

How To Integrate Cisco WSA using ISE and TrustSec through pxGrid

Table of Contents

About this Document	4
Solution Introduction- WSA with TrustSec, ISE and pxGrid	6
Cisco Web Security Appliance (WSA).....	6
Cisco TrustSec.....	6
Cisco Identity Service Engine (ISE)	7
Cisco pxGrid.....	7
Dynamic Security Group Tag Assignment Using ISE	10
Cisco WSA Installation	11
WSA System Wizard.....	11
WSA and ISE pxGrid Node Configuration using CA-Signed Certificates	16
Adding CA Root Certificate to WSA Certificate Trust Store.....	16
Add CA Root Certificate to WSA Trusted Store	16
Configuring CA-Signed WSA Client Certificate	17
Creating WSA private key and CSR request	17
Creating WSA private key and CSR request from WSA (alternative)	18
ISE Service configuration on WSA.....	21
Uploading primary pxGrid node certificate	22
Uploading secondary pxGrid node certificate.....	22
Uploading Primary Monitoring node certificate.....	23
Uploading Secondary Monitoring node certificate	23
Uploading the WSA certificate and private key	23
Running Test.....	24
Verifying WSA as a registered pxGrid client.....	26
WSA Policies	27
Create identification Profile on WSA	27
Create WSA Access Policy	28
Create WSA Decryption Application Policy	31
Application Decryption	33
Obtaining root public/private key pair	35
Client Testing	37
User Reports	39
WSA and ISE pxGrid node Configuration using Self-Signed Certificates in an ISE Stand-Alone environment ...	43
Create Self-Signed Certificate for the WSA.....	43

ISE Self-Signed Identity Certificate & ISE pxGrid Configuration	44
WSA and ISE pxGrid node Configuration	46
Client testing	51
Use Case Scenarios.....	53
ISE Internal User and Default Sponsor Guest Portal	53
ISE Dynamic Tags, Authorization Profiles, and Authorization Policies.....	55
Dynamic Tags.....	55
Authorization Profile and Downloadable ACL's for CWA	55
Authorization Policy	57
Employee	58
Identification Profile and Web Access Policy	58
Testing.....	60
Guest	67
Identification Profile and Web Access Policy	67
Testing.....	69
Contractor	75
Identification Profile and Web Access Policy	75
Testing.....	77
Troubleshooting.....	84
Restful ISE Node Failures	84
ISE pxGrid client Connectivity Issues.....	84
CPU RAM utilization 100% on WSA Virtual	84
Appendices.....	85
Internet Explorer Proxy Settings.....	85
Switch and redirect ACL Settings for CWA	86
Redirect ACL	86
CWA Switch Settings.....	86
References.....	87

About this Document

This document is for partners, customers, Cisco engineers who are deploying Cisco Web Security Appliance (WSA 9.0.0-324 or higher) with Cisco Identity Service Engine (ISE 1.3 or higher) and leveraging Cisco Platform Exchange Grid (pxGrid).

The readers of this document should be familiar with the WSA, TrustSec, ISE and pxGrid.

This document covers the WSA and ISE pxGrid node integration in a Certificate Authority (CA) signed environment. It is assumed that the ISE pxGrid nodes are deployed in a distributed ISE deployment as separate nodes, one being the primary and the other being the secondary.

If you are not familiar with deploying pxGrid in a Distributed ISE environment, please see:

http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf

WSA and ISE pxGrid node integration includes:

- WSA private key and certificate signing request (CSR) generation using openssl
- Uploading of ISE pxGrid node and ISE monitoring node (MNT) certificates
- Uploading CA root certificate into WSA trusted store
- Creation of web access policies and application decryption policies denying end-users assigned an engineering security group tag from Facebook access.

It is assumed that ISE pxGrid nodes have already been configured in a distributed ISE environment using signed certificates from the same CA authority that will sign the WSA client certificates.

A Security Group Tag (SGT) representing the engineering group will be created and assigned to an authorization policy allowing successfully authenticated users who belong to the Windows /Domain/Users group.

Security group tags provide an easier way to implement corporate security policies.

SGT's are a convenient, flexible way to implement corporate security policies overcoming ACL and VLAN restrictions.

The following use cases are covered:

- An employee SGT will be assigned to end-users belonging to the Windows /Domain/Users Group and allowed Box.com access and denied Facebook access with Netflix bandwidth restrictions
- A guest SGT will be assigned to ISE internal users belonging to a Guest Identity group and allowed Facebook access and denied Box.com access.
- A contractor SGT will be assigned to ISE internal users belonging to a Contractor Identity group and allowed Facebook access and denied Box access.

These guest and contractor use case will rely on ISE Central Web Authentication (CWA). The reader should have the appropriate commands on the switch to allow for this operation. These are also listed in the Appendices.

It is also assumed that the switches support RADIUS Change of Authorization (CoA) and Central Web Authentication (CWA)

Please check with Cisco Switch compatibility matrix http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/compatibility/ise_sdt.html to ensure that the switch is supported.

Solution Introduction- WSA with TrustSec, ISE and pxGrid

The Cisco Web Security Appliance (WSA) provides secure web access by enforcing an organization's web security policies from users and groups from a variety of different authentication stores such as Microsoft Active Directory (AD), Novell's eDirectory and LDAP servers.

The WSA authenticates users or groups based on the creation of authentication realms, assigning them to the identification profile, and then to associated WSA web access policies. End-users are either prompted for their credentials or transparently redirected to the WSA for authentication. The Cisco Context Directory Agent (CDA) is used for transparent user redirection. The Cisco Context Directory Agent (CDA) is installed on a Microsoft Active Directory (AD) domain and defined in the WSA authentication realm settings. The WSA will query the context directory agent for the IP-username mapping in AD, and obtain the username. The end-user is never prompted for their credentials, resulting in single-sign on (SSO) for web transactions. The IP-Username information is cached on the WSA and will query the CDA for updated or new user authentication information.

Cisco TrustSec can help streamline the WSA SSO process by assigning a SGT to successfully authenticated 802.1X end-users or non-802.1X authenticated devices. This same SGT can be applied to the WSA web access policy(s) enhancing the WSA identity policy(s).

For example, a Security Group Tag of engineering is defined in the Cisco Identity Service Engine (ISE). This will represent an organization's web security access policy for its engineering department. This SGT represents the end-users Engineering AD group, device type, posture compliant status that represents an organization's web security compliance policy.

Once the end-user successfully authenticates via 802.1X through ISE and meets these authorization conditions, they will be assigned the Security Group Tag. This SGT can then applied the WSA's identification policy and associated web security policy.

Centralized user and device management is provided from the ISE management console. SSO is provided from the successful 802.1X end-user authentications in ISE. Non-802.1X devices such as printers, cameras, etc. are profiled and provided or non-provided network access pending ISE authorization policies. These can also be assigned a Security Group Tag and tied to a WSA web access policy as well.

It is crucial that the WSA knows the identity of the originator of the web transaction. The SGT provides this information and also includes additional ISE contextual information.

Cisco Platform Exchange Grid (pxGrid) provides the framework for the WSA to consume this contextual information from ISE.

Cisco Web Security Appliance (WSA)

The Security Web Security Appliance (WSA) provides advanced malware protection, application visibility controls, and acceptable-usage policies for securing corporate web traffic. In this document, the identity profiles and web security policies will be tagged and enforced using the SGT to differentiate between the different levels of web access.

Cisco TrustSec

Security Group Tags (SGT) are part of the Cisco TrustSec Solution. These Security Group Tags are defined in ISE and applied at ingress (inbound to the network). These Security Group Tags are defined in ISE and can represent a grouping of users, endpoint devices, line of business, etc. These tags can then be applied to a network access policy and used by network devices to make forwarding decisions and share access control policies across the network

infrastructure. A SGT is a unique 16-bit security group number assigned to a security group. For ease of understanding a security group can also have a descriptive name.

These security group tags are defined and implemented as authorization profiles in an ISE authorization policy consisting of condition rules defining an organizations security policy.

These security group tags can make an organization's security policy uniform or global across the network.

In this document, an authorization policy will be created such that all successfully authenticated end-users belonging to the /users/domain Windows group receive an engineering security group tag mapping them to the SGT. The security group tag will be mapped to the end-user's device and used to establish restricted WSA access policies denying end-users assigned and Engineering SGT from accessing Facebook.

Cisco Identity Service Engine (ISE)

Identity Service Engine (ISE) is a security policy management and identity access management platform solution. ISE provides centralized management by defining/issuing/enforcing 802.1X authentications, guest management policies, posture, client provisioning and TrustSec policies. The ISE session directory provides contextual information with regards to authenticated 802.1X and non-802.1X devices such as username, IP address, device type, SGT, posture status, MAC address which is used by pxGrid to publish this information to registered pxGrid clients.

In addition ISE simplifies access control and security compliance for wired, wireless, and VPN connectivity and supports corporate security policy initiatives, such as BYOD.

Cisco pxGrid

Cisco Platform Exchange Grid (pxGrid) enables multivendor, cross platform network system collaboration among parts of the IT infrastructure such as security monitoring and detection system, network policy platforms, asset and virtually configuration management, identity and access management platforms, and virtually and other IT operations platform.

When business or operational needs arise, Cisco's Security Solutions such as WSA and ecosystem partners can use pxGrid to exchange contextual information via a publish/subscribe method.

ISE publishes topics of information exposing ISE contextual information using session attributes, the pxGrid clients, such as the WSA will subscribe to the ISE published sessions:

Topics include:

- TrustsecMetadata information exposes the security group tag number and description

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

- EndpointProfileMetadata, providing ISE endpoint policy information such as changes/modifications to the ISE profiling policy

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

- EndpointProtection Service Capability exposes the Adaptive Network Control (ANC) mitigation actions that are available to pxGrid clients that can take mitigation actions such as quarantining an IP/unquaranting by MAC address of an authenticated endpoint.
- SessionDirectory exposes the authenticated use session attribute information such as the username and device information

