
Organization:
Organizational Unit:
Country:
Expiration Date: Jun 18 02:46:19 2017 GMT
Basic Constraints: Not Critical

WSA Client Certificate: For secure communication between the WSA and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

Use Uploaded Certificate and Key

Certificate: No file selected.

Key: No file selected.

Key is Encrypted

Common name: wsa.lab6.com
Organization: Cisco
Organizational Unit: Engineering
Country: US
Expiration Date: Jun 23 02:44:03 2017 GMT
Basic Constraints: Not Critical

Use Generated Certificate and Key

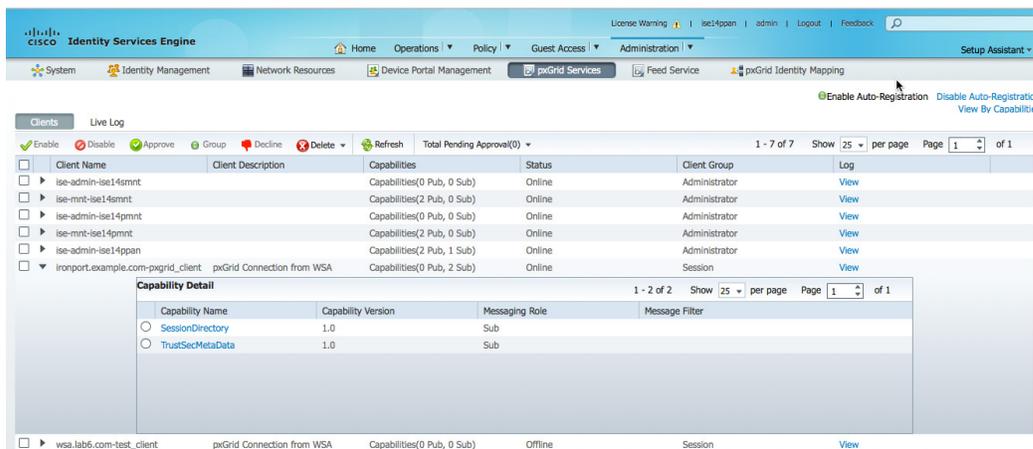
No certificate has been generated.

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。



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and pxGrid Identity Mapping. The main content area displays the 'Clients' page with a 'Live Log' section. A table lists clients with columns for Client Name, Client Description, Capabilities, Status, Client Group, and Log. One client is highlighted: 'ironport.example.com-pxgrid_client' with a description of 'pxGrid Connection from WSA'. Below this, a 'Capability Detail' table shows the following data:

Capability Name	Capability Version	Messaging Role	Message Filter
SessionDirectory	1.0	Sub	
TrustSecMetaData	1.0	Sub	

At the bottom of the screenshot, another client entry is visible: 'wsa.lab6.com-test_client' with a description of 'pxGrid Connection from WSA' and a status of 'Offline'.

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)

Identification Profiles: ISE	
Client / User Identification Profile Settings	
<input checked="" type="checkbox"/> Enable Identification Profile	
Name: ?	ISE <small>(e.g. my IT Profile)</small>
Description:	
Insert Above:	1 (Global Profile) ▾
User Identification Method	
Identification and Authentication: ?	Transparently identify users with ISE ▾
Fallback to Authentication Realm or Guest Privileges: ?	If user information is not available from the Identity Services Engine: Support Guest Privileges ▾ <small>Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).</small>
Membership Definition	
<small>Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.</small>	
Define Members by Subnet:	10.0.0.0/24 <small>(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)</small>
Define Members by Protocol:	<input checked="" type="checkbox"/> HTTP/HTTPS <input type="checkbox"/> Native FTP
Advanced	<small>Define additional group membership criteria.</small>

- 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。

Authorized Secure Group Tags

Use the search function below to add Secure Group Tags. To remove Secure Group Tags from this policy, use the Delete option.

0 Secure Group Tag(s) currently included in this policy.

Secure Group Tag Name	SGT Number	SGT Description	Delete
No Secure Group Tags selected.			
			All

Delete

Secure Group Tag Search

Enter any text to search for a Secure Group Tag name, number, or description. Select one or more Secure Group Tags from the list and use the Add button to add to this policy.

Search

0 Secure Group Tag(s) selected for Add Add

Secure Group Tag Name	SGT Number	SGT Description	Select
Unknown	0	Unknown Security Group	<input type="checkbox"/>
Engineering	3	__NONE__	<input type="checkbox"/>
ASA	2	__NONE__	<input type="checkbox"/>
ANY	65535	Any Security Group	<input type="checkbox"/>

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。

Secure Group Tag Search

Enter any text to search for a Secure Group Tag name, number, or description. Select one or more Secure Group Tags from the list and use the Add button to add to this policy.

Search

1 Secure Group Tag(s) selected for Add Add

Secure Group Tag Name	SGT Number	SGT Description	Select
Unknown	0	Unknown Security Group	<input type="checkbox"/>
Engineering	3	__NONE__	<input checked="" type="checkbox"/>
ASA	2	__NONE__	<input type="checkbox"/>
ANY	65535	Any Security Group	<input type="checkbox"/>

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。

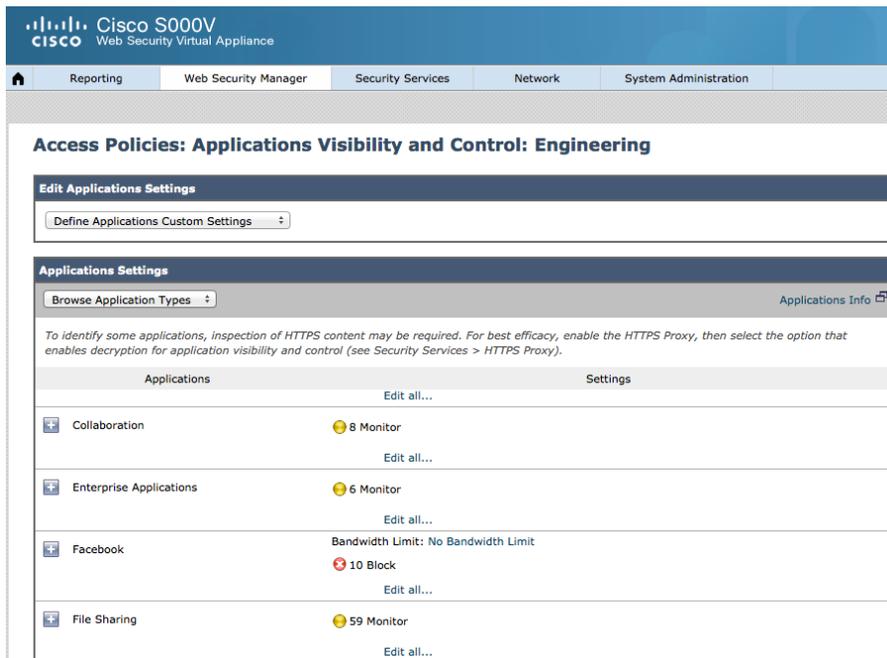
ステップ 7 [URL フィルタリング (URL Filtering)] で、[グローバル ポリシー (Global Policy)] を選択し、次のように設定します。

Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn	Quota-Based	Time-Based
Real Estate	Select all <input checked="" type="checkbox"/>	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Reference	<input checked="" type="checkbox"/>					
Religion	<input checked="" type="checkbox"/>					
SaaS and B2B	<input checked="" type="checkbox"/>					
Safe for Kids	<input checked="" type="checkbox"/>					
Science and Technology	<input checked="" type="checkbox"/>					
Search Engines and Portals	<input checked="" type="checkbox"/>					
Sex Education	<input checked="" type="checkbox"/>					
Shopping	<input checked="" type="checkbox"/>					
Social Networking	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Social Science	<input checked="" type="checkbox"/>					
Society and Culture	<input checked="" type="checkbox"/>					
Software Updates	<input checked="" type="checkbox"/>					
Sports and Recreation	<input checked="" type="checkbox"/>					
Streaming Audio	<input checked="" type="checkbox"/>					
Streaming Video	<input checked="" type="checkbox"/>					
Tobacco	<input checked="" type="checkbox"/>					

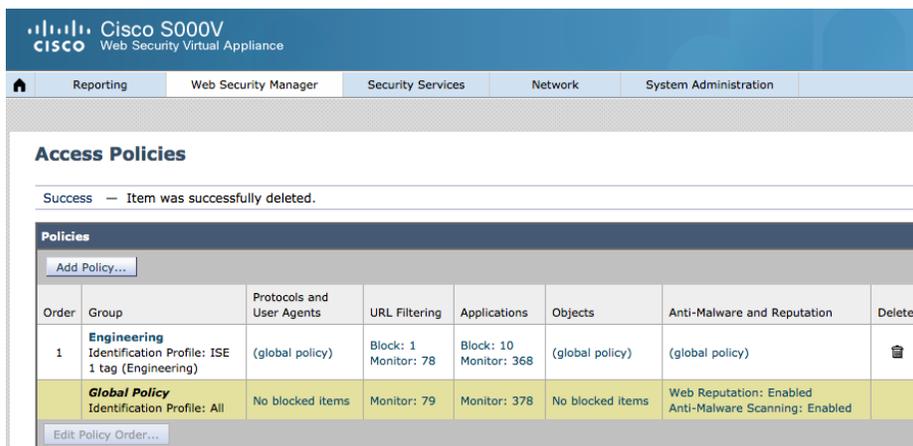
ステップ 8 [送信 (Submit)] を選択します

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 : DecryptEngineering (Policy Name: DecryptEngineering)]

Decryption Policy: DecryptEngineering

Policy Settings	
<input checked="" type="checkbox"/> Enable Policy	
Policy Name: ?	DecryptEngineering <small>(e.g., my IT policy)</small>
Description:	<input type="text"/>
Insert Above Policy:	1 (Global Policy) ▾

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。

Policy Member Definition					
<i>Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.</i>					
Identification Profiles and Users:	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> Select One or More Identification Profiles ▾ Add Identification Profile </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Identification Profile</th> <th style="width: 40%;">Authorized Users and Groups</th> </tr> </thead> <tbody> <tr> <td>ISE ▾</td> <td> <input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users ? ISE Secure Group Tags: Engineering Users: No users entered <input type="radio"/> Guests (users failing authentication) </td> </tr> </tbody> </table> </div>	Identification Profile	Authorized Users and Groups	ISE ▾	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users ? ISE Secure Group Tags: Engineering Users: No users entered <input type="radio"/> Guests (users failing authentication)
Identification Profile	Authorized Users and Groups				
ISE ▾	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users ? ISE Secure Group Tags: Engineering Users: No users entered <input type="radio"/> Guests (users failing authentication)				
Advanced	<p><small>Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.</small></p> <p>Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.</p> <p>The following advanced membership criteria have been defined:</p> <p>Proxy Ports: None Selected</p> <p>Subnets: None Selected</p> <p>Time Range: No Time Range Definitions Available <small>(see Web Security Manager > Defined Time Ranges)</small></p> <p>URL Categories: None Selected</p> <p>User Agents: None Selected</p>				

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 (Decrypt)] で [ソーシャル ネットワーキング (Social Networking)] を選択します。

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					
		Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Pornography		✓				–	–
Professional Networking		✓				–	–
Real Estate		✓				–	–
Reference		✓				–	–
Religion		✓				–	–
SaaS and B2B		✓				–	–
Safe for Kids		✓				–	–
Science and Technology		✓				–	–
Search Engines and Portals		✓				–	–
Sex Education		✓				–	–
Shopping		✓				–	–
Social Networking				✓		–	–
Social Science		✓				–	–
Society and Culture		✓				–	–
Software Updates		✓				–	–
Sports and Recreation		✓				–	–
Streaming Audio		✓				–	–

Cancel Submit

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。

Decryption Policies

Success — Item was successfully deleted.

Order	Group	URL Filtering	Web Reputation	Default Action	Delete
1	DecryptEngineering Identification Profile: ISE 1 tag (Engineering)	Pass Through: 77 Monitor: 1 Decrypt: 1	(global policy)	(global policy)	
	Global Policy Identification Profile: All	Pass Through: 78 Monitor: 1	Enabled	Decrypt	

Edit Policy Order...

アプリケーションの復号化

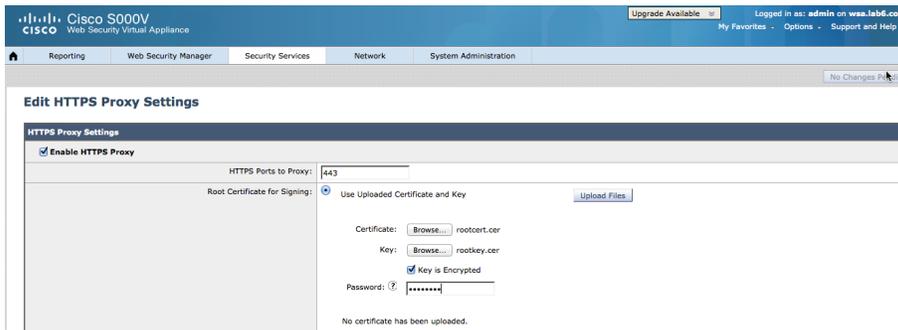
HTTPS プロキシを有効にし、暗号化された Web サイトを復号化できるようにします。次に、ルート公開/秘密キーのペアをアップロードする例を示します。下位の CA テンプレートを 사용하여 CA の署名付き証明書をアップロードするオプションもあります。エンジニアリング SGT が割り当てられているユーザをブロックするため、後でこれを Web アクセス ポリシー内に使用します。

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。

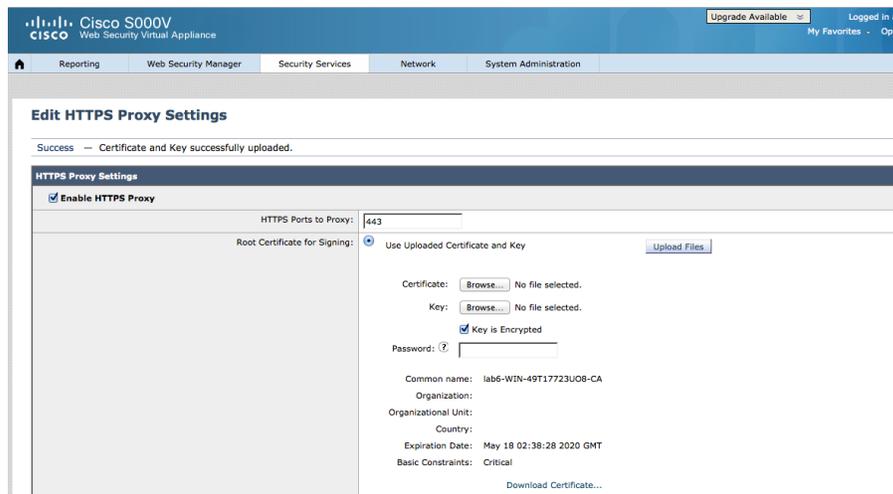
ステップ 2 [設定の有効化および編集 (Enable and Edit Settings)] > [プロキシ契約に署名する (Sign Proxy Agreement)] をクリックします。

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。

Decryption Options	
Decrypt for Authentication: ?	<input checked="" type="checkbox"/> Enable decryption for authentication <i>If the user has not been authenticated prior to the HTTPS transaction, the request will be denied if not decrypted.</i>
Decrypt for End-User Notification: ?	<input checked="" type="checkbox"/> Enable decryption for display of end-user notification pages. <i>Decryption is necessary to display an end-user notification page in the event of a policy block.</i>
Decrypt for End-User Acknowledgement: ?	<input checked="" type="checkbox"/> Enable decryption for display of the end-user acknowledgement page <i>If the user has not acknowledged the web proxy prior to the HTTPS transaction, the acknowledgement page cannot be displayed and the request will be denied.</i>
Decrypt for Application Detection: ?	<input checked="" type="checkbox"/> Enable decryption for enhanced application visibility and control <i>Enabling this option will improve the efficacy of detection for some HTTPS applications. However, decryption may cause outages unless the root certificate for signing is installed on the client.</i>
Invalid Certificate Options	

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。

Expired Certificate

Mismatched Hostname

Unrecognized Root Authority / Issuer

Invalid

Invalid

All other error types

No end-user notification page displayed

Revoked Certificate

Confirm Enable

Once the HTTPS proxy service is enabled, HTTPS blocking will no longer be available in Access policies. In addition, the HTTPS protocol can no longer be used to define membership in Access, Routing, Outbound Malware Scanning, Cisco Data Security Policies, and External DLP policies. All HTTPS policy decisions will be handled by Decryption policies.