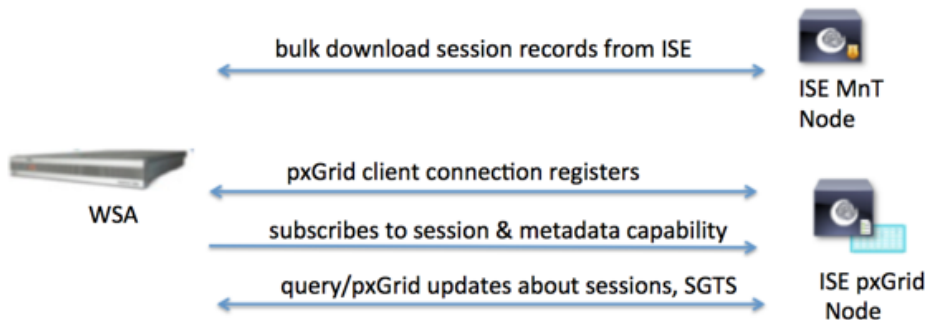
```
session (ip=192.168.1.14, Audit Session Id=0A0301030000001E00FEBAD7, User Name=jsmith, Domain=lab4.com, Calling station id=00:0C:29:77:A8:C7, Session state= STARTED, Epsstatus=null, Security Group=Engineering, Endpoint Profile=Microsoft-Workstation, NAS IP=192.168.1.2, NAS Port=GigabitEthernet1/0/9, 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 exposes ISE user and group information, also if the group was profiled.

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

Cisco security solutions and ecosystem partners will register as a pxGrid client to the ISE pxGrid node and subscribe to these topics in providing more contextual information around the event, such as user identity information, device operating system, security group tags (SGT) These pxGrid clients can also download bulk session records.

As in the case of the WSA, the Session and SGT bulk downloads occur only on the WSA ISE service start or restart (i.e. due to WSA ISE config changes), and is downloaded from the ISE MNT node via the ISE RESTful API. End-users are identified based on their session information, IP address and associated IP-session mappings obtained from ISE. The SGT IP-session mapping are cached locally. If the WSA finds the IP address of the request it will do a lookup locally for the IP-SGT mapping and associate the transaction with the corresponding SGT, else will make an on-demand query the ISE pxGrid node for the SGT for new IP address based on its subscription to the Session Directory and TrustsecMetadata topics.



Below is the WSA registered as the ISE pxGrid and subscribed to the published information topics.

License Warning | ise14ppan | admin | Logout | Feedback

Identity Services Engine | Home | Operations | Policy | Guest Access | Administration | Setup Assistant

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

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

Clients | Live Log

Enable
 Disable
 Approve
 Group
 Decline
 Delete
 Refresh
 Total Pending Approval(0)
 1 - 7 of 7
 Show 25 per page
 Page 1 of 1

Client Name	Client Description	Capabilities	Status	Client Group	Log
<input type="checkbox"/> ▶ ise-admin-ise14smnt		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
<input type="checkbox"/> ▶ ise-mnt-ise14smnt		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
<input type="checkbox"/> ▶ ise-admin-ise14pmnt		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
<input type="checkbox"/> ▶ ise-mnt-ise14pmnt		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
<input type="checkbox"/> ▶ ise-admin-ise14ppan		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
<input type="checkbox"/> ▼ 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

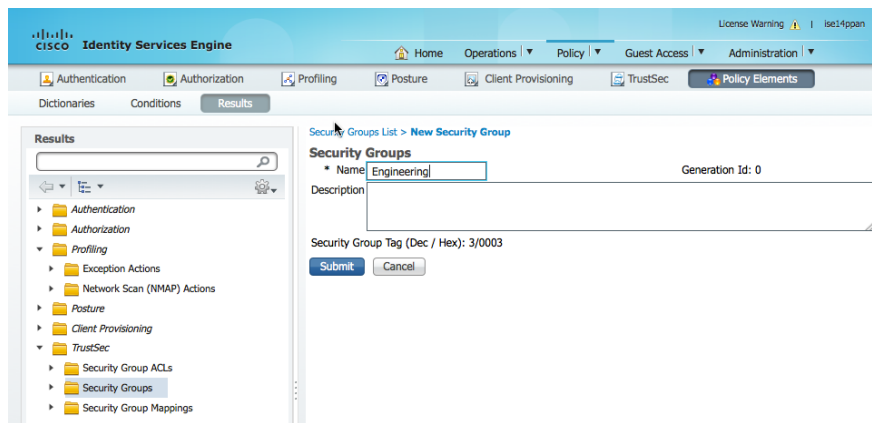
Capability Name	Capability Version	Messaging Role	Message Filter
<input type="radio"/> SessionDirectory	1.0	Sub	
<input type="radio"/> TrustSecMetaData	1.0	Sub	

<input type="checkbox"/> ▶ wsa.lab6.com-test_client	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session	View
---	----------------------------	----------------------------	---------	---------	----------------------

Dynamic Security Group Tag Assignment Using ISE

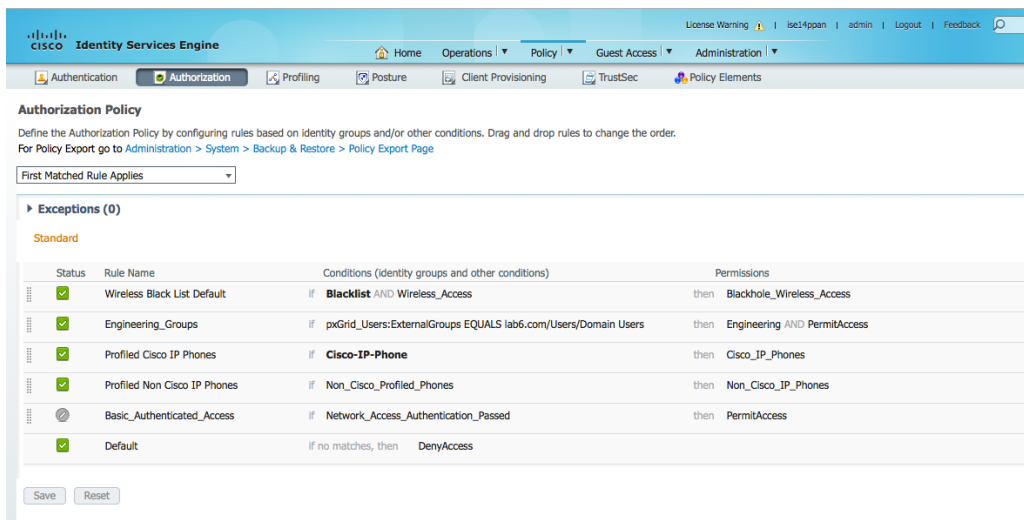
Organizations security policies can be defined based on these security group tags (SGT). This allows an organization to have uniform and global security policies across the network. Some other examples include: corporate end-users with recommended devices coming on the corporate network following corporate acceptable usage policies. This can be represented by a single SGT. If Cisco TrustSec is enabled on the organization switches, these security group tags can also be enforced on the network. Typically, security group tags of 2 are given to network devices such as switches, routers, firewalls.

Step 1 Create an engineering security group tag
Policy->Policy Elements->Trustsec->Security Groups->Add->Engineering->Submit



Step 2 Create Authorization Policy to assign SGT authorization profile to policy
Policy->Authorization-> and add the following authorization rule:

Rule Name: Engineering;
New Condition: External Groups>equals:pxGrid_Users
Authorization Profile(s): Engineering and Permit Access



Step 3 Select->Save

Cisco WSA Installation

This initial WSA setup will be performed using the WSA System Wizard. This includes the WSA network configuration, interfaces for management and traffic monitoring, changing default admin credentials.

WSA System Wizard

Step 1 System Administration->System Setup->System Setup Wizard, enter the management IP address of the WSA.

Note: In this document, 10.0.0.9 is used at the management IP address of the WSA

http://10.0.0.9:8080

Step 2 Enter the system information and DNS server information

Step 3 Select->Next

Step 4 If there are no other web proxies in your network, Select Next

Step 5 In this document, all M1 is used for management and also for handling all the traffic

Cisco S000V Web Security Virtual Appliance

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

Network Interfaces and Wiring

Note:
M1 : This interface is used to manage the appliance. Optionally, it may also handle web traffic.
P1 : This interface may be used to handle web traffic.

Interfaces

Ethernet Port:	M1 <input type="checkbox"/> Use M1 port for management only	P1 <i>(Optional if M1 used for data)</i>
IPv4 Address / Netmask:	<input type="text" value="10.0.0.9/24"/>	<input type="text"/>
<i>If multiple interfaces are configured, they must be assigned IP addresses on different subnets.</i>		
IPv6 Address / Netmask:	<input type="text"/>	<input type="text"/>
Hostname:	<input type="text" value="mgmt.wsa.lab6.com"/> <i>(e.g. wsa.example.com)</i>	<input type="text"/> <i>(e.g. data.example.com)</i>

Step 6 Click->Next

Step 7 In this document, Simplex TAP is set

Cisco S000V Web Security Virtual Appliance

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

Layer 4 Traffic Monitor Wiring

Note:
T1, T2 : These interfaces are used for the L4 Traffic Monitor.
 In addition, web proxy interfaces (M1, P1 or P2) may be used for L4TM blocking.

Interfaces

Wiring Type:

- Duplex TAP:
T1 (In/Out)
- Simplex TAP:
T1 (In) and T2 (Out)

< Prev | Cancel | Next >

Step 8 Click->Next

Step 9 Enter the network routes

The screenshot shows the 'IPv4 Routes for Management and Data Traffic (Interface M1: 10.0.0.9)' configuration page. It includes a progress bar with steps: 1. Start, 2. Network, 3. Security, 4. Review. The 'Default Gateway' is set to 10.0.0.1. Below is a 'Static Routes Table' with one entry: Name: Internal, Internal Network: 10.0.0.0/24, Internal Gateway: 10.0.0.1. There are 'Prev', 'Cancel', and 'Next' buttons at the bottom.

Step 10 In this document an explicit proxy will be used, Click->Next

Note: PC client proxy settings are listed in the Appendices

The screenshot shows the 'Transparent Connection Settings' configuration page. It includes a progress bar with steps: 1. Start, 2. Network, 3. Security, 4. Review. The 'Transparent Redirection Device' is set to 'Layer 4 Switch or No Device'. There are checkboxes for 'Enable standard service ID: 0 web_cache (port 80)' and 'Enable router security for this service'. There are input fields for 'Router Addresses', 'Password', and 'Confirm Password'. There are 'Prev', 'Cancel', and 'Next' buttons at the bottom.

Step 11 Enter admin name, password, email address

Cisco S000V Web Security Virtual Appliance

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

Administrative Settings

Administrator Password: Password:
 Must be 6 or more characters
 Confirm Password:

Email system alerts to:
 e.g. admin@company.com

Send Email via SMTP Relay Host (optional): Port:
 i.e., smtp.example.com, 10.0.0.3 optional

AutoSupport: Send system alerts and weekly status reports to Cisco Customer Support

SensorBase Network Participation

Network Participation: Allow Cisco to gather anonymous statistics on HTTP requests and report them to Cisco in order to identify and stop web-based threats.

Participation Level: Limited - Summary URL information.
 Standard - Full URL information. (Recommended)
Learn what information is shared...

< Prev Cancel Next >

Step 12 Click->Next

Step 13 In this document, all the defaults are set

Cisco S000V Web Security Virtual Appliance

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

Security Settings

Global Policy Default Action: Monitor all traffic
 Block all traffic
If block all traffic is selected, the Global Access Policy will be initially configured to block all proxied protocols (HTTP, HTTPS, FTP over HTTP, and native FTP).

L4 Traffic Monitor: Action for Suspect Malware Addresses Monitor only
 Block

Acceptable Use Controls: Enable
The Global Access Policy will be initially configured to monitor all pre-defined categories.

Reputation Filtering: Enable
The Global Access Policy will be initially configured to use Web Reputation Filtering and Adaptive Scanning.

Malware and Spyware Scanning: Enable Webroot Enable McAfee Enable Sophos
The Global Access Policy and Outbound Malware Scanning Policy will be initially configured to apply the actions configured below.
Action for Detected Malware: Monitor only
 Block

Cisco Data Security Filtering: Enable
The Global Cisco Data Security Policy will be initially configured to block uploads based on Web Reputation (if enabled) and monitor all other uploads.

< Prev Cancel Next >

Step 14 Click->Next

Step 15 Review the settings

Cisco S000V
Web Security Virtual Appliance

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

Review Your Configuration

[Printable Page](#)

Please review your configuration. If you need to make changes, click the Previous button to return to the previous page.

Network Settings		Edit
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		Edit
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		Edit
Default IPv4 Gateway:	10.0.0.1	
Static IPv4 Routes:	No static routes have been defined.	
Transparent Connection Settings		Edit
Transparent Redirection Device Type:	Layer 4 Switch or No Device	

Step 16 Click->Install this configuration

WSA and ISE pxGrid Node Configuration using CA-Signed Certificates

This section covers the WSA and ISE pxGrid node configuration in a Distributed ISE Deployment with dedicated primary and secondary pxGrid nodes in an Active Standby Configuration. Please note that a Microsoft Enterprise 2008 CA Certificate Authority (CA) server was used to sign the ISE nodes, ISE pxGrid nodes and the WSA. Please note a customized pxGrid template containing an EKU of both client authentication and server authentication was created and used for the WSA and ISE pxGrid node certificates.

First we will upload the CA root certificate into the WSA trusted store

Note: The CA root certificate has already been imported into the ISE trusted system store.

The WSA private key and the certificate-signing request (CSR) will be created. The CSR request will be copied/pasted into a Microsoft's advanced user request using the customized pxGrid template. The WSA certificate will be downloaded and both the WSA public certificate and private key will be uploaded to the WSA.

ISE access logs will be configured on the WSA to help trouble-shoot WSA+ISE integration issues, such as WSA services restarting, and not being able to resolve the ISE+pxGrid IP address or FQDN through the WSA.

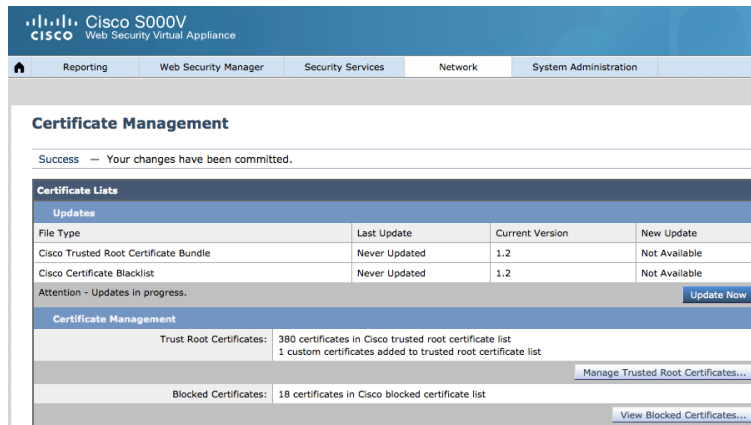
The CA root certificate from the pxGrid primary and pxGrid secondary nodes will be uploaded into the WSA. The pxGrid nodes will query the admin nodes to see which one is operational. By default the primary pxGrid node will be active and the secondary pxGrid node inactive. In the event a complete PPAN failure occurs, and the SPAN becomes active, the primary pxGrid node will see the SPAN as active PPAN.

The public certificates from the primary and secondary ISE and MNT nodes are uploaded into the WSA for bulk session download information for the initial WSA startup. If the primary MNT goes down, the WSA will still contain the SGT-IP mappings in the cache and will also detect that the primary MNT is down via query checks from the primary admin node (PPAN). The MNT nodes will also query the admin nodes to which one is operational. If the MNT nodes have multiple certificates, the one designated for admin purpose will be selected.

Adding CA Root Certificate to WSA Certificate Trust Store

Add CA Root Certificate to WSA Trusted Store

Step 1 Select->Network->Certificate Management->Manage Trusted Root Certificates->Import and upload the CA root certificate->Submit->Commit



Configuring CA-Signed WSA Client Certificate

Creating WSA private key and CSR request

You can use a MAC or Linux server for creating the private key and CSR request. In this example, a MAC was used. In the below example, the WSA private key was created:

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

In the below example, the CSR request is generated from the WSA private key:

```
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 []:
```

Copy/paste the CSR request into the pxGrid-customized template and download in a base-64 encoded format

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 req Request box.

Saved Request:

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

```
MSLtljofmDFsDk8ZogFzRHRet0At3xuy5GYIPVT0TkK7
rDAAcYpOGa1+7bgXNoRjnuEA32XP3pOb5ap6Hrt54I
2O7dbnNGd9bbiEkzbOKM7y9AvHEJB8Ehr8fcfx+Mbv
AZ/X/wpsmnLO1E91C88FrcjHAvh5fGaw5FMKAhyl
8/x29MNHAguykoXHISglPMIEOC7IH9K3GmRl85HOF!
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

pxGrid

Additional Attributes:

Attributes:

Submit >

- Step 1 Select-Submit
- Step 2 Download “base-64”

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



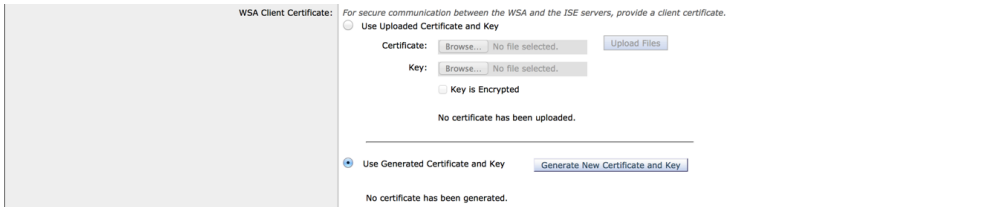
[Download certificate](#)
[Download certificate chain](#)

- Step 3 Download “base-64”, then submit
- Step 4 Also download the root certificate in “base-64”

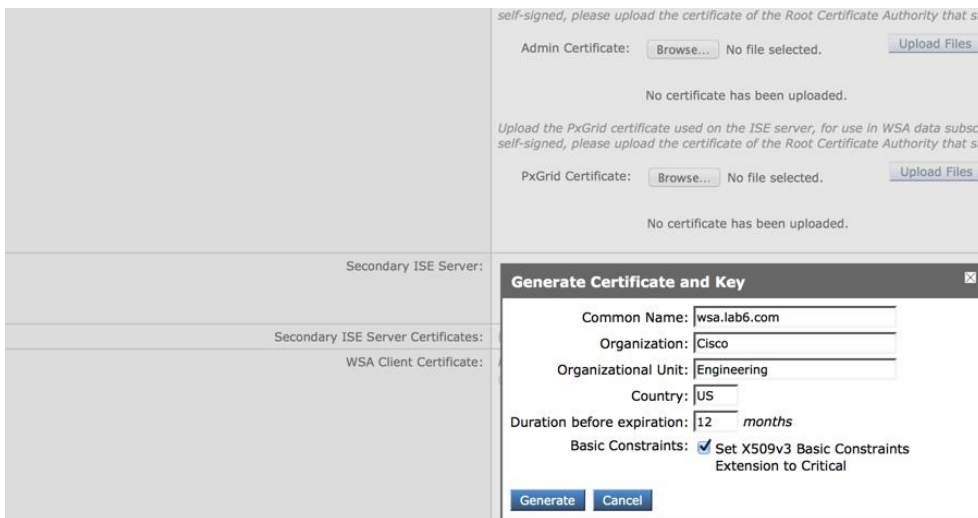
Creating WSA private key and CSR request from WSA (alternative)

Generate WSA CSR for pxGrid operation

- Step 1 Select->Network->Identification Service->Identity Service Engine->Edit Settings->WSA Client Certificate->Generate New Certificate and Key

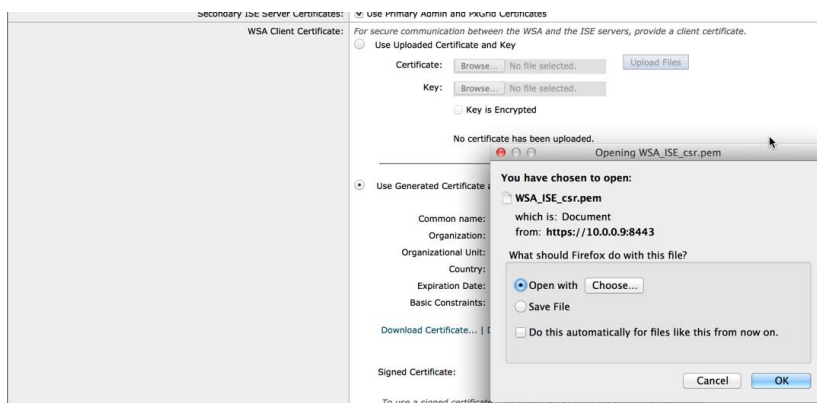


Step 2 This will generate the CSR request, enter the information

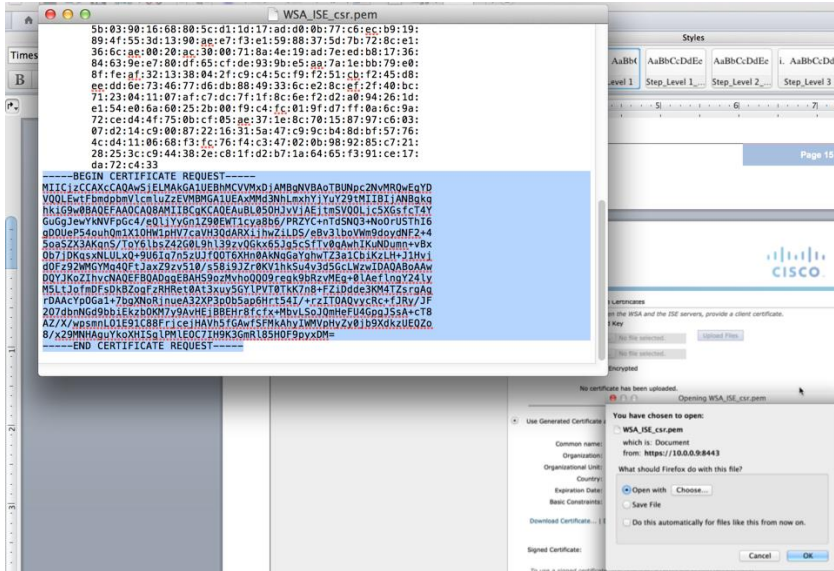


Step 3 Select->Generate, you should see that the certificate and key have been successfully generated.

Step 4 Select->Download the Certificate Signing Request and open using an editor



Step 5 Cut/Paste into customized pxGrid template



Step 6 Submit Advanced User request

Microsoft Active Directory Certificate Services – lab6-WIN-49T17723UO8-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):

```
MSLlJofmDFsDk8ZogFzRHRet0At3xuy5GYPVt0TKk7
rDAAcYpOGa1+7bgXNoRjnueA32XP3pOb5ap6Hrt54I
207dbnNGd9bbiEkzbOKM7y9AvHjBBEHR8fCfx+Mbv
AZ/X/wpsmnlOE1C88frcjehAVh5FGAwSfMkAhyI
8/x29MNHAguykoXHISgIPMIEOC7IH9K3GmRi85HOF
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

pxGrid

Additional Attributes:

Attributes:

Submit >

Step 7 Select-Submit

Step 8 Download “base-64 encoded”

Microsoft Active Directory Certificate Services – lab6-WIN-49T17723UO8-CA

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

[Download certificate](#)
[Download certificate chain](#)

Step 9 Click->Submit

Step 10 Also download the root certificate in “base-64 encoded”

Step 11 Upload the WSA+pxGrid identity certificate

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

ISE Service configuration on WSA

Step 1 Create access log to include the custom field:
 System Administration->Log Subscription->access logs->Custom Fields-%m

Note: this will be used to troubleshoot WSA and ISE+pxGrid node connection issues, such as non-resolvable host if the WSA RESTful API cannot be established upon boot.

Cisco S000V
 Web Security Virtual Appliance

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

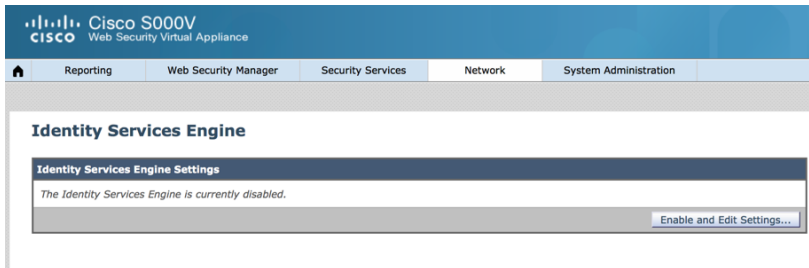
Edit Log Subscription

Log Type:	Access Logs
Log Name:	accesslogs <i>(will be used to name the log directory)</i>
Rollover by File Size:	10G Maximum <i>(Add a trailing K or M to indicate size units)</i>
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"/> <i>(Enter the HTTP status codes of transactions that should not be included in the Access Log)</i>
Retrieval Method:	<input checked="" type="radio"/> FTP on mgmt.wsa.lab6.com <input type="radio"/> FTP on Remote Server
	Maximum Number of Files: 10

Step 2 Submit->Commit the changes

Uploading primary pxGrid node certificate

Step 1 Select->Network->Identification Services->Identification Service Engine



Step 2 Select->Enable and Edit Settings

Step 3 Enter the pxGrid1 IP address or FQDN

Note: You can only have 2 pxGrid nodes per ISE deployment. This serves as a pxGrid Active-Standby configuration; only one ISE+pxGrid node can be active at a time. In a pxGrid Active-Standby configuration, all information is passed through the PSPAN, where the second ISE+pxGrid node remains inactive.

Step 4 Upload the CA root certificate for the primary pxGrid node
Upload the CA root public certificate.



Uploading secondary pxGrid node certificate

Step 1 Enter the pxGrid2 IP address or FQDN

Step 2 Upload the CA root certificate for the primary pxGrid node
Upload the CA root public certificate.

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

Uploading Primary Monitoring node certificate

Step 1 Upload the Primary MNT public certificate

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

Uploading Secondary Monitoring node certificate

Step 1 Upload the Secondary MNT public certificate

Secondary ISE Monitoring Node Admin Certificate:

Certificate: No file selected.

Common name: ise14smt.lab6.com
 Organization:
 Organizational Unit:
 Country:
 Expiration Date: Jun 18 02:46:19 2017 GMT
 Basic Constraints: Not Critical

Uploading the WSA certificate and private key

Step 1 Under WSA Client Certificate, upload the public certificate, wsa1.cer and WSA private key, wsa1.key

WSA Client Certificate: *For secure communication between the WSA and the ISE servers, provide a client certificate.*

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

Running Test

Step 1 Start Test, you should see the following:

```
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: isel4pmnt.lab6.com

Test completed successfully.
```

Below is a summary of the CA-signed WSA certificate configuration with pxGrid Active Standby in a distributed ISE environment

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.*

(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.*

(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: ise14pmnt.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: ise14smnt.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.

Step 2 Select->Commit changes twice

Verifying WSA as a registered pxGrid client

Here we verify that the WSA has registered as a pxGrid client

Step 1 Select->Administration->pxGrid Services, note the WSA has registered as a pxGrid client

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 'Clients' section is active, displaying a table of registered clients. The table has columns for Client Name, Client Description, Capabilities, Status, Client Group, and Log. One client is expanded to show its 'Capability Detail'.

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

WSA Policies

An ISE Identification profile is created on the WSA to accept ISE authentications. A web access policy is created for end-users assigned to the engineering security group tag. This web access policy denies Facebook access based on URL filtering, and application decryption policies.

Create identification Profile on WSA

- Step 1** Select->Web Security Manager->Authentication->Identification Profiles>Add Identification Profile
 Provide NAME: **ISE**
 Identification and Authentication: Transparently modify users with ISE
 Fallback to Authentication Realm or Guest Privileges: 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:	<input type="text"/>
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>

- Step 2** Select->Submit Changes and then commit twice

Create WSA Access Policy

Step 1 Select->Web Security Manager->Web Policies->Add Policy->Policy Name: Engineering

Step 2 Select->Web Security Manager->Web Policies->Add Policy->Identification Profiles and Users->Select one or more identification policies->ISE->Select Groups and Users->No Tags Entered

You will see the following:

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"/>

Step 3 Select “Engineering”->Add”, the SGT will be added to the access policy

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"/>

Step 4 Click->Done. Note “Engineering” SGT tag is selected

You should see the following:

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

Identification Profile	Authorized Users and Groups	Add Identification Profile
ISE	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users ? ISE Secure Group Tags: Engineering Users: No users entered	

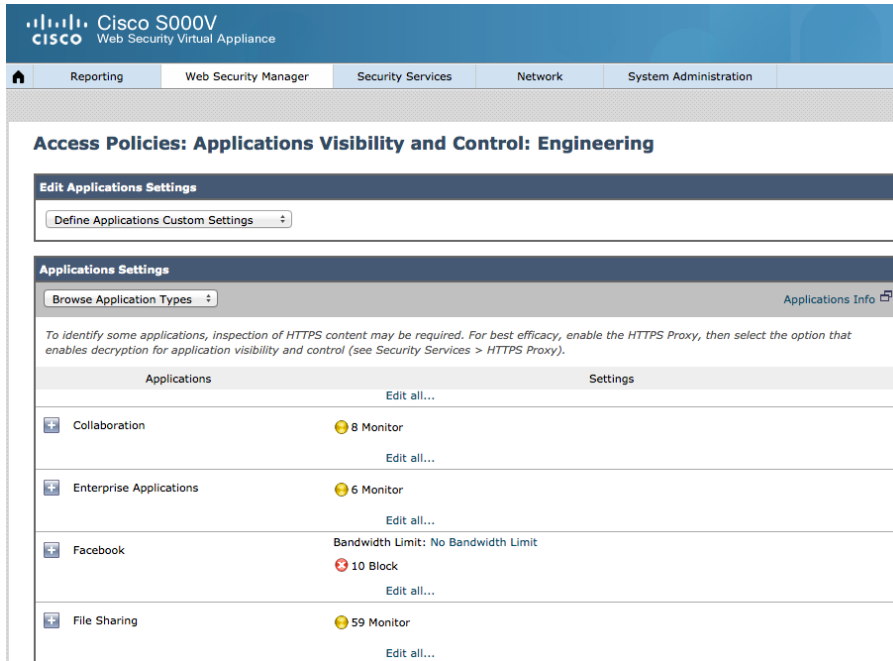
- Step 5** Click->Done
- Step 6** Click->Submit

Step 7 Under “URL Filtering” select->Global Policy and set to the following:

Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn ?	Quota-Based	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
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	✓				—	—
Streaming Video	✓				—	—
Tobacco	✓				—	—

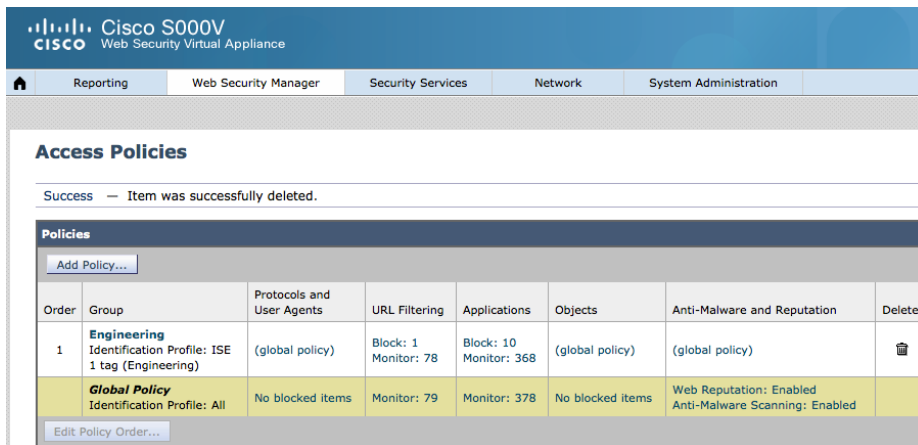
Cancel Submit

- Step 8** Select->Submit
- Step 9** Under “Applications” click on Global Policy
- Step 10** Under “Edit Applications Settings” select “Define Applications Customs Settings and block all Facebook applications



Step 11 Click->Submit and Commit Changes twice

You will see the following:



Create WSA Decryption Application Policy

Step 1 Web Security Manager->Web Policies->Decryption Policies->Add Policy->Enable Policy->Policy Name: DecryptEngineerig

Decryption Policy: DecryptEngineering

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

Step 2 Identification Profiles and Users ->Select One or More Identification Profiles->ISE->ISE Secure Group Tags: No Tags Entered and select Engineering SGT

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:	Authorized Users and Groups	Add Identification Profile
<input type="text" value="Select One or More Identification Profiles"/>	<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)	<input type="button" value="Add Identification Profile"/>
<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><small>Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.</small></p> <p>The following advanced membership criteria have been defined:</p> <p>Proxy Ports: None Selected Subnets: None Selected Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges) URL Categories: None Selected User Agents: None Selected</p>		

Step 3 When completed, select->done->submit

Step 4 Under “URL Filtering” ->”Global Policy->Pass-through->Select All” and Decrypt Social Networking

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		<input checked="" type="checkbox"/>					
Professional Networking		<input checked="" type="checkbox"/>					
Real Estate		<input checked="" type="checkbox"/>					
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 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"/>					

Cancel Submit

Step 5 Click-Submit->Commit (twice)
Step 6 You should see the following:

Cisco S000V
Web Security Virtual Appliance

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

Decryption Policies

Success — Item was successfully deleted.

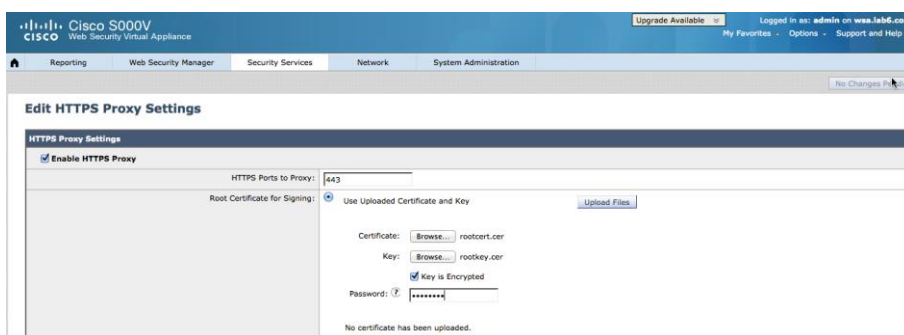
Order	Group	URL Filtering	Web Reputation	Default Action	Delete
1	DecryptEngineering Identification Profile: ISE 1 tag (Engineering)	Pass Through: 77 Monitor: 1 Decrypt: 1	(global policy)	(global policy)	
	Global Policy Identification Profile: All	Pass Through: 78 Monitor: 1	Enabled	Decrypt	

Edit Policy Order...

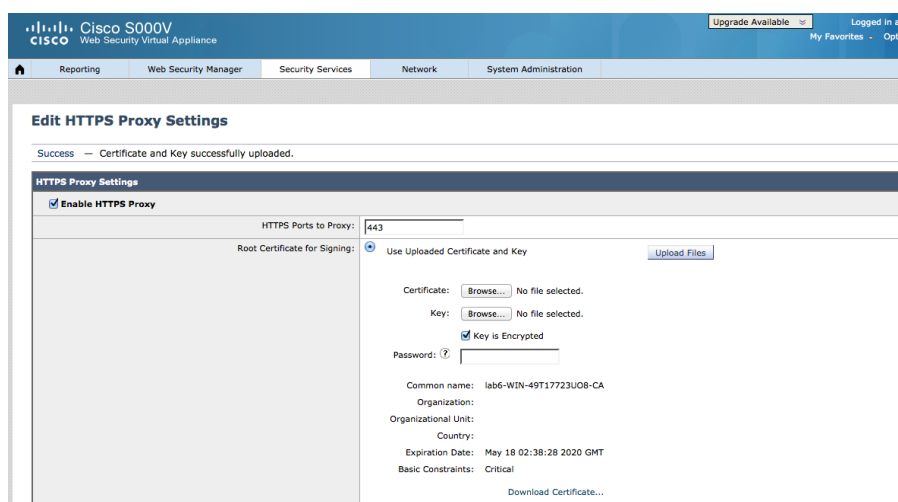
Application Decryption

HTTPS Proxy is enabled to decrypt encrypted web sites. The root public/private key pair will be uploaded in this example. You also have the option of uploading a CA signed certificate, using a subordinate CA template. This will be then used in a web access policy to block users who are assigned an Engineering SGT.

- Step 1** Go to Security Services->Proxy Settings->HTTPS Proxy
- Step 2** Click Enable and Edit Settings->Sign Proxy Agreement
- Step 3** Decryption Options->Decrypt for End-User Acknowledgement->Enable->Enable decryption for display of the end-user acknowledge page
- Step 4** Security Services->Use Uploaded Certificate and Key and select the root certificate public/private key pair and enter the password from **Obtaining Root/private key pair** below.



- Step 5** Select->Upload Files, you should see they have been successfully uploaded



- Step 6** Under “Decrypt for Application Detection”, enable “Enable decryption for enhanced application visibility...”

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	

Step 7 Click ->submit, you will see the following, click “continue”

Expired Certificate

Mismatched Hostname

Unrecognized Root Authority / Issuer

Invalid

Invalid

All other error types

No end-user notification

is not 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?

Step 8 Click Submit Changes->Commit twice

Step 9 You should see the following:

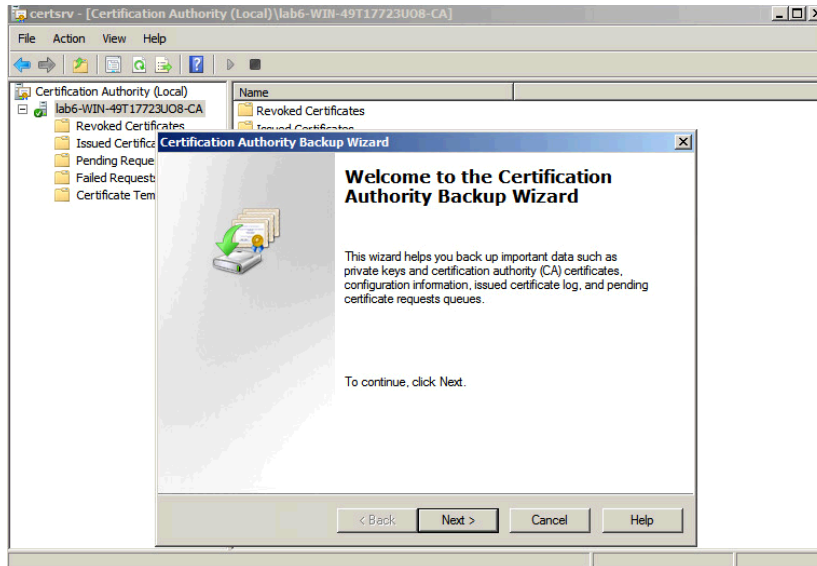
HTTPS Proxy

Success — Your changes have been committed.

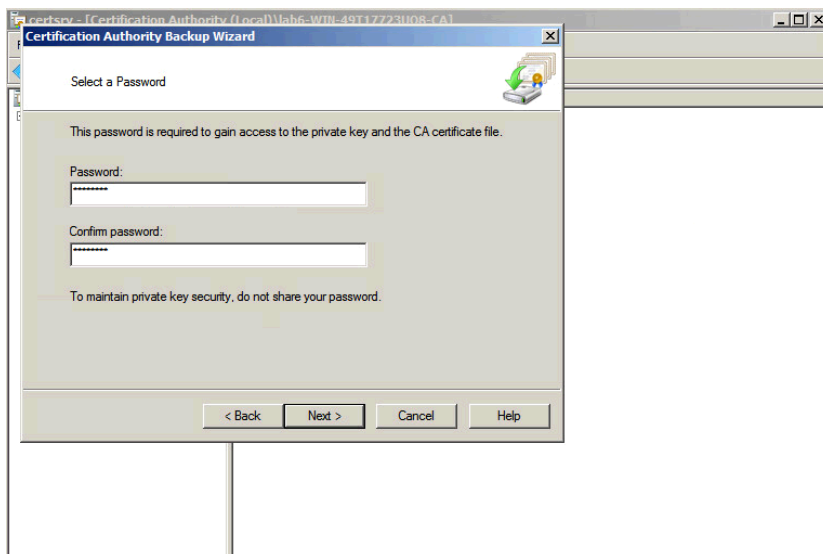
HTTPS Proxy Settings	
HTTPS Proxy:	Enabled
HTTPS Ports to Proxy:	443
Root Certificate and Key for Signing:	Using Uploaded Certificate: Common name: lab6-WIN-49T17723U08-CA Organization: Organizational Unit: Country: Expiration Date: May 18 02:38:28 2020 GMT Basic Constraints: Critical
Decryption Options	
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

Obtaining root public/private key pair

- Step 1** Backup up root ca with private key
CA Authority->Right-click on PC->All Tasks->Backup CA



- Step 2** Select->Next
Step 3 Select Private Key and CA certificate, backup location, and provide a password



- Step 4** Select->Next
Step 5 This will be saved as .P12 file Use openssl to export the private/public key from the .P12 file certificate