Do you want to continue?

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。

HTTPS Proxy

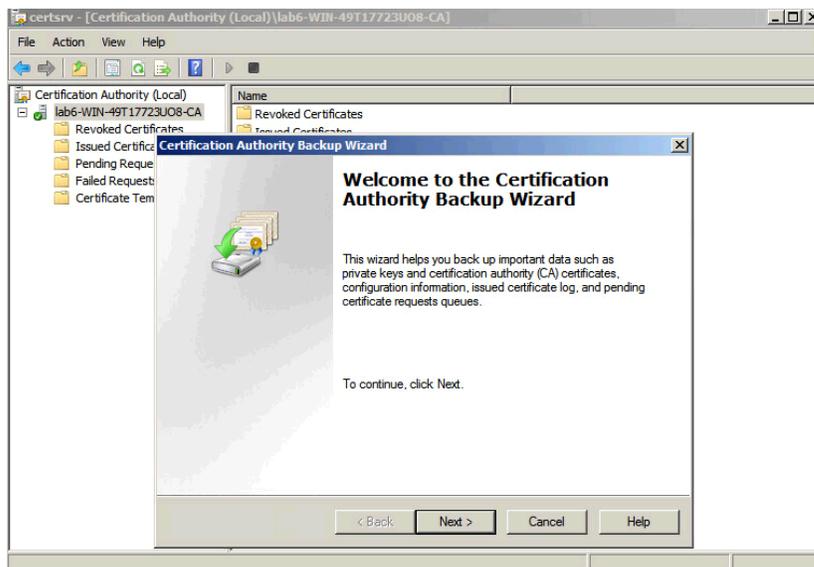
Success — Your changes have been committed.

HTTPS Proxy Settings	
HTTPS Proxy:	Enabled
HTTPS Ports to Proxy:	443
Root Certificate and Key for Signing:	Using Uploaded Certificate: Common name: lab6-WIN-49T17723U08-CA Organization: Organizational Unit: Country: Expiration Date: May 18 02:38:28 2020 GMT Basic Constraints: Critical
Decryption Options	
Decrypt for Authentication:	Enabled
Decrypt for End-User Notification:	Enabled
Decrypt for End-User Acknowledgement:	Enabled
Decrypt for Application Detection:	Enabled
Invalid Certificate Options	
Invalid Certificate Handling:	Expired: Monitor Mismatched Hostname: Monitor Unrecognized Root Authority / Issuer: Drop Invalid Signing Certificate: Drop Invalid Leaf Certificate: Drop All other error types: Drop

ルート公開キー/秘密キー ペアの取得

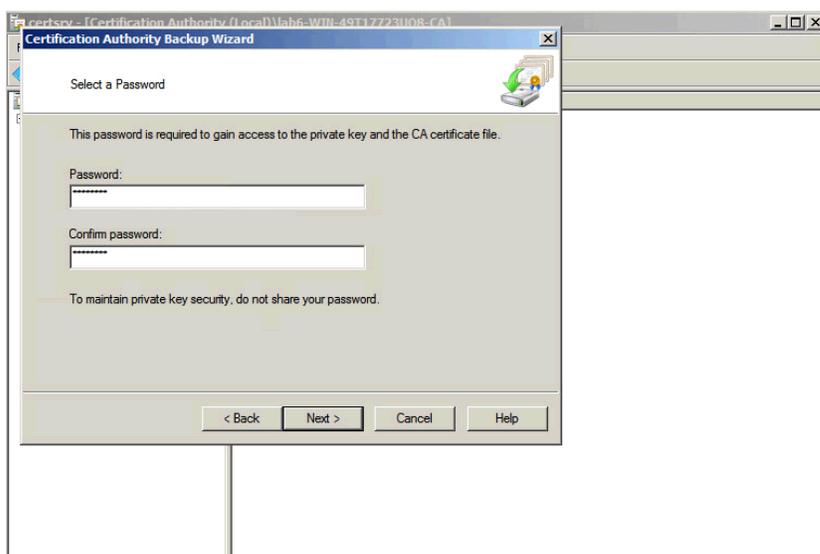
ステップ 1 秘密キーを使用してルート CA をバックアップします。

[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-49T17723U08-CA.p12 -nocerts -out rootkey.cer
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

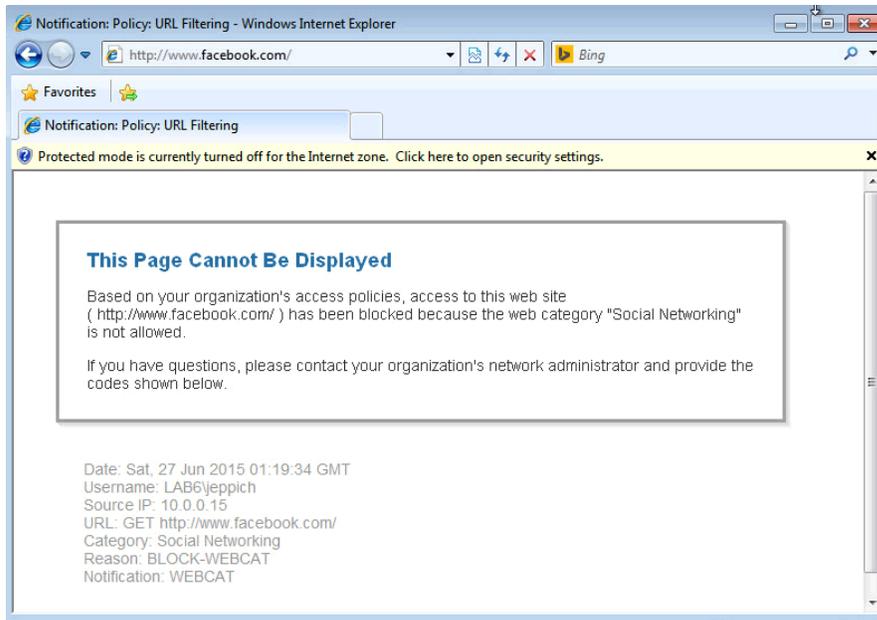
openssl pkcs12 -in lab6-WIN-49T17723U08-CA.p12 -clcerts -nokeys -out rootcert.cer
Enter Import Password:
MAC verified OK
```

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。

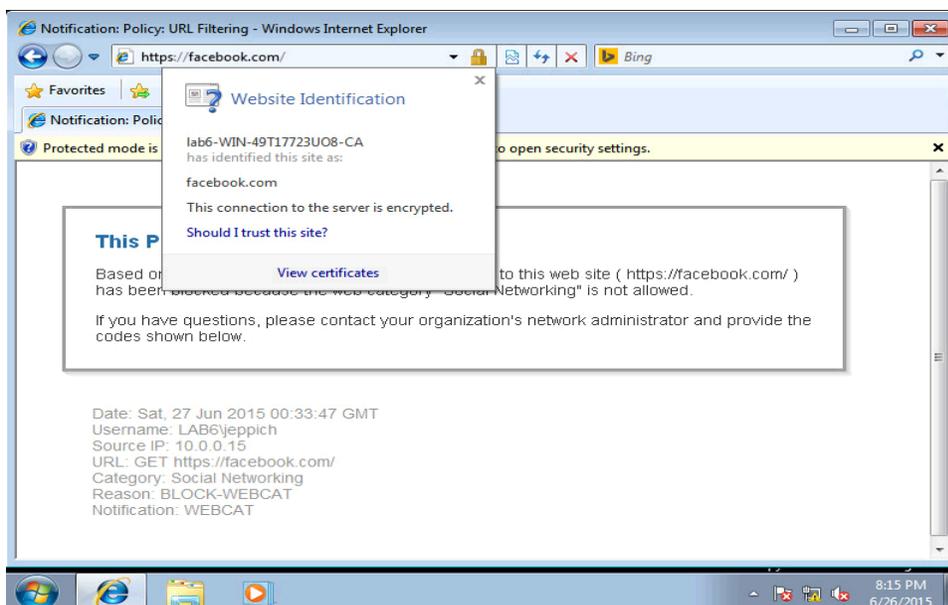
クライアントのテスト

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。

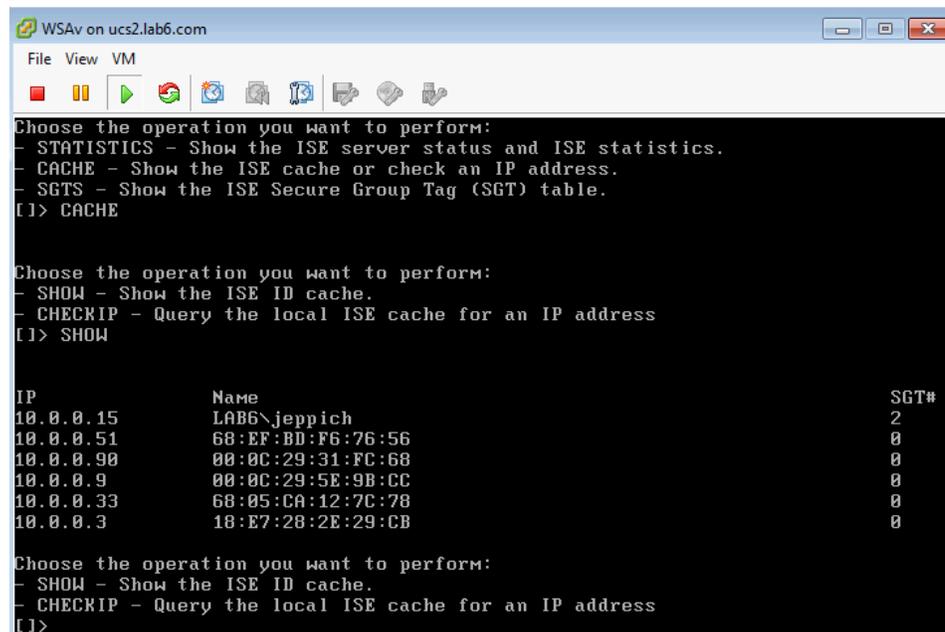


ステップ 2 ユーザが <https://facebook.com> と入力しても、アクセスは拒否されます。



ステップ 3 仮想 WSA で、次のように入力します。

```
isedata
CACHE
SHOW
```



```
Choose the operation you want to perform:
- STATISTICS - Show the ISE server status and ISE statistics.
- 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        2
10.0.0.51         68:EF:BD:F6:76:56   0
10.0.0.90         00:0C:29:31:FC:68   0
10.0.0.9          00:0C:29:5E:9B:CC   0
10.0.0.33         68:05:CA:12:7C:78   0
10.0.0.3          18:E7:28:2E:29:CB   0

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

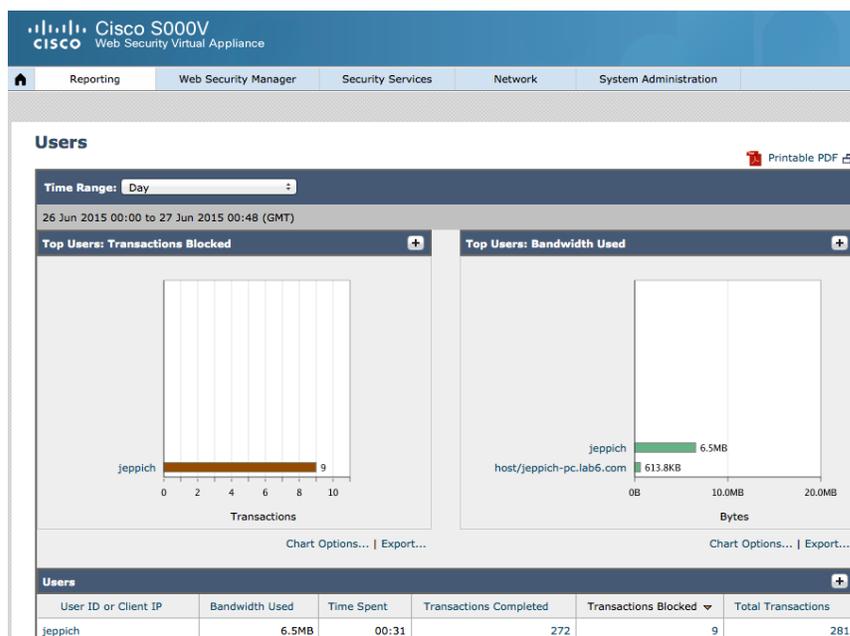
認証済みユーザの SG-IP のマッピングに注意してください。

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。

The screenshot shows the Cisco S000V Web Security Virtual Appliance interface. The 'Web Tracking' section is active, displaying search criteria and results. The search criteria include: Time Range: Day, User/Client IPv4 or IPv6: LAB6\jeppich, Website: (empty), Transaction Type: Blocked. The results table shows two entries for blocked transactions to Facebook.

Time (GMT +00:00)	Website (count)	Disposition	Bandwidth	User / Client IP
27 Jun 2015 00:33:47	https://facebook.com:443	Block - URL Cat	0B	jeppich 10.0.0.15
27 Jun 2015 00:24:33	http://www.facebook.com	Block - URL Cat	0B	jeppich 10.0.0.15

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。

The screenshot shows the Cisco S000V Web Security Virtual Appliance interface with the 'Policy Trace' section active. The 'Destination' field is set to 'https://facebook.com'. The 'Transaction' section is configured with 'Authentication / Identification' set to 'Identity Services Engine (ISE)', 'Client IP Address' set to '10.0.0.15', and 'User Name' left empty. A 'Find Policy Match' button is visible at the bottom right.