```
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:
```

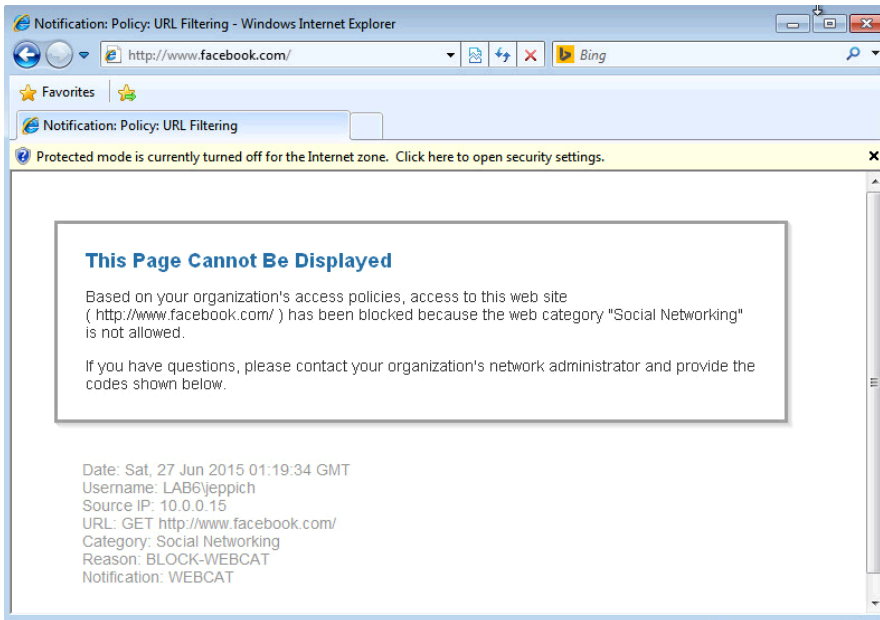
```
openssl pkcs12 -in lab6-WIN-49T17723U08-CA.p12 -clcerts -nokeys -out rootcert.cer
Enter Import Password:
MAC verified OK
```

Note: Import and PEM passphrase will be the password that was specified when exporting the CA backup certificate

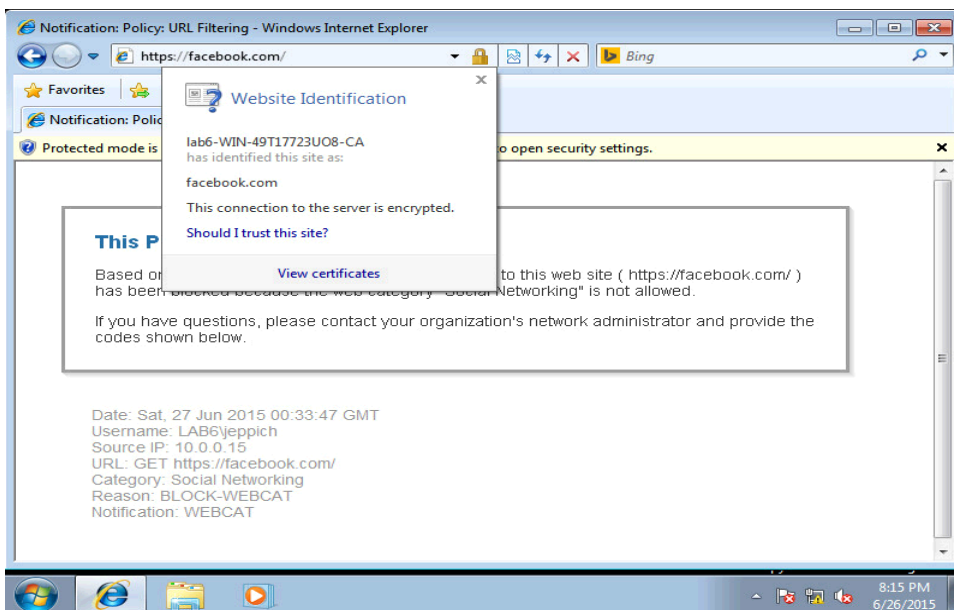
Client Testing

The end-user authenticates and is assigned to Engineering SGT, based on the initial policy web access and bandwidth are monitored. An explicit proxy was used on the client PC, user types <https://facebook.com> in browser. Internet Explorer proxy settings can be found in the Appendices.

Step 1 User accesses Facebook by typing: www.facebook.com, access is denied

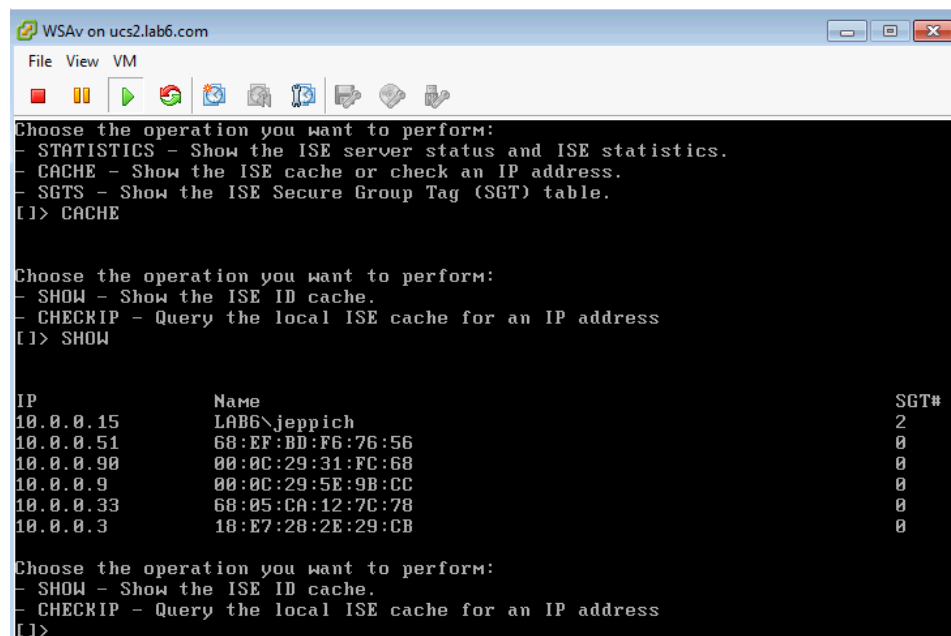


Step 2 User types: <https://facebook.com>, access is denied



Step 3 On the virtual WSA, type:

```
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.
[1]> CACHE

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[1]> 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
[1]>
```

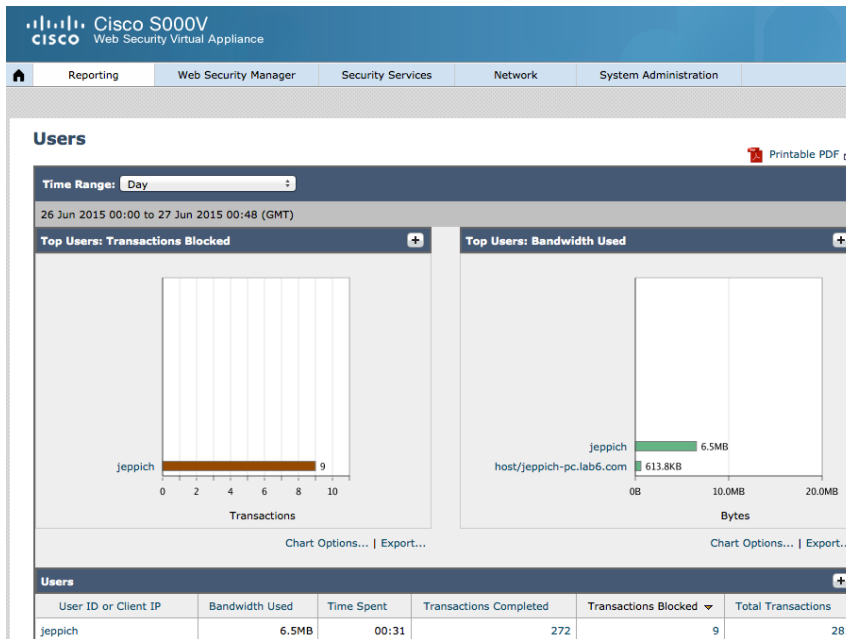
Note the SG-IP mapping for the authenticated user

Iseedata provides ISE operational statistics on downloaded tags and provide a display of IP-SGT username mappings

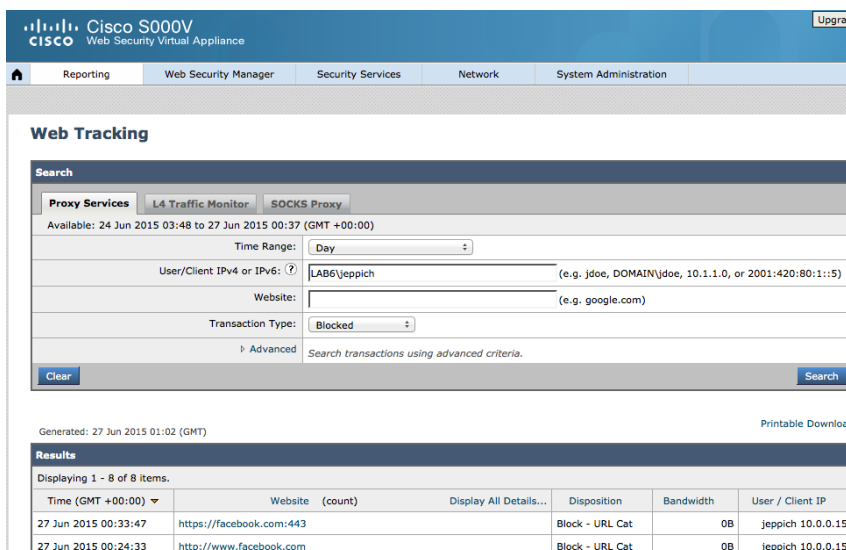
User Reports

The WSA reporting provides visibility into end-users traffic pattern by accessing web sites, monitoring web usage, providing details on blocked web transactions. Reporting also includes tracing back the end-user’s IP address from a specific URL to provide details of the web transaction.

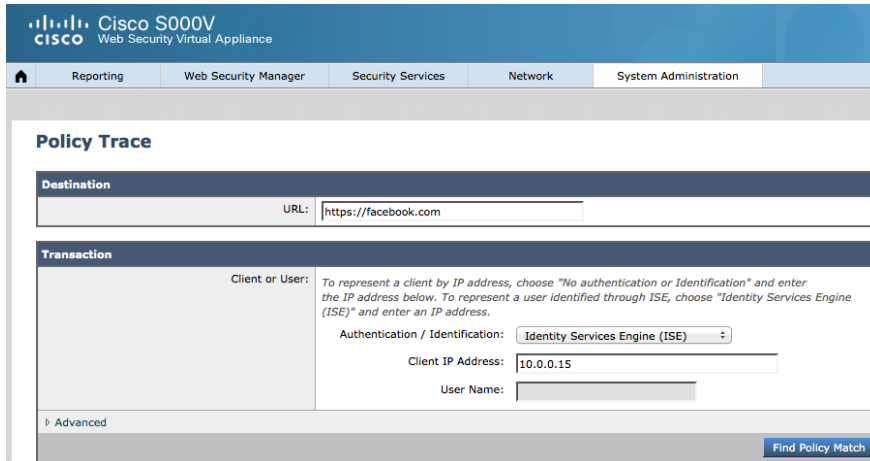
Step 1 Select->Reporting->Users. The user has some blocked transactions



Step 2 In the report, select “Transactions Blocked”, note the details transactions on the blocked facebook transaction



Step 3 You can also select a Policy Trace under System Administration, enter Identity Services Engine (ISE for Authentication/Identification and the client IP address



The screenshot shows the 'Policy Trace' configuration page in the Cisco S000V Web Security Virtual Appliance. The 'Destination' section has the URL 'https://facebook.com'. The 'Transaction' section has 'Authentication / Identification' set to 'Identity Services Engine (ISE)' and 'Client IP Address' set to '10.0.0.15'. There is also a 'User Name' field which is empty. A 'Find Policy Match' button is visible at the bottom right.

You should see the following policy trace

Note the Decryption Policy and the Access policy



The screenshot shows the 'Results' page with the following information:

- 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

Step 4 The overall user report will display the WSA matched access policy

Cisco S000V
Web Security Virtual Appliance
Upgrade

Reporting
Web Security Manager
Security Services
Network
System Administration

Users > LAB6\jeppich Printable PDF

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

URL Categories: Total Transactions

Trend: Total Transactions

URL Categories Matched Items Displayed 10

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

Columns... | Export...

Domains Matched Items Displayed 10

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

Columns... | Export...

Applications Matched

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

Advanced Malware Protection Threats Detected					
No data was found in the selected time range					
Malware Threats Detected					
No data was found in the selected time range					
Policies Matched					
Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions
DefaultGroup	Decryption	3.1MB	111	0	111
Engineering	Access	367.5KB	65	9	74
Engineering	Decryption	2.0MB	61	0	61
ExemptEngineering	Decryption	1.0MB	28	0	28
DefaultGroup	Access	54.5KB	6	0	6
DecryptEngineering	Decryption	5,201B	1	0	1
Totals (all available data):		--	272	9	281

[Find Policy Name](#) [Columns...](#) | [Export...](#)

WSA and ISE pxGrid node Configuration using Self-Signed Certificates in an ISE Stand-Alone environment

An ISE stand-alone environment using self-signed certificates may be used in a POC environment. The self-signed certificates for the WSA will be generated on a system that has openssl and keytool usually a Linux system. In this document, a MAC was used to generate the WSA private key, CSR request, and self-sign the certificates.

The ISE self-signed certificate will be exported from ISE and imported into the WSA trusted store. In an ISE stand-alone environment, the ISE identity certificate serves the purpose of all the ISE nodes and is the self-signed certificate. This certificate will be exported from the ISE system store and imported into the ISE trusted system store. The ISE identity certificate is exported and imported into the WSA trusted certificate store.

The WSA self-signed certificate will be exported and imported into the ISE trusted system certificate store. The WSA self-signed certificate will also be imported into the WSA trusted store. The self-signed certificate by default is not trusted and must be imported into the WSA trusts store, otherwise the WSA will not be able to download the initial bulk session record information and not be able to connect with the ISE pxGrid node.

The same WSA self-signed certificates can also be used for the HTTPS proxy certificates used in the WSA Decryption policies.

Create Self-Signed Certificate for the WSA

The self-signed certificate public/key pair will be created and generated. The WSA self-signed certificate will be uploaded to the WSA, and to the ISE+pxGrid node trusted system store. This certificate will also be used for the HTTPS proxy setting.

Step 1 Create a private key for the WSA

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

Step 2 Generate CSR request for the WSA from the private key