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。

Results

User Information
 User Name: None
 Authentication Realm Group Membership: None
 Secure Group Tag Membership: Engineering
 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:38.0) Gecko/20100101 Firefox/38.0

URL Check
 WBSR Score: 7.0
 URL Category: Social Networking
 Scanner "AVC" Verdict (Request): Facebook General (Facebook)

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

Final Result
Request completed
 Details: HTTPS request decrypted based on URL category
 Trace session complete

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。

Cisco S000V Web Security Virtual Appliance

Reporting | Web Security Manager | Security Services | Network | System Administration

Users > LAB6\jeppich

Time Range: Day
 26 Jun 2015 01:00 to 27 Jun 2015 01:07 (GMT)

URL Categories: Total Transactions

URL Category	Transactions
Social Networking	158
Uncategorized URLs	34
Business and Industry	29
Search Engines and Portals	27
Computer Security	11
Computers and Internet	8
Advertisements	5
Web Hosting	3
Infrastructure and Content Delivery Netw...	2
Web-based Email	2

Trend: Total Transactions

URL Categories Matched

URL Category	Bandwidth Used	Time Spent	Blocked URL Category	Transactions Completed	Total Transactions
Social Networking	4.8MB	00:21	5	150	158
Uncategorized URLs	351.8KB	00:05	0	34	34
Business and Industry	192.3KB	00:01	0	29	29
Search Engines and Portals	908.4KB	00:00	0	27	27
Computer Security	19.1KB	00:00	0	11	11
Computers and Internet	125.0KB	00:01	0	8	8
Advertisements	62.9KB	00:00	0	5	5
Web Hosting	7,413B	00:00	0	3	3
Infrastructure and Content Delivery Netw...	80.0KB	00:00	0	2	2
Web-based Email	10.8KB	00:00	0	2	2
Totals (all available data):	6.5MB	00:31	5	272	280

Find URL Category

Domains Matched					
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
<input type="text"/> 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):		--	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):		--	272	9	281
<input type="text"/> 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。

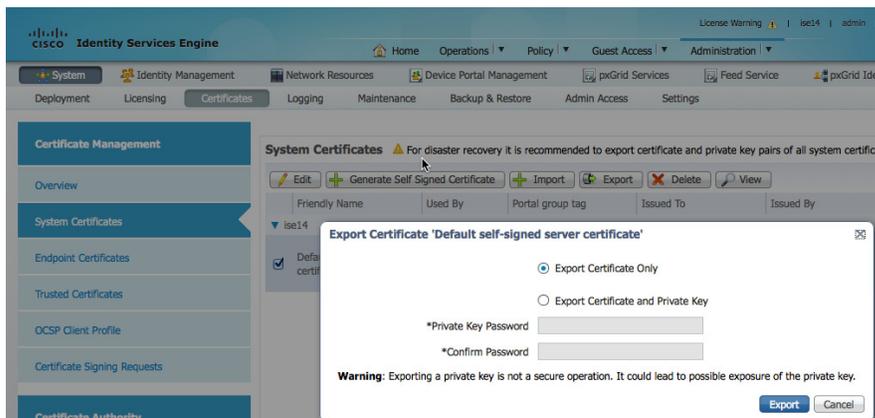
```
openssl req -x509 -days 365 -key wsa_self.key -in wsa_self.csr -out wsa_self.cer
```

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)]

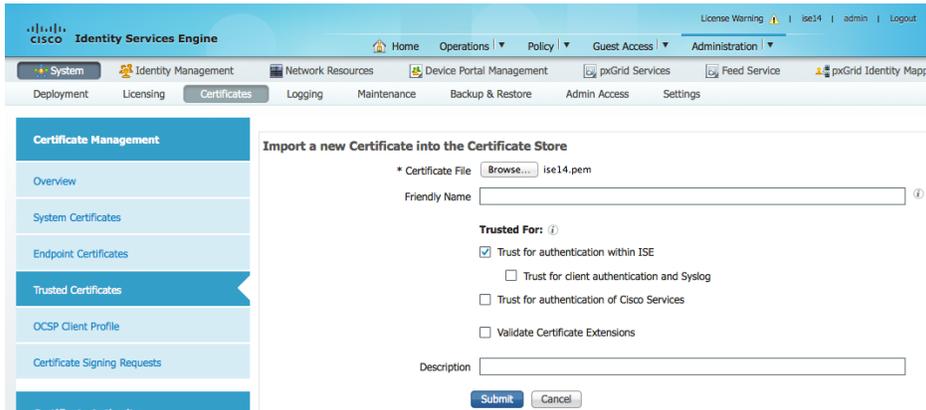
注: 秘密キーは不要です。



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。

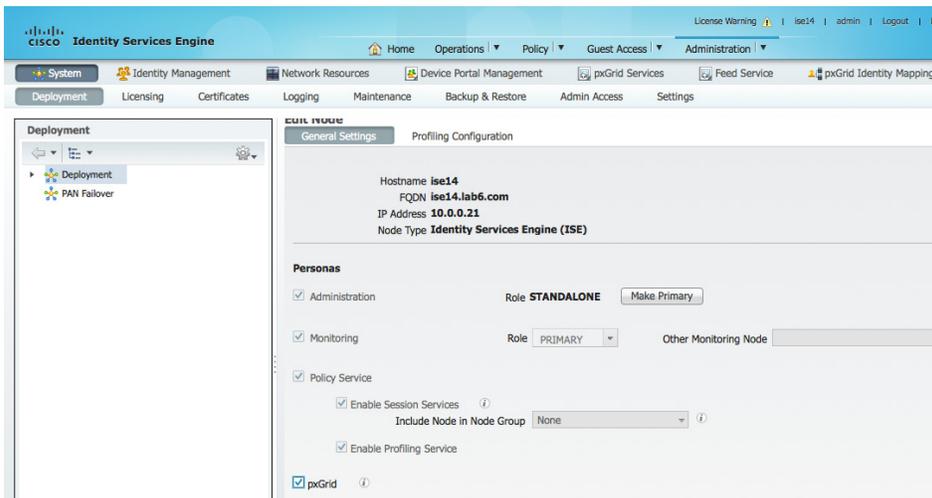
ステップ 3 [管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [信頼できる証明書 (Trusted Certificates)] > [インポート (Import)] > [証明書ファイル (Certificate file)] を選択し、PEM ファイルを選択してアップロードします。

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。

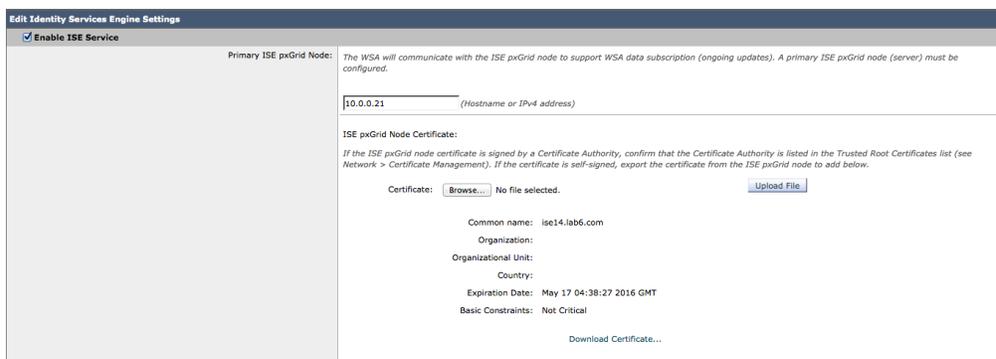


WSA と ISE pxGrid ノードの設定

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。

Secondary ISE pxGrid Node (optional): The WSA will communicate with the ISE pxGrid node to support WSA data subscription (ongoing updates). Specifying a secondary ISE pxGrid node (server) is optional.

(Hostname or IPv4 address)

ISE pxGrid Node Certificate:

If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.

Certificate: No file selected.

No certificate has been uploaded. If a secondary pxGrid node is in use, ensure that the pxGrid certificate is signed by a trusted Certificate Authority.

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。

ISE Monitoring Node Admin Certificates: The WSA will communicate with an ISE Monitoring node for WSA data initialization (bulk download). The ISE pxGrid node(s) configured above will provide a list of Monitoring nodes. However, additional certificates may need to be uploaded here to enable this communication.

If the ISE Monitoring Node Administration certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.

Primary ISE Monitoring Node Admin Certificate:

Certificate: No file selected.

Common name: ise14.lab6.com
 Organization:
 Organizational Unit:
 Country:
 Expiration Date: May 17 04:38:27 2016 GMT
 Basic Constraints: Not Critical

ステップ 5 セカンダリ MNT ノードは空白のままにします。

Secondary ISE Monitoring Node Admin Certificate:

Certificate: No file selected.

No certificate has been uploaded. If a secondary ISE Monitoring node is in use, ensure that the Monitoring Admin certificate used on the ISE pxGrid server is signed by a trusted Certificate Authority.

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。

WSA Client Certificate: For secure communication between the WSA and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

Use Uploaded Certificate and Key

Certificate: No file selected.

Key: No file selected.

Key is Encrypted

Common name:
 Organization: Internet Widgits Pty Ltd
 Organizational Unit:
 Country: AU
 Expiration Date: Jun 26 19:56:00 2016 GMT
 Basic Constraints: Not Critical

Use Generated Certificate and Key

No certificate has been generated.