```
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 []:
```

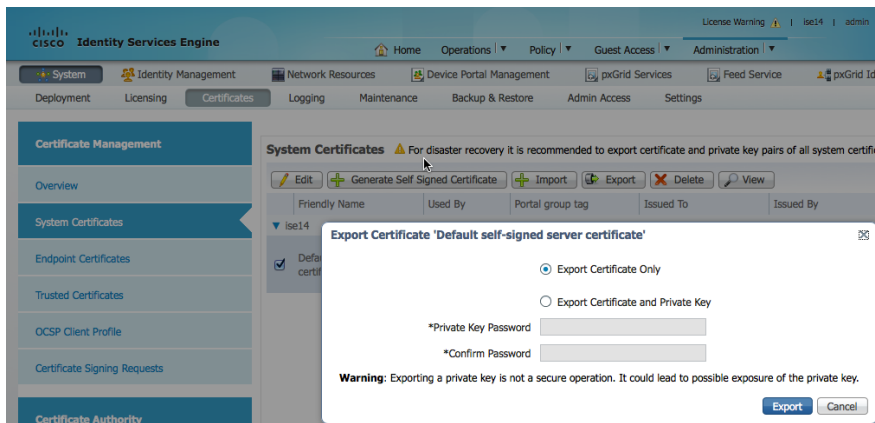
Step 3 Type the following to self-sign the WSA certificate

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

ISE Self-Signed Identity Certificate & ISE pxGrid Configuration

Step 1 Export ISE Identity certificate into System Trusted Store
Administration->System->Certificates->System Certificates->select ISE Identity Certificate->Export->Export Certificate Only

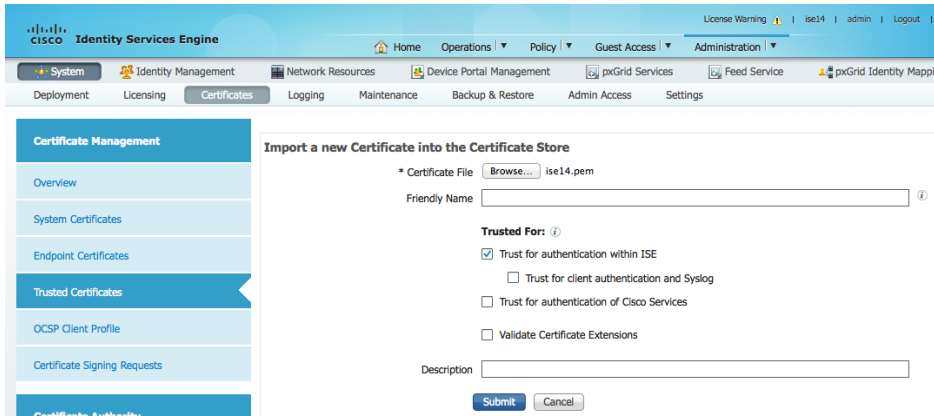
Note: The private key is not required



Step 2 Save the defaultsignedservercert.pem file, you can rename this file also

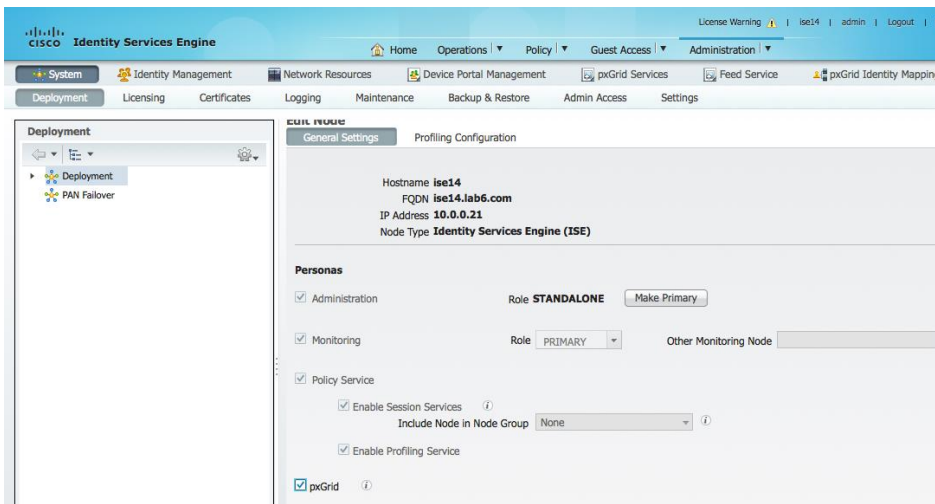
Step 3 Select->Administration->System->Certificates->Trusted Certificates->Import->Certificate file->select the PEM file and upload

Note: Ensure "Trust for Authentication within ISE" is enabled



Step 4 Click->Submit

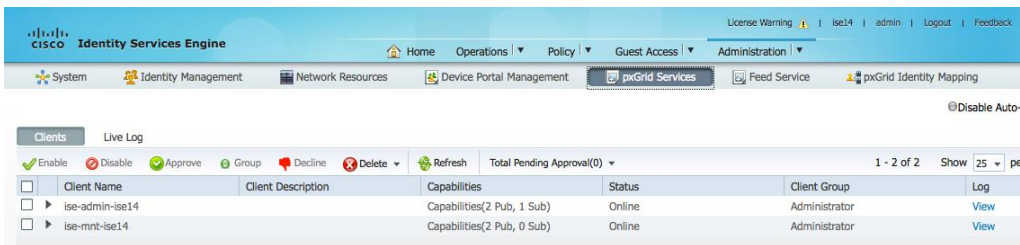
Step 5 Select->Administration->System->Deployment->select ISE node->Enable pxGrid



Step 6 Click->Save

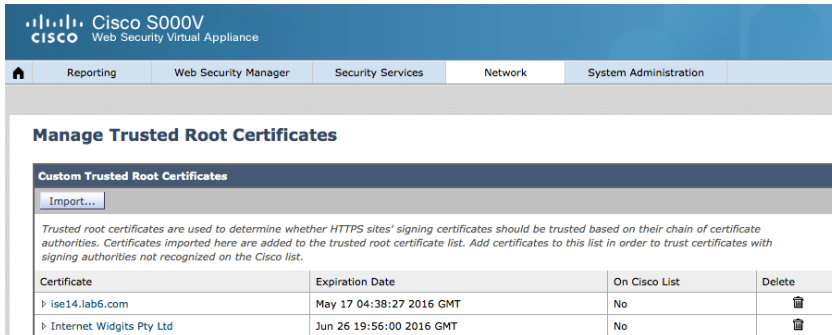
Step 7 Select->Administration->pxGrid Services. Ensure the ISE published nodes appear

Note: This may take a minute for the pxGrid services to initialize

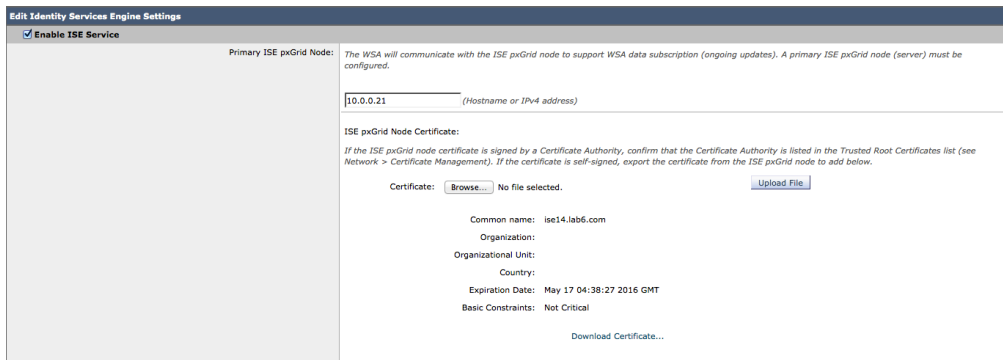


WSA and ISE pxGrid node Configuration

Step 1 Upload the WSA self signed certificate and the ISE self-signed Identity certificate to the WSA trusted store
 Select->Network->Certificate Management->Manage Trusted Root Certificates->Import the files and submit->Commit Changes twice



Step 2 Upload ISE Identity Certificate pem file to the WSA
 Select->Network->Identification Services->Identity Services Engine->Enable ISE Service, provide the ISE+pxGrid IP address or FQDN->upload the ISE identity certificate



Step 3 Leave the secondary ISE+pxGrid node blank



Step 4 Upload the ISE identity certificate as the MNT node certificate

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

Step 5 Leave the secondary MNT node blank

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.

Step 6 Upload both the WSA self-signed public certificate and the self-signed private key to the WSA

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.

Step 7 Under Test Communication with ISE server->Start Test

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

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

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

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

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

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

Test completed successfully.

Step 8 You should see the following:

Identity Services Engine

Success — Settings have been saved.

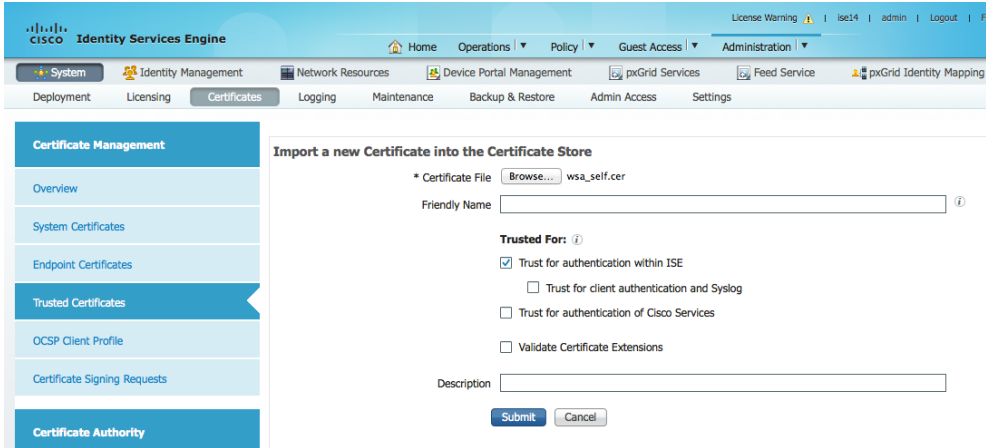
Identity Services Engine Settings	
Primary ISE Server:	10.0.0.21
Primary ISE Server Certificates:	Admin Certificate: Common name: ise14.lab6.com Organization: Organizational Unit: Country: Expiration Date: May 17 04:38:27 2016 GMT Basic Constraints: Not Critical PxGrid Certificate: Common name: ise14.lab6.com 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

[Edit Settings...](#)

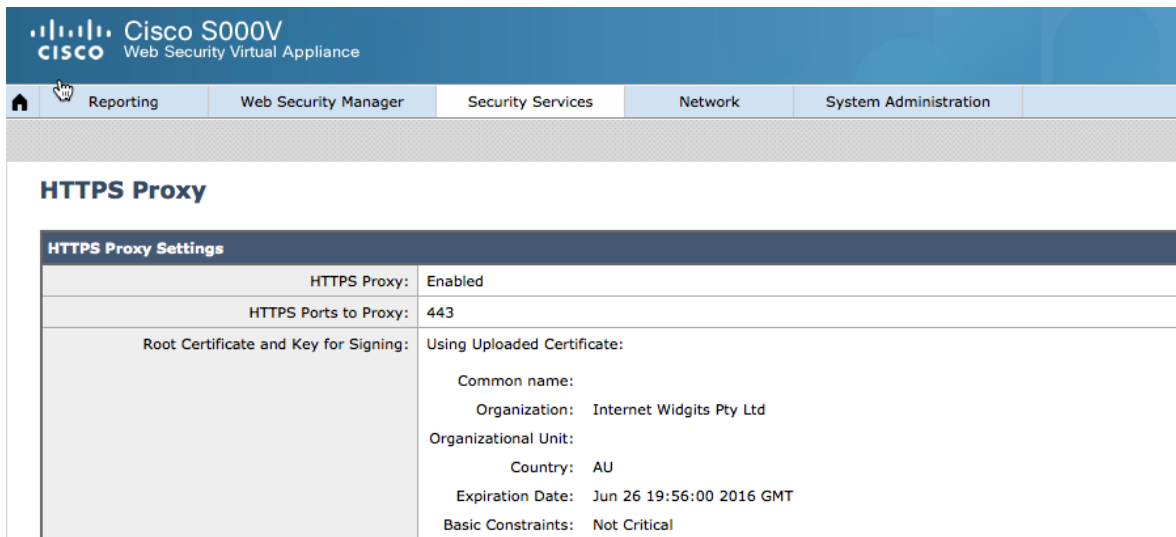
Step 9 Commit changes twice

Step 10 Upload wsa_self.cer into ISE trust store
 Select->Administration->Certificates->Certificate Management->Trusted Certificates and upload the wsa_self1.cer file.

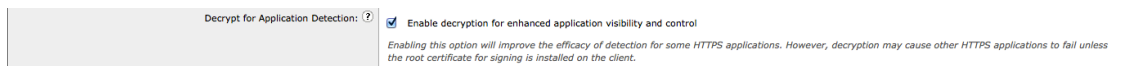
Note: Enable Trust for authentication within ISE



Step 11 Use the same WSA self-signed certs for the HTTPS Proxy
 Select->Security Services->Enable HTTP proxy and upload the public and private key from the self-signed certificate



Step 12 Enable decryption for enhanced visibility and security



Step 13 Click->Submit->

Step 14 You should see the following

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	