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: isel4.lab6.com

Test completed successfully.

```

ステップ 8 次が表示されます。

Identity Services Engine

Success — Settings have been saved.

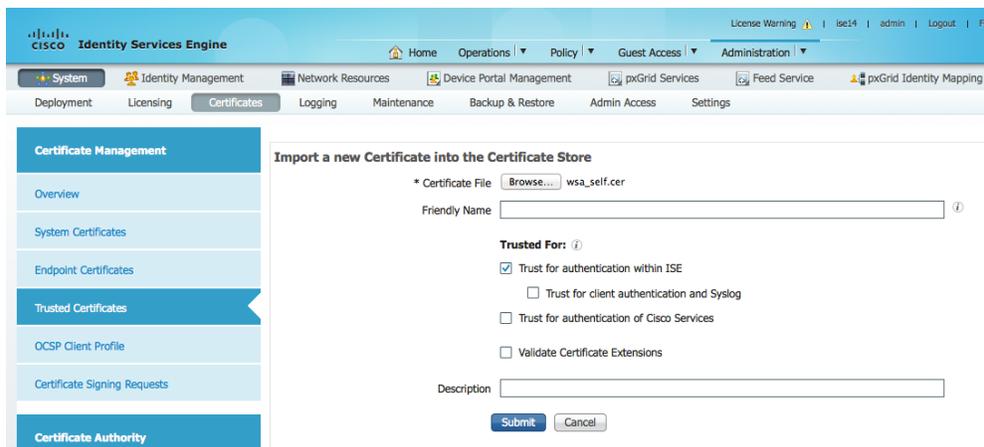
Identity Services Engine Settings	
Primary ISE Server:	10.0.0.21
Primary ISE Server Certificates:	Admin Certificate: Common name: isel4.lab6.com Organization: Organizational Unit: Country: Expiration Date: May 17 04:38:27 2016 GMT Basic Constraints: Not Critical PxGrid Certificate: Common name: isel4.lab6.com Organization: Organizational Unit: Country: Expiration Date: May 17 04:38:27 2016 GMT Basic Constraints: Not Critical
Secondary ISE Server:	Server is not configured
Secondary ISE Server Certificates:	Use Primary Admin and PxGrid Certificates
WSA Client Certificate:	Using Uploaded Certificate: Common name: Organization: Internet Widgits Pty Ltd Organizational Unit: Country: AU Expiration Date: Jun 26 19:56:00 2016 GMT Basic Constraints: Not Critical

ステップ 9 変更を 2 回確定します。

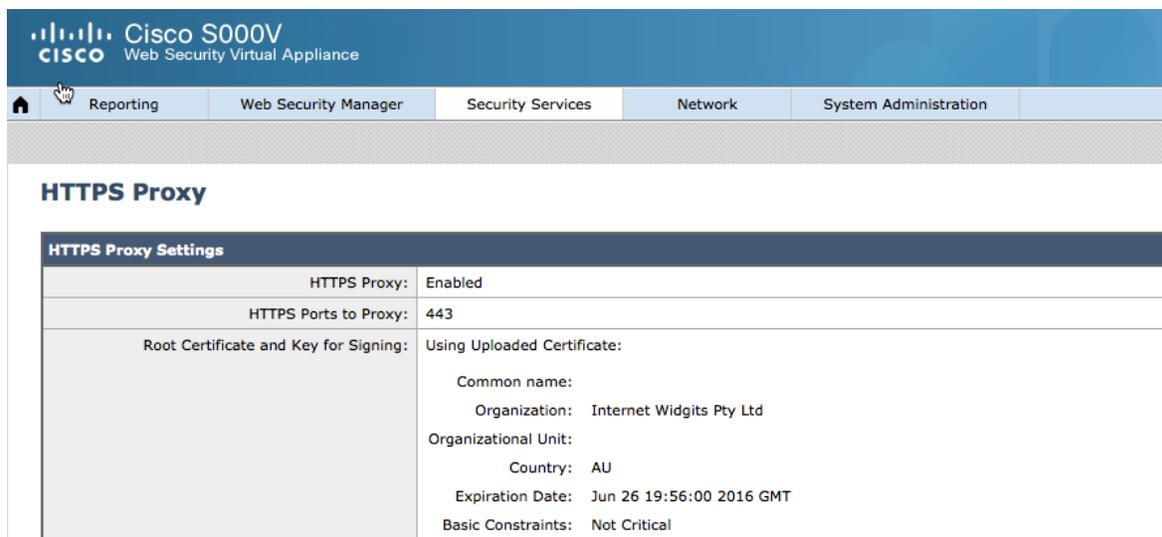
ステップ 10 ISE 信頼ストアに wsa_self.cer をアップロードします。

[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。

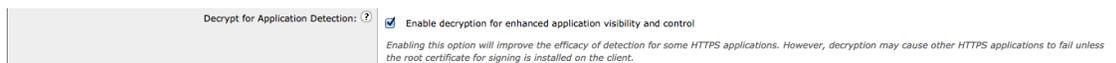
注: ISE 内での認証の信頼を有効にします。



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。

HTTPS Proxy Settings	
HTTPS Proxy:	Enabled
HTTPS Ports to Proxy:	443
Root Certificate and Key for Signing:	Using Uploaded Certificate: Common name: Organization: Internet Widgits Pty Ltd Organizational Unit: Country: AU Expiration Date: Jun 26 19:56:00 2016 GMT Basic Constraints: Not Critical
Decryption Options	
Decrypt for Authentication:	Enabled
Decrypt for End-User Notification:	Enabled
Decrypt for End-User Acknowledgement:	Enabled
Decrypt for Application Detection:	Enabled
Invalid Certificate Options	
Invalid Certificate Handling:	Expired: Monitor Mismatched Hostname: Monitor Unrecognized Root Authority / Issuer: Drop Invalid Signing Certificate: Drop Invalid Leaf Certificate: Drop All other error types: Drop
Online Certificate Status Protocol Options	
OCSLP Result Handling:	Revoked Certificate: Drop Unknown Certificate: Monitor OCSLP Error: Monitor

[Edit Settings...](#)

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。

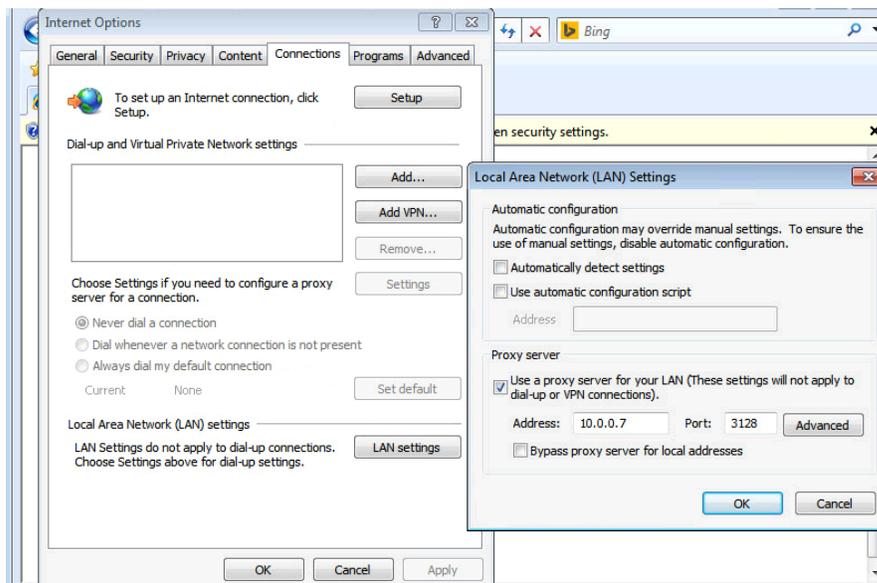
クライアントのテスト

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。

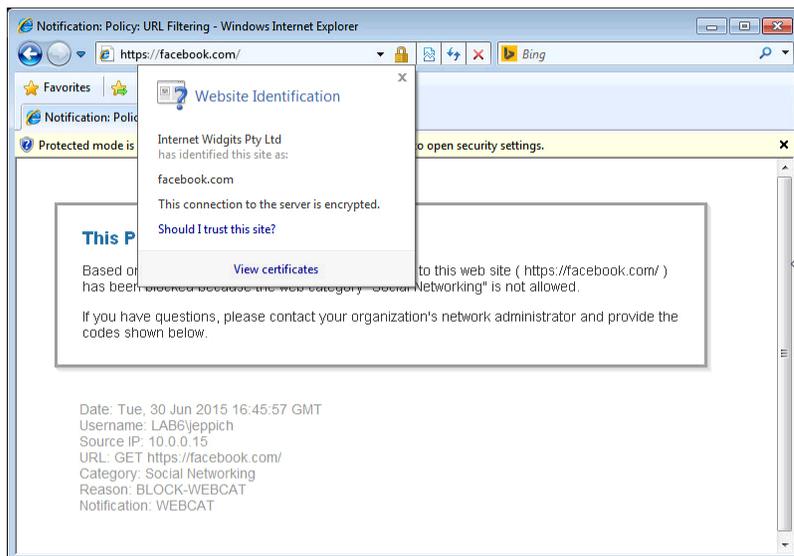
ステップ 1 エンドユーザが正常にログインすると、エンジニアリング SGT が割り当てられます。

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port
2015-06-30 12:44:43.820			0	18-E7:28-2E:29-C	18-E7:28-2E:29-CC	Cisco-Device	Default >> MAB >> Def.	Default >> Basic_Auth...	PermitAccess	sw	GigabitEthernet1/0/37
2015-06-30 12:44:43.813			0	18-E7:28-2E:29-C	18-E7:28-2E:29-CC	Cisco-Device	Default >> MAB >> Def.	Default >> Basic_Auth...	PermitAccess	sw	GigabitEthernet1/0/37
2015-06-30 12:42:55.973			0	LAB6/jeppich	00:0C:29:79:02:AB	VMWare-Device	Default >> Dot1X >> D.	Default >> Engineering	Engineering,PermitAccess	sw	GigabitEthernet1/0/43
2015-06-30 12:42:55.965			0	LAB6/jeppich	00:0C:29:79:02:AB	VMWare-Device	Default >> Dot1X >> D.	Default >> Engineering	Engineering,PermitAccess	sw	GigabitEthernet1/0/43

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。

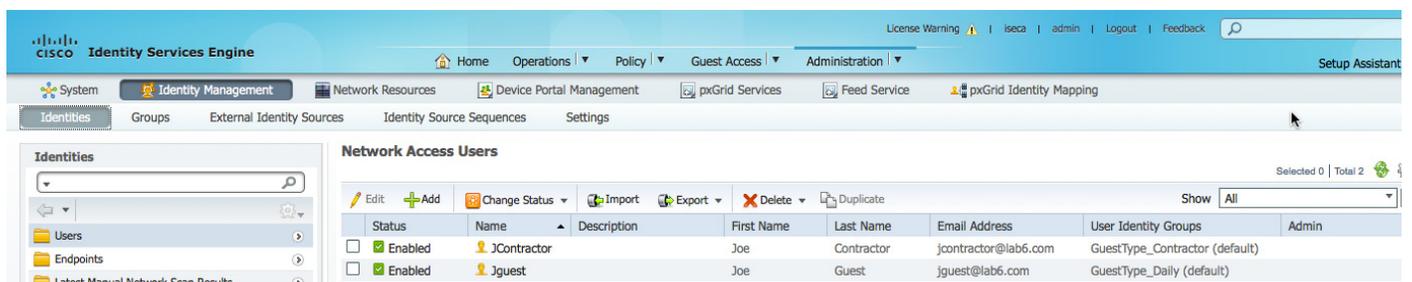
個別の識別プロファイルと Web アクセス ポリシーが、従業員およびゲスト用に定義され、請負業者は WSA で定義されます。

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。

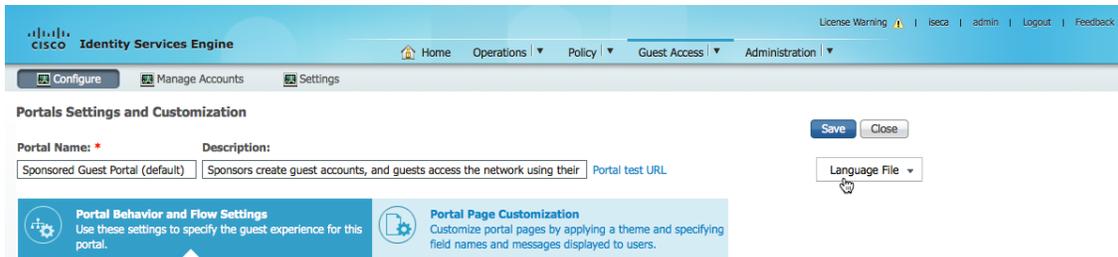
ステップ 2 ユーザごとに [送信 (Submit)] を選択します。



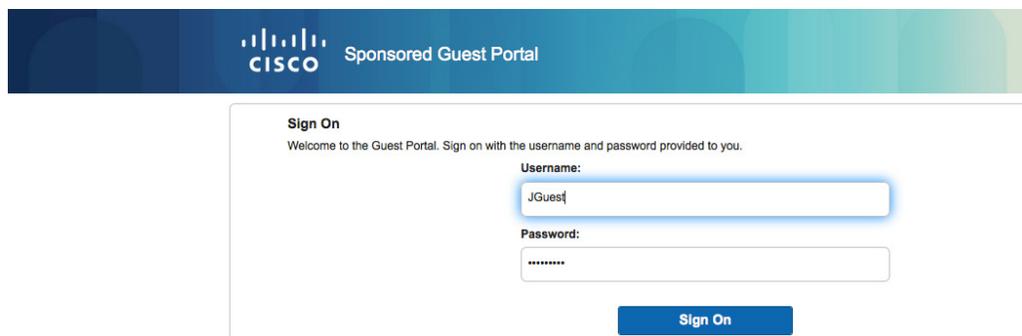
Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input checked="" type="checkbox"/> Enabled	JContractor		Joe	Contractor	jcontractor@lab6.com	GuestType_Contractor (default)	
<input checked="" type="checkbox"/> Enabled	Jguest		Joe	Guest	jguest@lab6.com	GuestType_Daily (default)	

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。

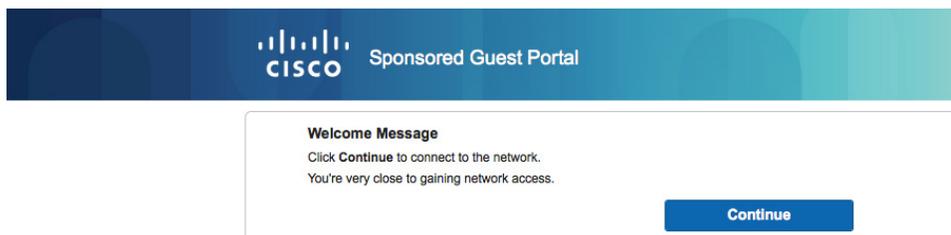
ステップ 4 [ポータルテストの URL(Portal Test URL)] を選択し、ユーザ名を入力して、ISE 内部ユーザをテストします。



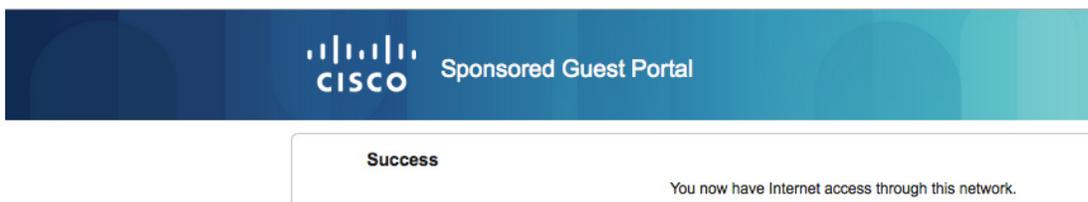
ステップ 5 ユーザクレデンシャルを入力し、サインインします。



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。

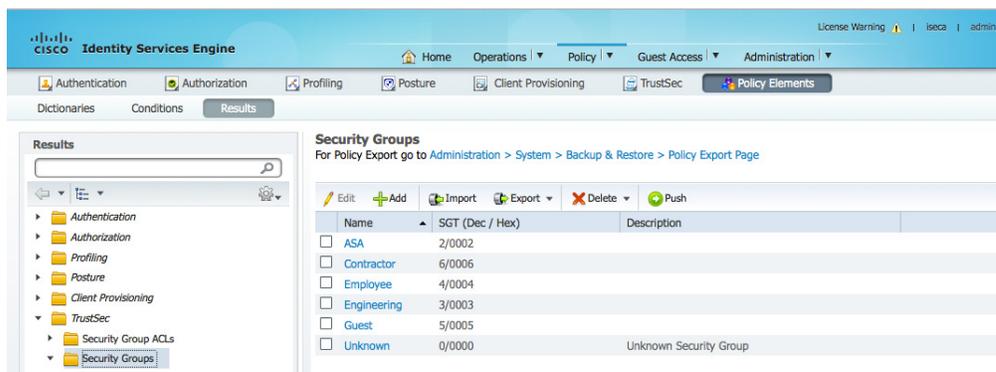
ISE 動的タグ、認可プロファイル、および認可ポリシー

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。

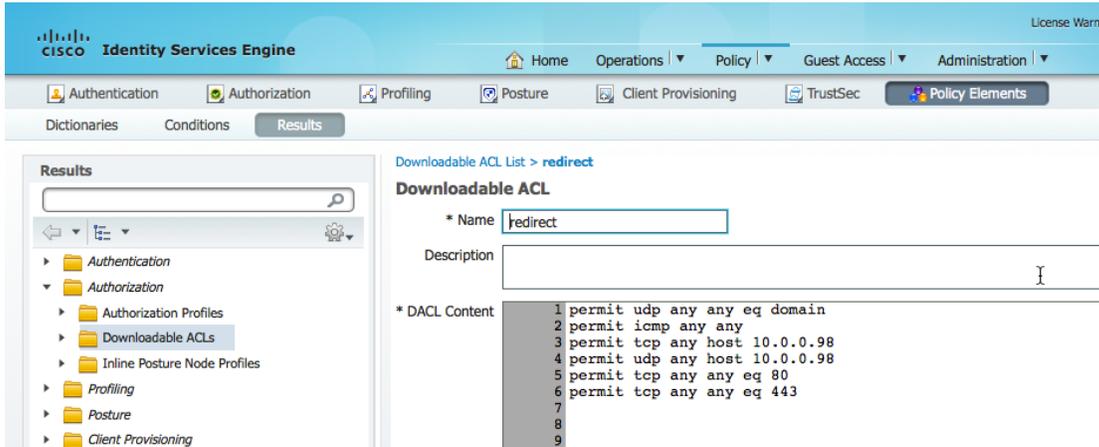
ステップ 1 [ポリシー (Policy)] > [ポリシー要素 (Policy Elements)] > [結果 (Results)] > [TrustSec] > [セキュリティグループ]) で従業員、ゲスト、および請負業者用のタグを追加し、送信します。



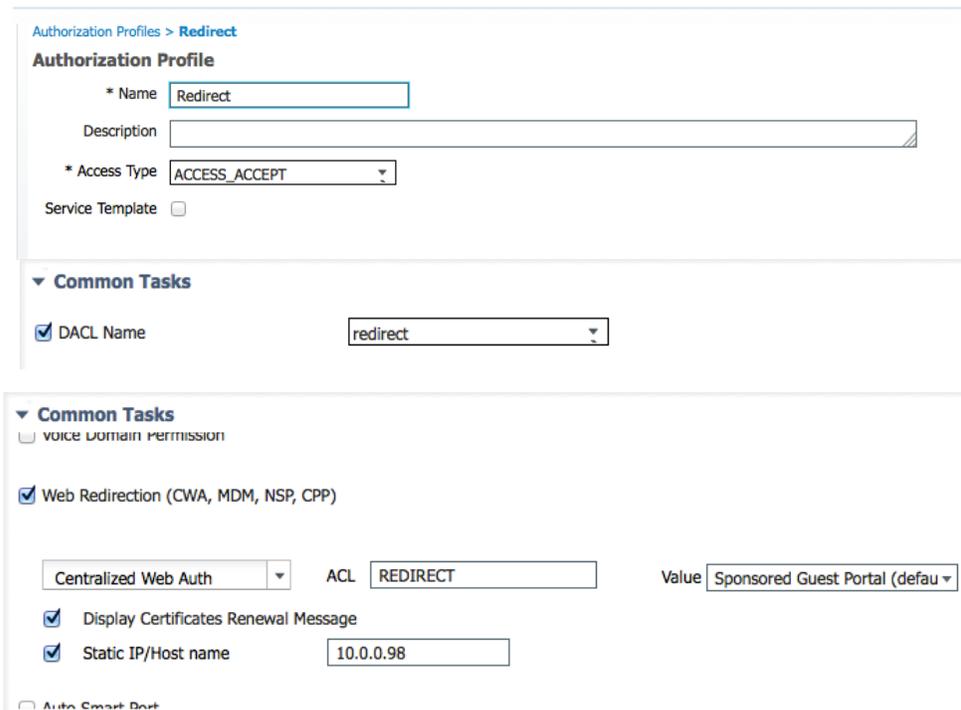
許可プロファイルと CWA 用のダウンロード可能な ACL

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。

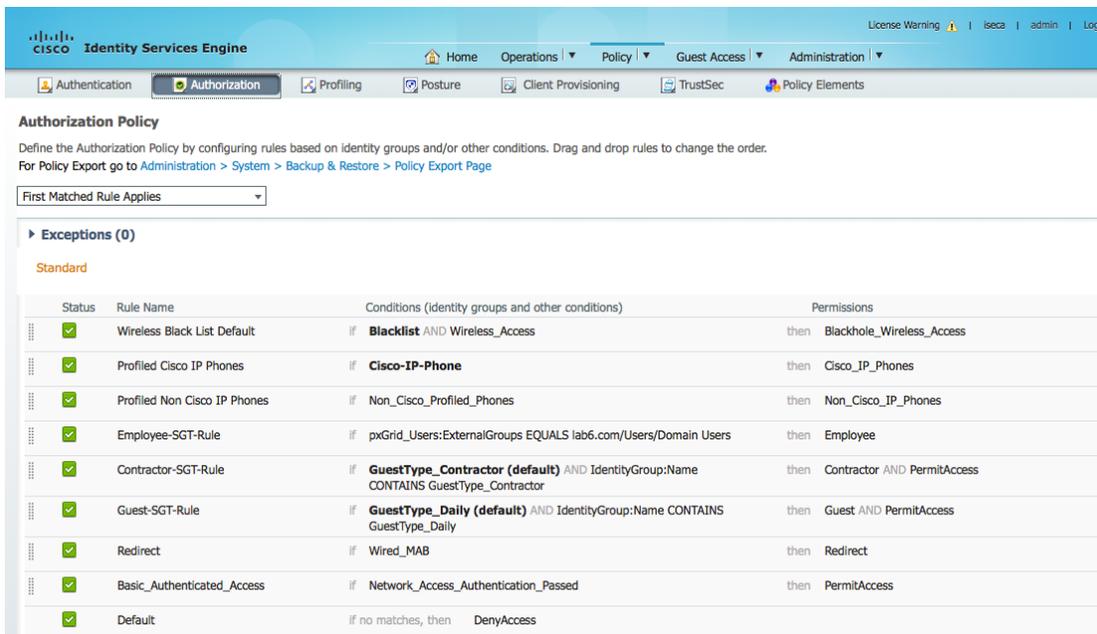
ステップ 1 [ポリシー (Policy)] > [認証 (Authorization)] を選択し、従業員 SGT ルール、請負業者 SGT ルール、およびゲスト SGT ルールを追加します。

[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



Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
✓	Employee-SGT-Rule	if pxGrid_Users:ExternalGroups EQUALS lab6.com/Users/Domain Users	then Employee
✓	Contractor-SGT-Rule	if GuestType_Contractor (default) AND IdentityGroup:Name CONTAINS GuestType_Contractor	then Contractor AND PermitAccess
✓	Guest-SGT-Rule	if GuestType_Daily (default) AND IdentityGroup:Name CONTAINS GuestType_Daily	then Guest AND PermitAccess
✓	Redirect	if Wired_MAB	then Redirect
✓	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then PermitAccess
✓	Default	if no matches, then DenyAccess	

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。

Authorized Secure Group Tags

Use the search function below to add Secure Group Tags. To remove Secure Group Tags from this policy, use the Delete option.

1 Secure Group Tag(s) currently included in this policy.

Secure Group Tag Name	SGT Number	SGT Description	Delete <input type="checkbox"/> All
Employee	4	__NONE__	<input type="checkbox"/>

[Delete](#)

Secure Group Tag Search

Enter any text to search for a Secure Group Tag name, number, or description. Select one or more Secure Group Tags from the list and use the Add button to add to this policy.

0 Secure Group Tag(s) selected for Add [Add](#)

Secure Group Tag Name	SGT Number	SGT Description	Select <input type="checkbox"/> All
Unknown	0	Unknown Security Group	<input type="checkbox"/>
Engineering	3	__NONE__	<input type="checkbox"/>
ASA	2	__NONE__	<input type="checkbox"/>
Guest	5	__NONE__	<input type="checkbox"/>
Employee	4	__NONE__	<input type="checkbox"/>
Contractor	6	__NONE__	<input type="checkbox"/>
ANY	65535	Any Security Group	<input type="checkbox"/>

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。

Policy Settings

Enable Policy

Policy Name: (e.g. my IT policy)

Description:

Insert Above Policy:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Identification Profile	Authorized Users and Groups	Add Identification Profile
<input type="text" value="ISE"/>	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users ? ISE Secure Group Tags: Employee Users: No users entered <input type="radio"/> Guests (users failing authentication)	

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。

Predefined URL Category Filtering

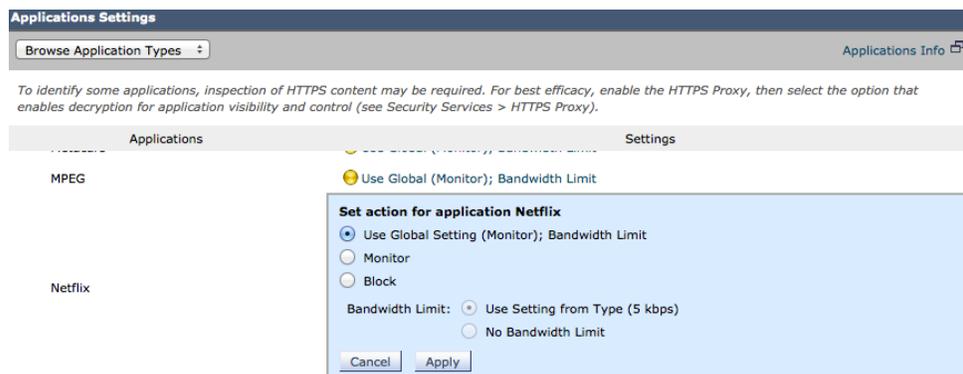
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn ?	Quota-Based	Time-Based
<input checked="" type="checkbox"/> Search Engines and Portals	✓	Select all	Select all	Select all	(Unavailable)	(Unavailable)
<input checked="" type="checkbox"/> Sex Education	✓				-	-
<input checked="" type="checkbox"/> Shopping	✓				-	-
<input checked="" type="checkbox"/> Social Networking		✓			-	-
<input checked="" type="checkbox"/> Social Science	✓				-	-

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。

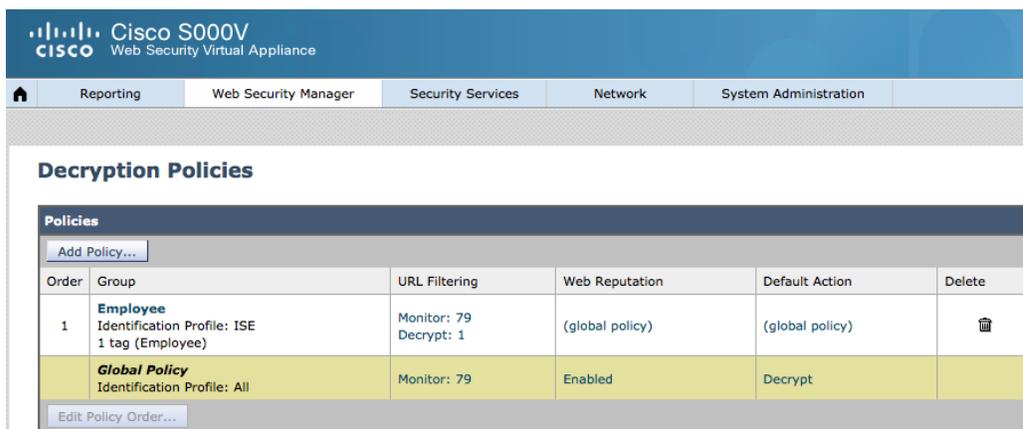


ステップ 12 [送信 (Submit)] > [変更を確定 (Commit Changes)] を 2 回クリックします。

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)	
---	--	-----------------	-------------------------	--	-----------------	-----------------	--

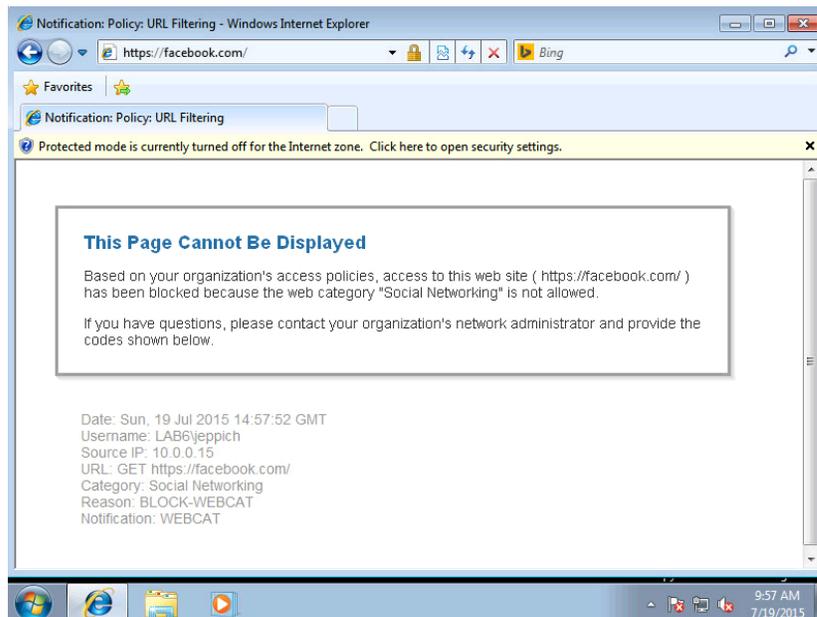
ステップ 14 従業員に Facebook の復号化ポリシーが作成されます。「アプリケーションの復号化」を参照してください。



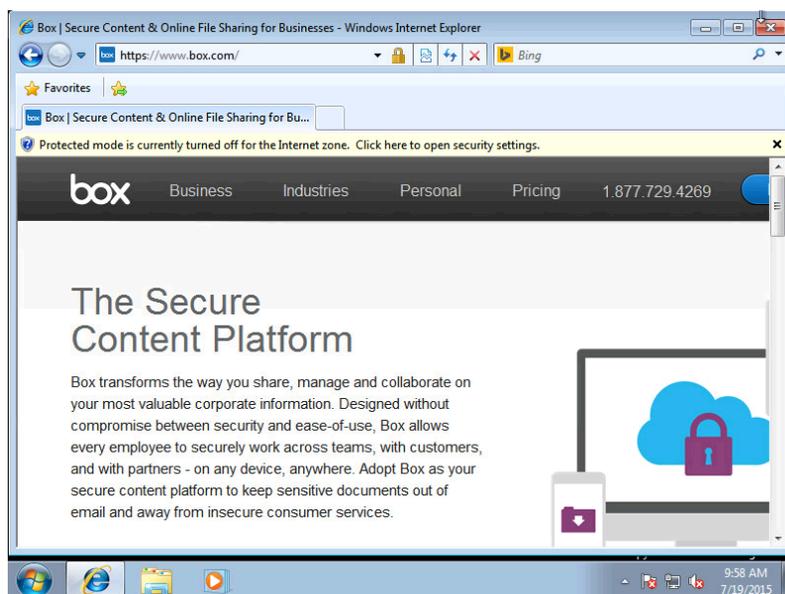
テスト

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。

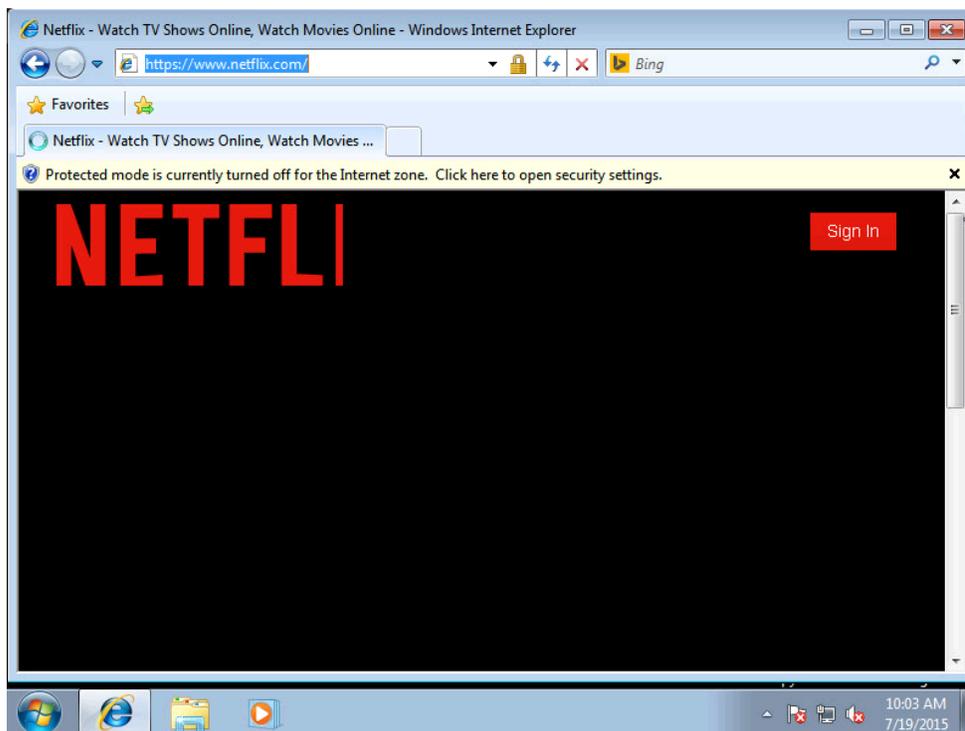
ステップ 1 従業員は、802.1X 経由で正常に認証され、従業員セキュリティグループ タグが付与され、Facebook アクセスは拒否されます。



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

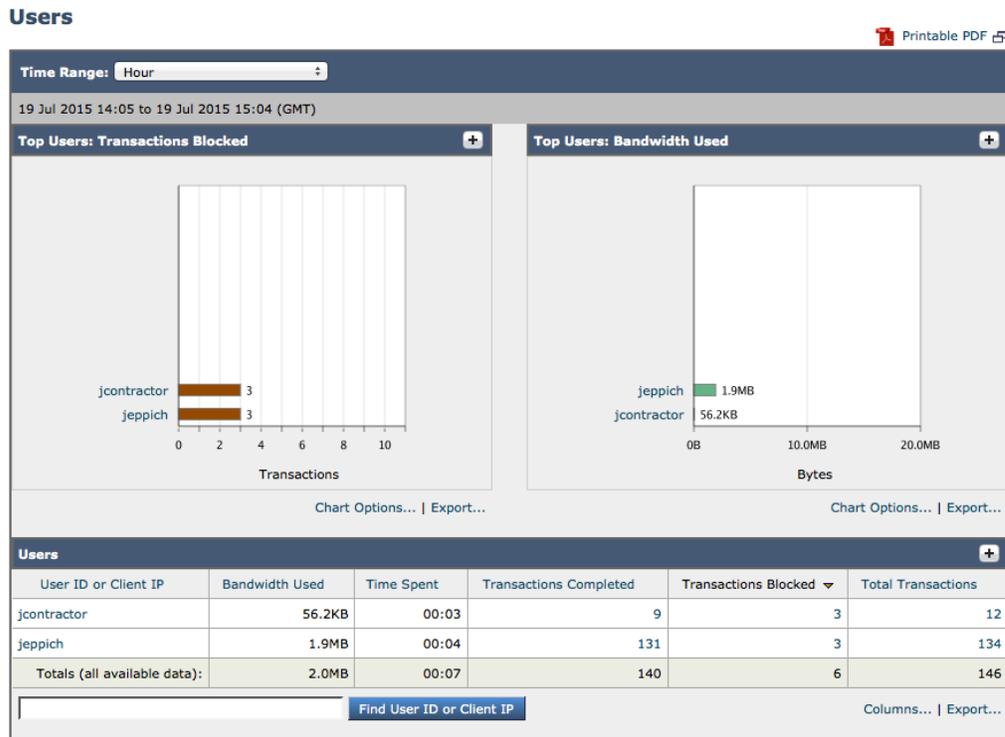
```
- CACHE - Show the ISE cache or check an IP address.  
- SGTS - Show the ISE Secure Group Tag (SGT) table.  
[]> CACHE
```

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

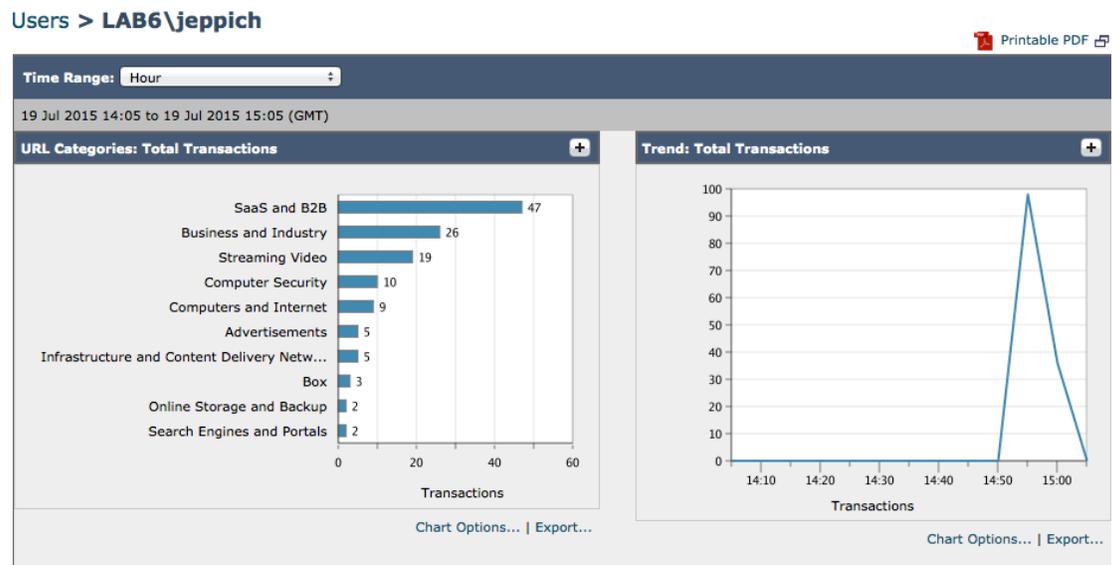
IP	Name	SGT#
10.0.0.15	LAB6\jeppich	4
10.0.0.98	00:0C:29:35:48:2A	0
169.254.57.162	00:0C:29:C7:16:48	0
10.0.0.22	00:0C:29:CA:A3:8F	0
10.0.0.33	68:05:CA:12:7C:78	0
10.0.0.21	jcontractor	6
10.0.0.3	18:E7:28:2E:29:CC	0

```
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。

Destination	
URL:	<input type="text" value="www.netflix.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:	<input type="text" value="Identity Services Engine (ISE)"/>
Client IP Address:	<input type="text" value="10.0.0.15"/>
User Name:	<input type="text"/>
<input type="button" value="Find Policy Match"/>	

Results	
User Information	
User Name: None Authentication Realm Group Membership: None Secure Group Tag Membership: Employee User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:39.0) Gecko/20100101 Firefox/39.0	
URL Check	
WBRS Score: 6.9 URL Category: Streaming Video Scanner "AVC" Verdict (Request): Netflix (Media) Scanner "Webroot" Verdict (Request): Unknown MIME-Type: text/html;charset=UTF-8 Object Size: 0 bytes	
Policy Match	
Cisco Data Security policy: None Decryption policy: None Routing policy: Global Routing Policy Identification Profile: ISE Access policy: Employee	

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。

Destination	
URL:	<input type="text" value="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:	<input type="text" value="Identity Services Engine (ISE)"/>
Client IP Address:	<input type="text" value="10.0.0.15"/>
User Name:	<input type="text"/>
<input type="button" value="Find Policy Match"/>	

Results

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

URL Check

WBR Score: 5.3
 URL Category: Online Storage and Backup
 Scanner "AVC" Verdict (Request): Box.net (File Sharing)
 Custom URL Category: Box
 Scanner "Webroot" Verdict (Request): Unknown
 MIME-Type: text/html; charset=iso-8859-1
 Object Size: 228 bytes
 Scanner "AVC" Verdict (Response): Box.net (File Sharing)
 Adaptive Scanning Verdict (Response): Unknown

Policy Match

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

Final Result

Request completed
 Details: Request monitored based on custom URL category

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。

Destination

URL:

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:

Client IP Address:

User Name:

▶ Advanced Cancel

Results

User Information

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

URL Check

WBR Score: 5.5
 URL Category: Social Networking
 Scanner "AVC" Verdict (Request): Facebook General (Facebook)

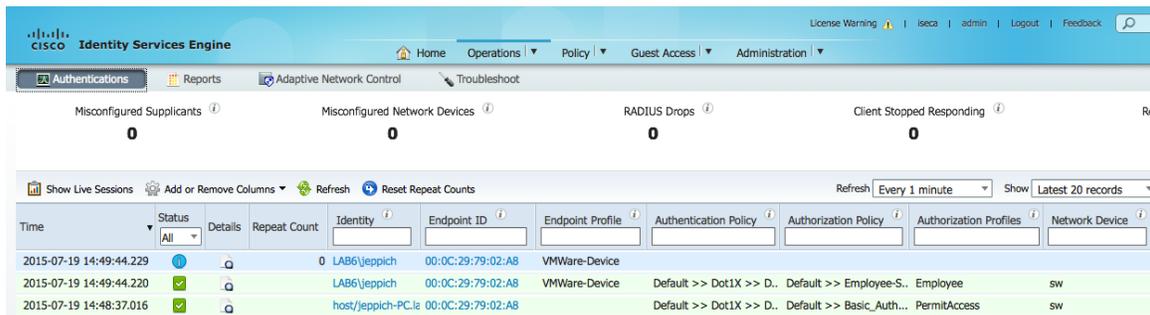
Policy Match

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

Final Result

Request blocked
 Details: Request blocked based on URL category
 Trace session complete

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。

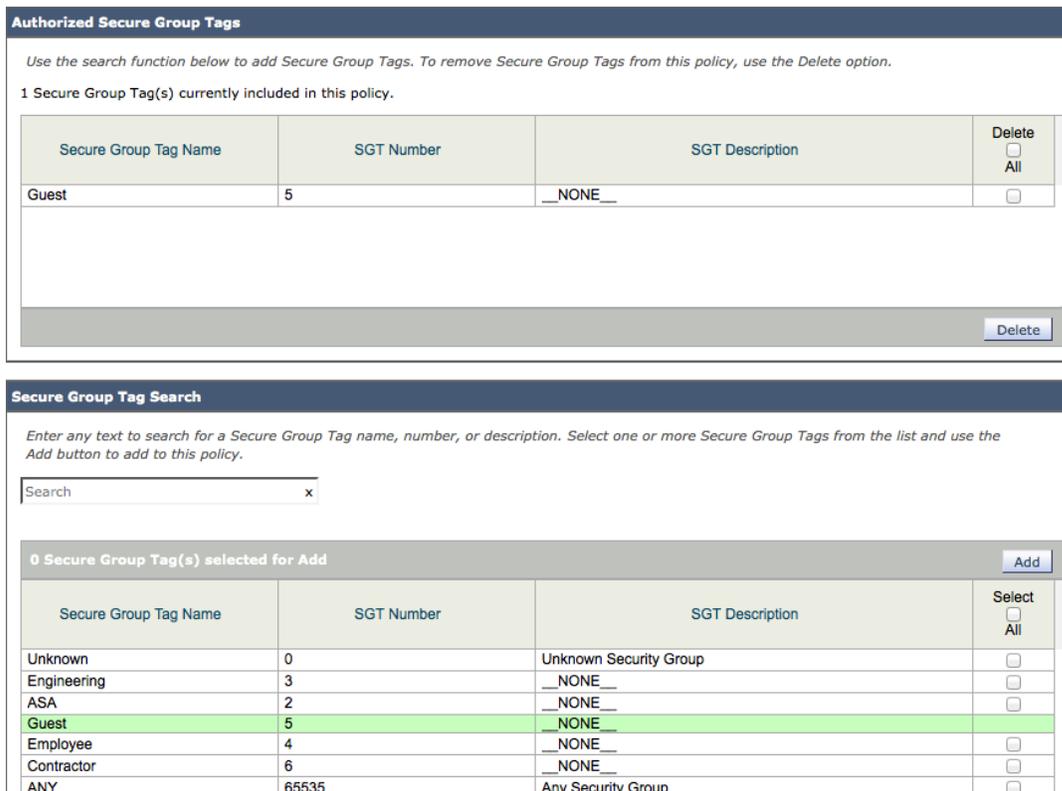


ゲスト

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。

Policy Settings

Enable Policy

Policy Name: ?

Guest
(e.g. my IT policy)

Description:

Insert Above Policy:

3 (Global Policy) ▾

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Select One or More Identification Profiles ▾
Add Identification Profile

Identification Profile	Authorized Users and Groups	
ISE ▾	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users ? ISE Secure Group Tags: Guest Users: No users entered	<input type="checkbox"/> Guests (users failing authentication)

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	✓				-	-

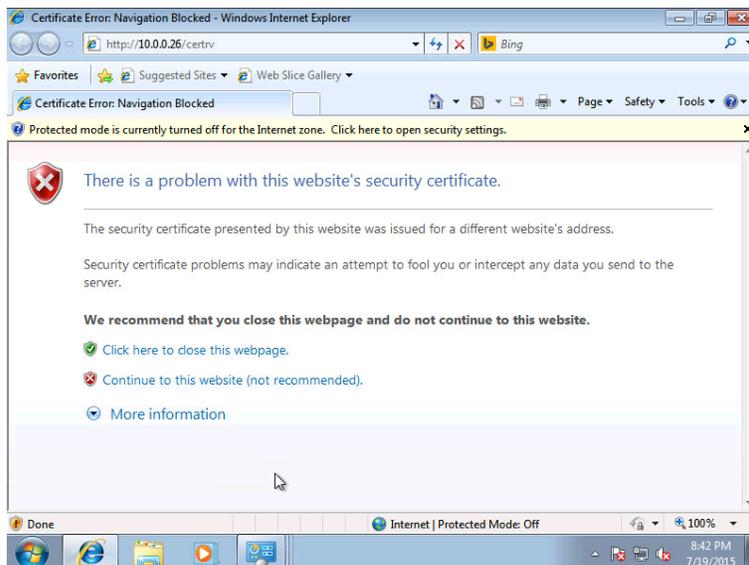
ステップ 7 Box の URL ポリシーを [モニタリング (Monitoring)] または [許可 (Allow)] に設定します。
ステップ 8 [送信 (Submit)] をクリックし、[変更を確定 (Commit Changes)] を 2 回クリックします。

テスト

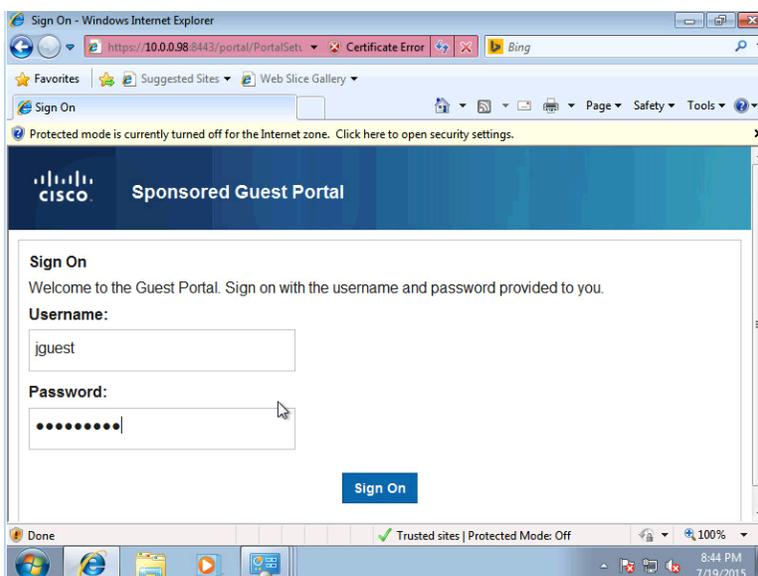
ゲスト ユーザがブラウザを開いて社内 Web サーバにアクセスすると、スポンサー ゲスト ポータルにリダイレクトされます。

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。

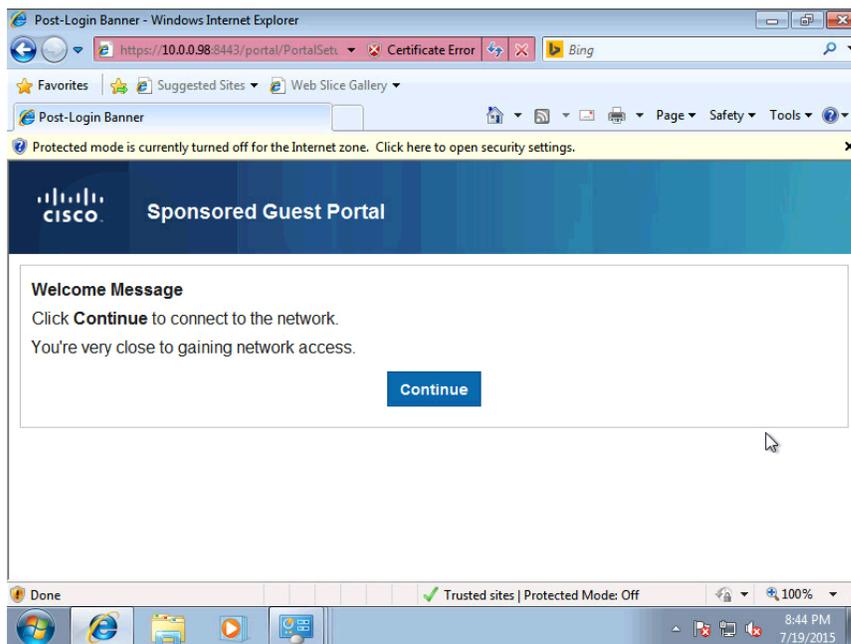
ステップ 1 ゲスト ユーザは、<http://10.0.0.26/certsrv> にアクセスすると ISE にリダイレクトされます。



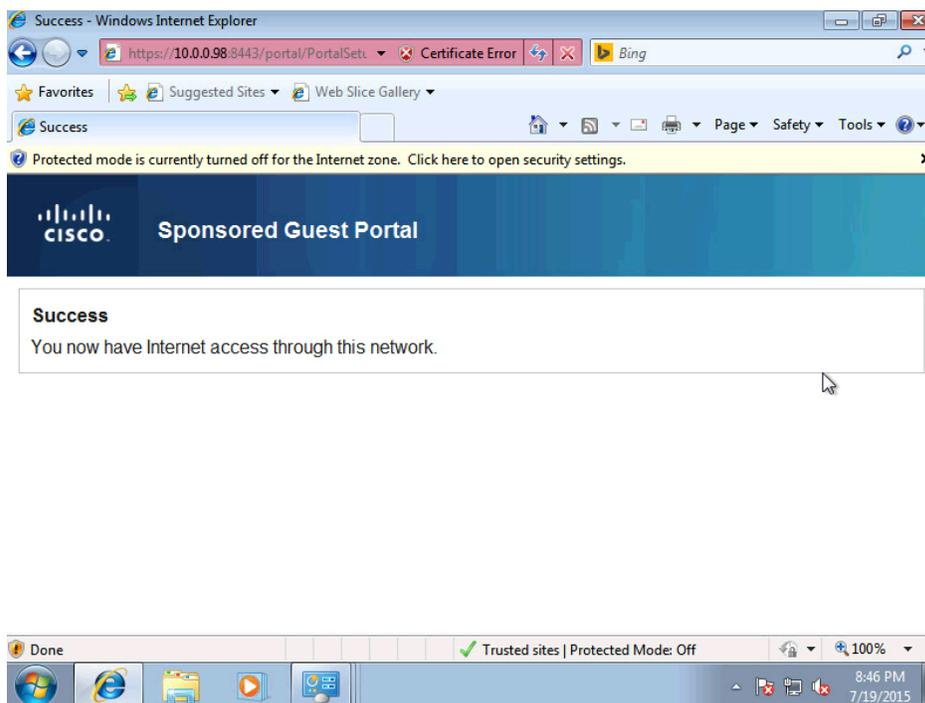
ステップ 2 ゲスト ユーザはクレデンシャルを入力してからサインオンします。



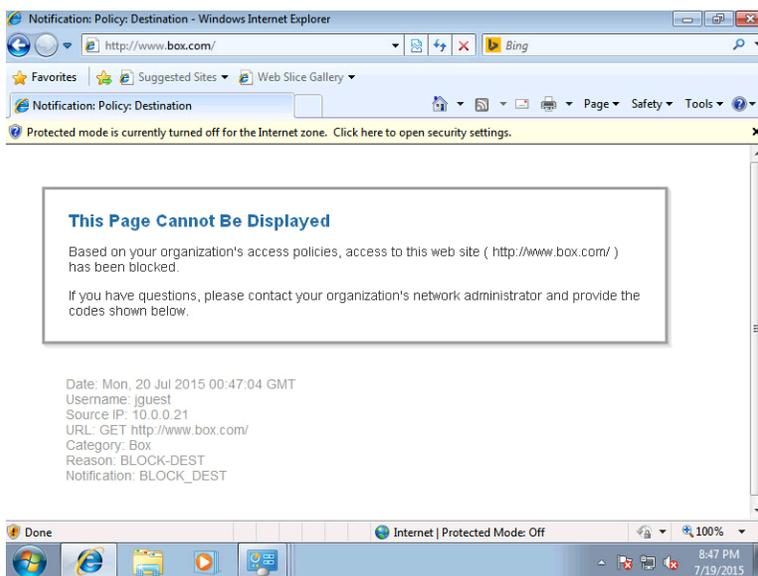
ステップ 3 [続行 (Continue)] を選択します



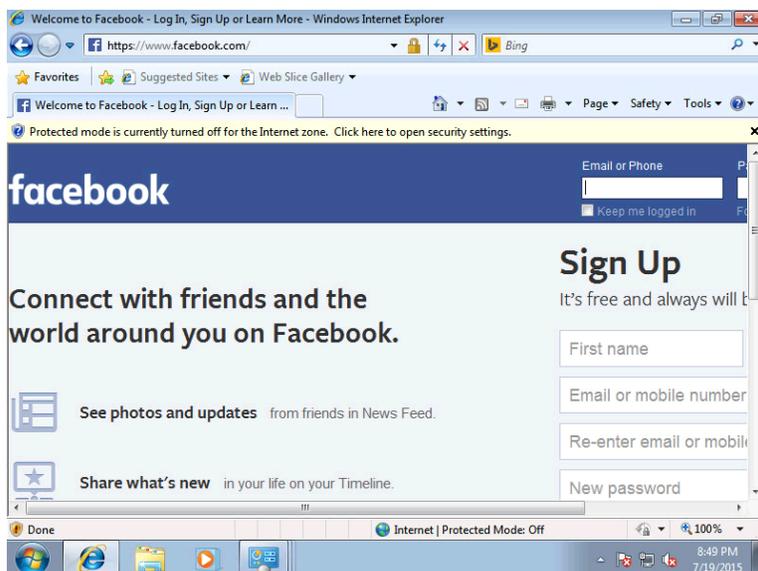
ステップ 4 Jguest に正常にログインしました。



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。

```

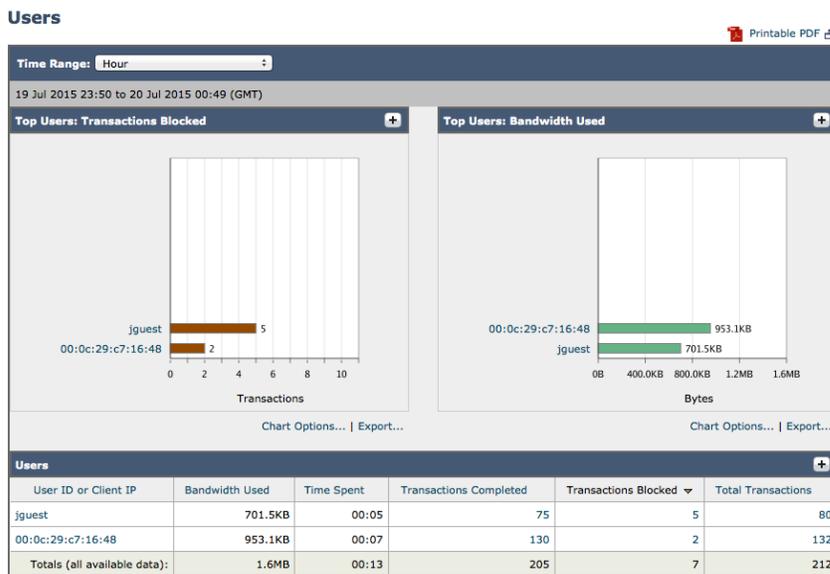
- CACHE - Show the ISE cache or check an IP address.
- SGTS - Show the ISE Secure Group Tag (SGT) table.
[ ]> CACHE

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

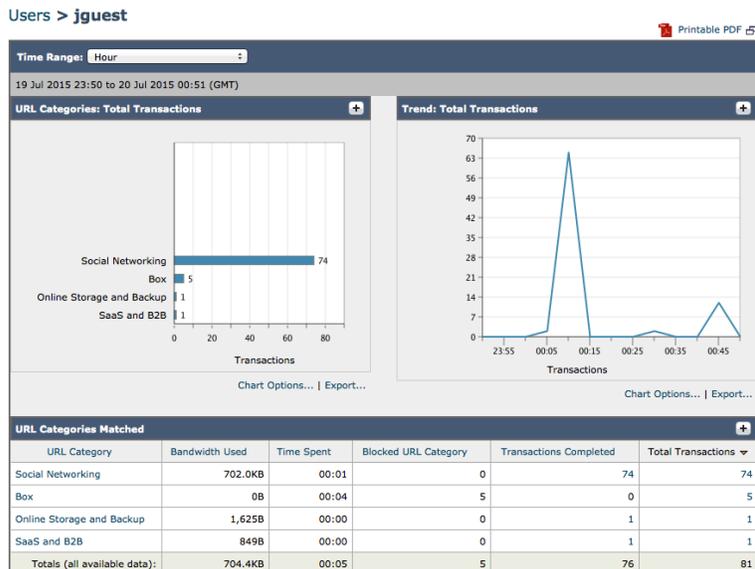
IP                Name                               SGT#
10.0.0.15         LAB6\jeppich                       4
10.0.0.98         00:0C:29:35:48:2A                 0
169.254.57.162   00:0C:29:C7:16:48                 0
10.0.0.22        00:0C:29:CA:A3:BF                 0
10.0.0.33        68:05:CA:12:7C:78                 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。

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
akamaihd.net	123.6KB	00:00	34	0	34
box.com	1,625B	00:03	1	4	5
facebook.com	43.0KB	00:01	5	0	5
snpengage.com	849B	00:00	1	0	1

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。

Application	Application Type	Bandwidth Used	Transactions Completed	Other Blocked Transactions	Total Transactions
Facebook General	Facebook	702.0KB	74	0	74
Box.net	File Sharing	1,625B	1	0	1
Totals (all available data):	--	703.6KB	75	0	75

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。

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:	
<p>Advanced</p> <p style="text-align: right;">Find Policy Match</p>	
Results	
User Information	
User Name: None Authentication Realm Group Membership: None Secure Group Tag Membership: Guest 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: Guest	
Final Result	
Request blocked	
Details: Request blocked based on custom URL category Trace session complete	

ステップ 13 Facebook のポリシー トレースも確認します。

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:	
<p>Advanced</p> <p style="text-align: right;">Find Policy Match</p>	
Results	
User Information	
User Name: None Authentication Realm Group Membership: None Secure Group Tag Membership: Guest User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:39.0) Gecko/20100101 Firefox/39.0	
URL Check	
WBRB 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: Guest	
Final Result	
Request completed	
Details: Transaction permitted Trace session complete	

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。

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
2015-07-20 00:45:55.580			0	jguest	00:0C:29:C7:16:48	Windows7-Worksta...				10.0.0.21
2015-07-20 00:45:55.567				jguest	00:0C:29:C7:16:48	Windows7-Worksta...	Default >> MAB	Default >> Guest-SGT...	Guest	10.0.0.21
2015-07-20 00:45:55.544				jguest	00:0C:29:C7:16:48					10.0.0.21
2015-07-20 00:44:50.360				jguest	00:0C:29:C7:16:48					10.0.0.21
2015-07-20 00:40:17.553				#ACSACL#-JP-rec						
2015-07-20 00:40:17.541				00:0C:29:C7:16:4	00:0C:29:C7:16:48		Default >> MAB >> Def.	Default >> Redirect	Redirect	10.0.0.21

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。

Authorized Secure Group Tags

Use the search function below to add Secure Group Tags. To remove Secure Group Tags from this policy, use the Delete option.

1 Secure Group Tag(s) currently included in this policy.

Secure Group Tag Name	SGT Number	SGT Description	Delete
Contractor	6	__NONE__	<input type="checkbox"/>

[Delete](#)

Secure Group Tag Search

Enter any text to search for a Secure Group Tag name, number, or description. Select one or more Secure Group Tags from the list and use the Add button to add to this policy.

Search

0 Secure Group Tag(s) selected for Add [Add](#)

Secure Group Tag Name	SGT Number	SGT Description	Select
Unknown	0	Unknown Security Group	<input type="checkbox"/>
Engineering	3	__NONE__	<input type="checkbox"/>
ASA	2	__NONE__	<input type="checkbox"/>
Guest	5	__NONE__	<input type="checkbox"/>
Employee	4	__NONE__	<input type="checkbox"/>
Contractor	6	__NONE__	<input checked="" type="checkbox"/>
ANY	65535	Any Security Group	<input type="checkbox"/>

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。

The screenshot shows two configuration panels. The top panel, 'Policy Settings', has 'Enable Policy' checked, 'Policy Name' set to 'Contractor', and 'Insert Above Policy' set to '1 (Employee)'. The bottom panel, 'Policy Member Definition', shows 'Identification Profiles and Users' with 'ISE' selected. Under 'Authorized Users and Groups', 'Selected Groups and Users' is selected, with 'ISE Secure Group Tags' set to 'Contractor' and 'Users' set to 'No users entered'.

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.

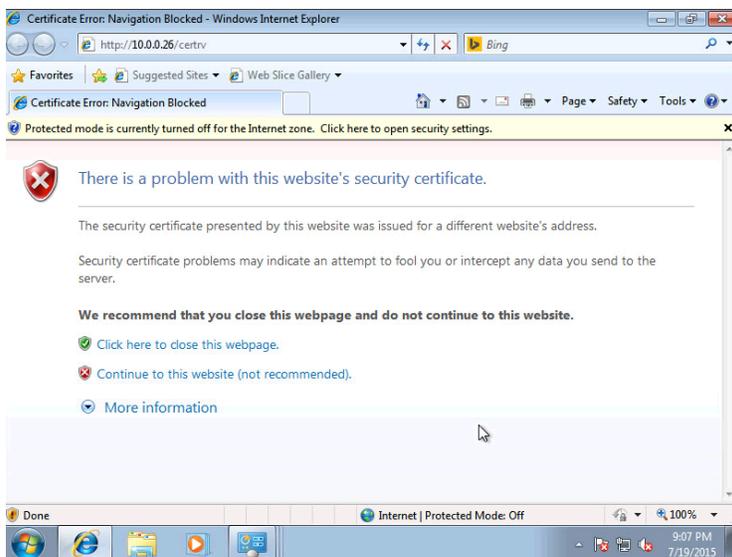
Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn	Quota-Based	Time-Based
Education	<input checked="" type="checkbox"/>					
Entertainment	<input checked="" type="checkbox"/>					
Extreme	<input checked="" type="checkbox"/>					
Fashion	<input checked="" type="checkbox"/>					
File Transfer Services		<input checked="" type="checkbox"/>				
Filter Avoidance	<input checked="" type="checkbox"/>					

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。

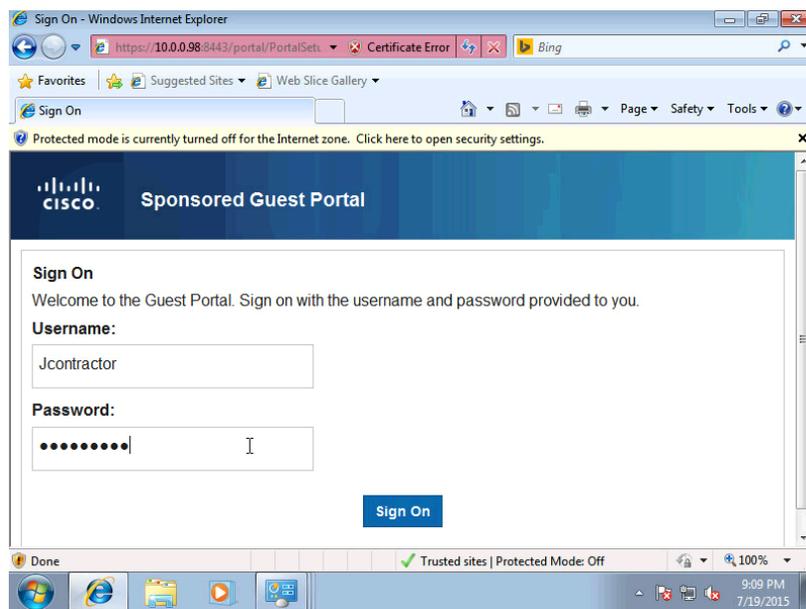
テスト

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。

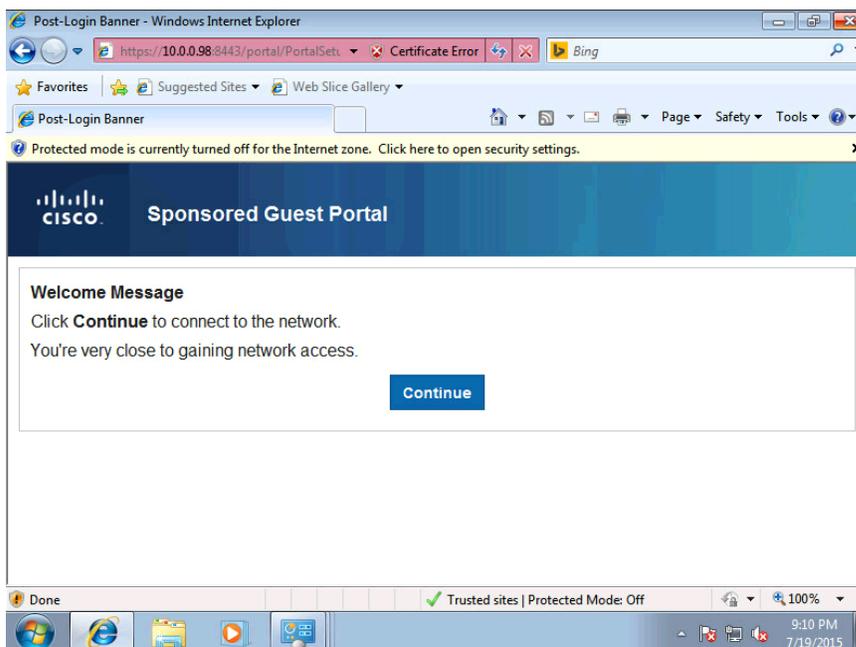
注: 証明書のエラー メッセージは、URL がサーバの IP アドレスであったことが原因です。FQDN を使用していれば、このエラー メッセージは表示されません。



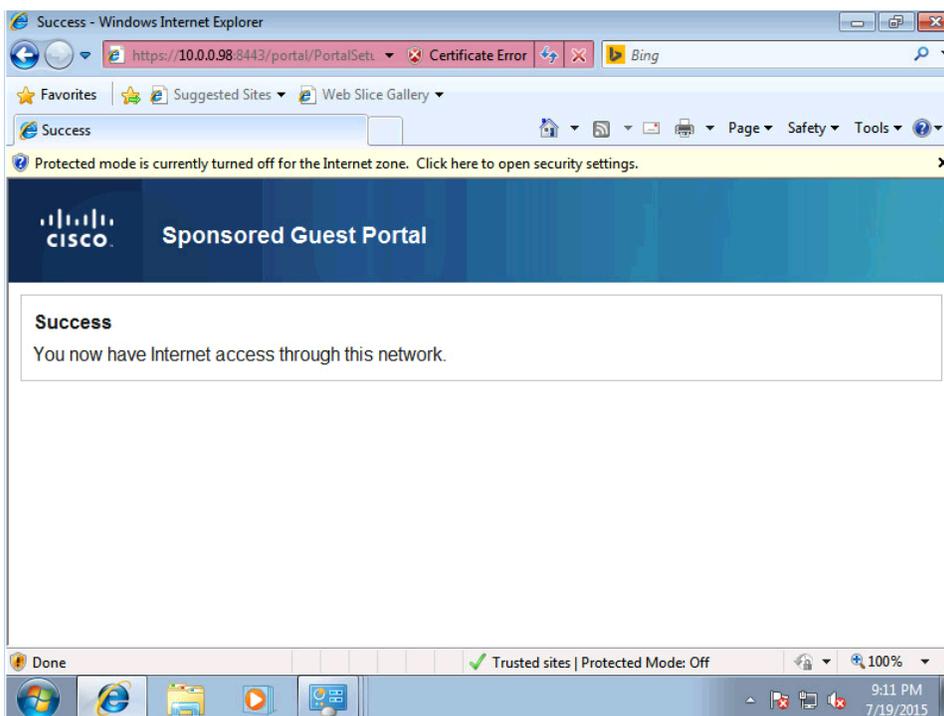
ステップ 2 請負業者が ISE の内部ユーザとして定義していたクレデンシャルを入力します。



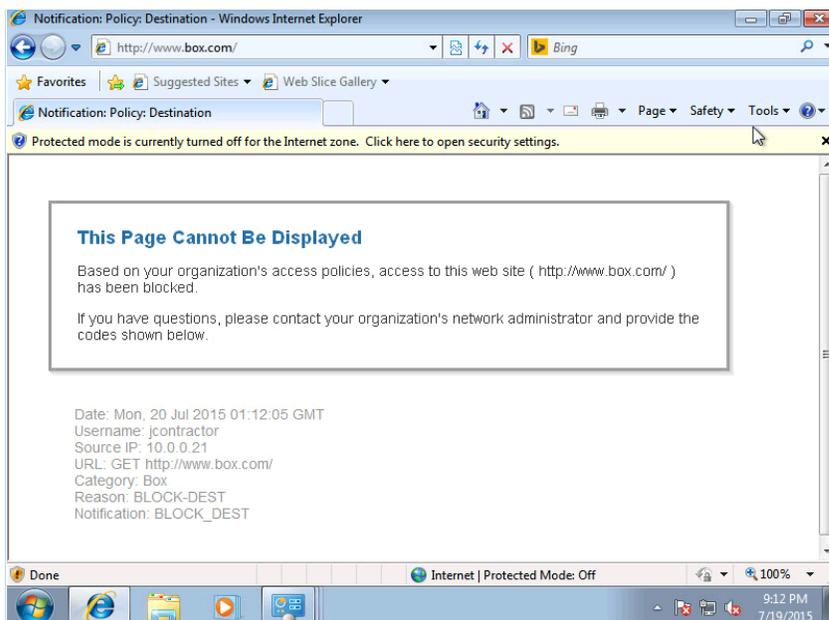
ステップ 3 請負業者が [続行 (Continue)] を選択します。



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。



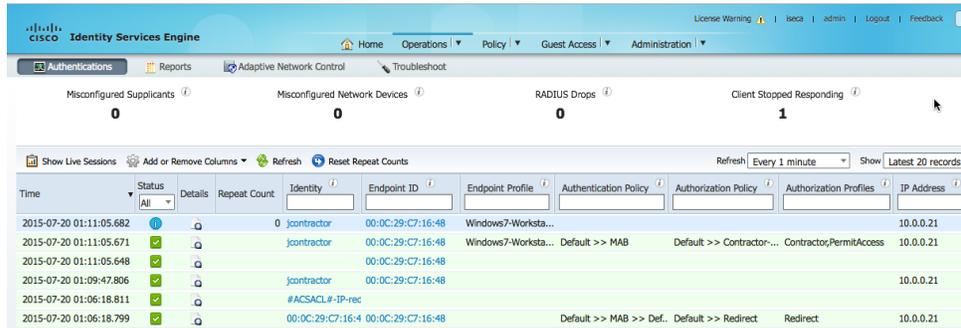
ステップ 5 請負業者が Box.com にアクセスし、拒否されます。



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

```

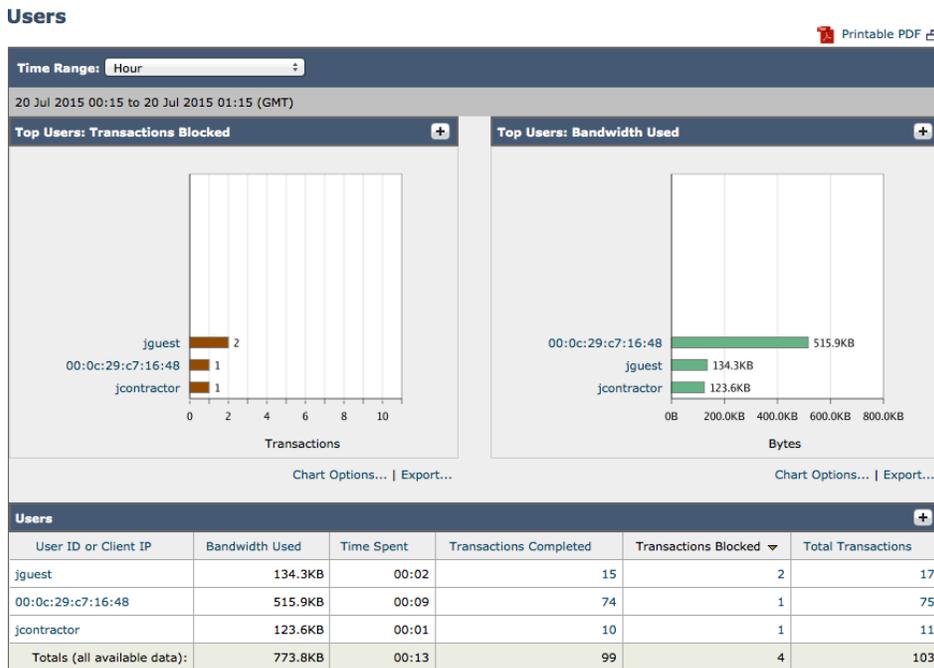
jpeppich — ssh — 80x24
- CACHE - Show the ISE cache or check an IP address.
- SGTS - Show the ISE Secure Group Tag (SGT) table.
[> CACHE

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

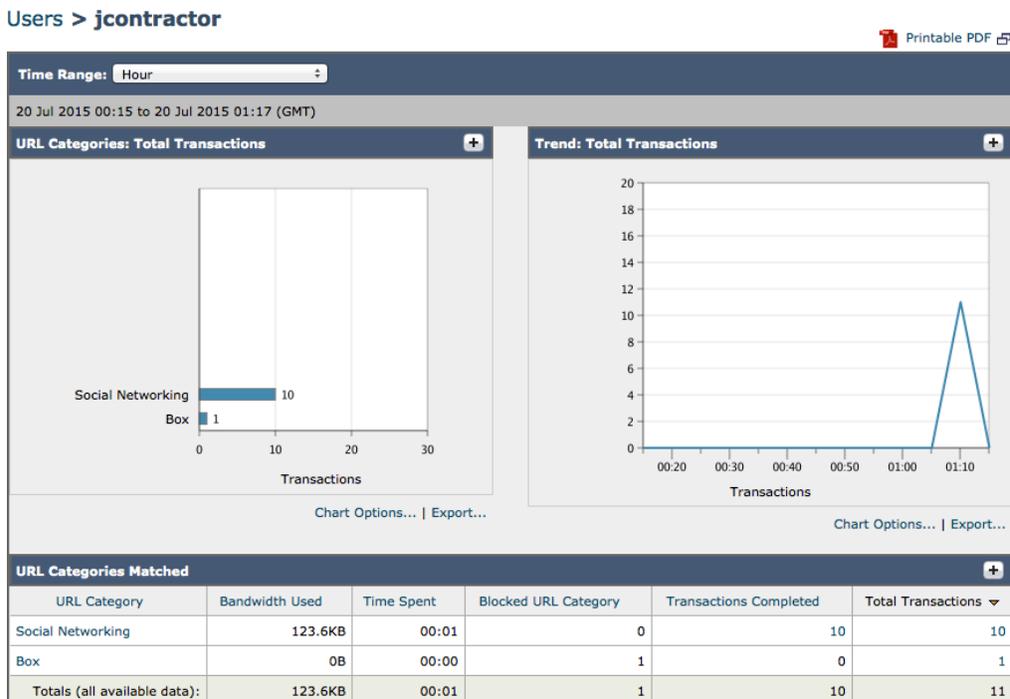
IP           Name                               SGT#
10.0.0.15    LAB6\jpeppich                       4
10.0.0.98    00:0C:29:35:48:2A                    0
169.254.57.162 00:0C:29:C7:16:48                    0
10.0.0.22    00:0C:29:CA:A3:8F                    0
10.0.0.33    68:05:CA:12:7C:78                    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 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

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):		--	10	1	11

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:

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:
Client IP Address:
User Name:

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:

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:
Client IP Address:
User Name:

Advanced

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
WBR 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ことができます。

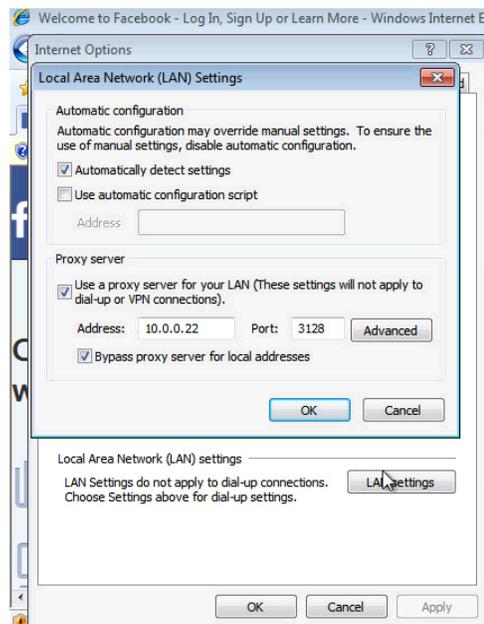
WSA 仮想での CPU RAM 使用率が 100%

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

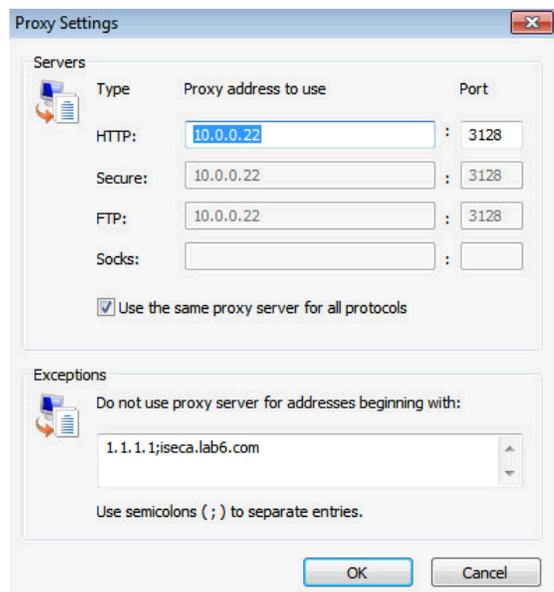
Internet Explorer のプロキシ設定

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