OCSF Result Handling:	Revoked Certificate: Drop Unknown Certificate: Monitor OCSF Error: Monitor
Edit Settings...	

Step 15 Commit Changes twice

Step 16 Please see **Dynamic Security Group Tag Assignment Using ISE, WSA Policies**

Client testing

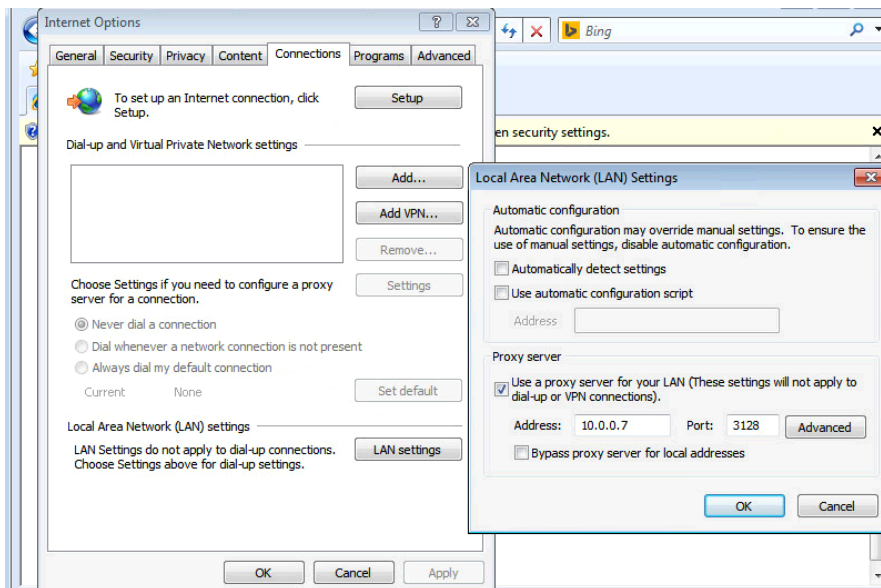
The use case is for the same one where the user successfully logs in and is assigned an engineering security group tag and is denied Facebook access by the WSA.

Step 1 End-user successfully logs in and is assigned an Engineering SGT

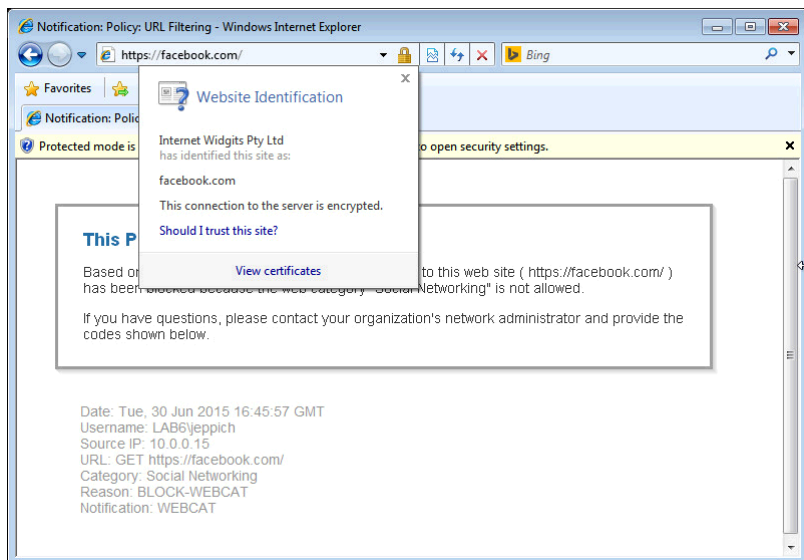
The screenshot shows the Cisco Identity Services Engine (ISE) dashboard. At the top, there are navigation tabs: Home, Operations, Policy, Guest Access, Administration, and Setup Assistant. Below the navigation, there are several status indicators: Misconfigured Suppliants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (0), and Repeat Counter (4). A table below displays session logs with columns for Time, Status, Details, Repeat Count, Identity, Endpoint ID, Endpoint Profile, Authentication Policy, Authorization Policy, Authorization Profiles, Network Device, and Device Port. The table shows three sessions, with the most recent one (2015-06-30 12:42:55.965) showing a successful login for user LAB6\jeppich on a VMWare-Device, assigned to the Engineering security group.

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					
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

Step 2 User enters their proxy information



Step 3 User access <https://facebook.com> and is denied access



Use Case Scenarios

Here will demonstrate the use cases of an organization's corporate web security policies with regards to employees, contractors, and guests. Each will be given security group tag representing an organization's web security policy

- An employee of the organization will be allowed Box.com access, denied Facebook access, and bandwidth restrictions on streamed media such as Netflix. An employee SGT will be assigned to the organization's employees.
- Guests will go through a sponsored guest portal. This default sponsor portal will be used for ISE internal users who belong to the guest and contractor identity groups. The organization's security web security for guest is to allow Facebook access and deny Box.com access. A guest SGT will be assigned to the organization's guest users.
- Contractors will be provided the same web security policy as guests.

Additionally, ISE needs to be configured for Central Web Authentication (CWA). Additional ACL's need to be put on the switch to redirect web traffic to ISE. An authorization profile for CWA will be created for initial Guest and Contractor access for redirection to ISE.

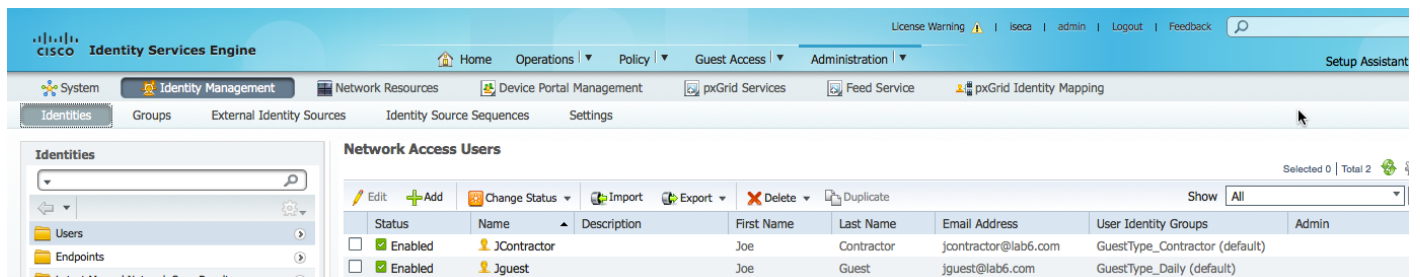
Note: Please make sure your switch is supported by ISE, by checking the ISE compatibility matrix:
http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/compatibility/ise_sdt.html

Separate identification profiles and web access policies will be defined for Employee, Guests, and Contractors will be defined on the WSA.

ISE Internal User and Default Sponsor Guest Portal

ISE internal users are configured for the Sponsor Guest portal.

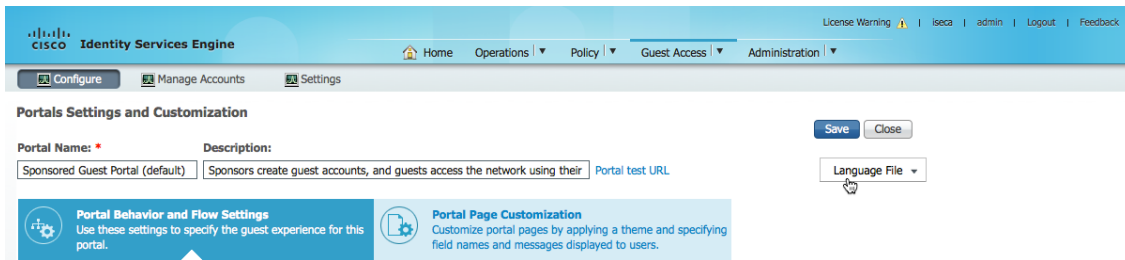
- Step 1** Select->Administrator->Users->Add the users below and the Identity Groups
Step 2 Select->Submit after each user



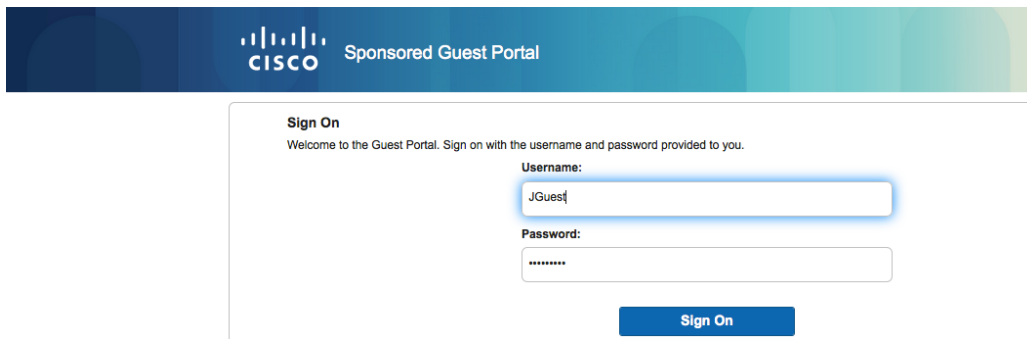
Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input checked="" type="checkbox"/>	JContractor		Joe	Contractor	jcontractor@lab6.com	GuestType_Contractor (default)	
<input checked="" type="checkbox"/>	Jguest		Joe	Guest	jguest@lab6.com	GuestType_Daily (default)	

Step 3 Select->Guest Access->Guest Portals->Sponsor Guest, and keep the defaults

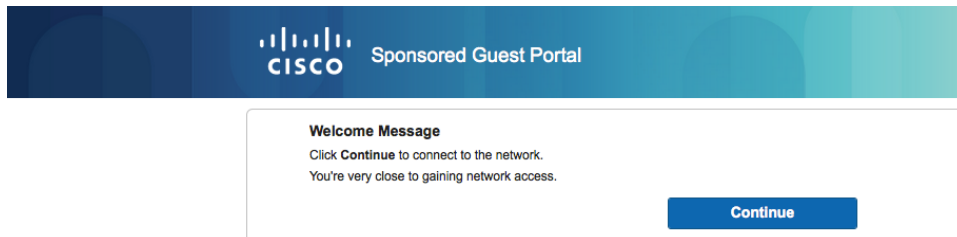
Step 4 Test the ISE internal users by selecting Portal Test URL and enter the usernames



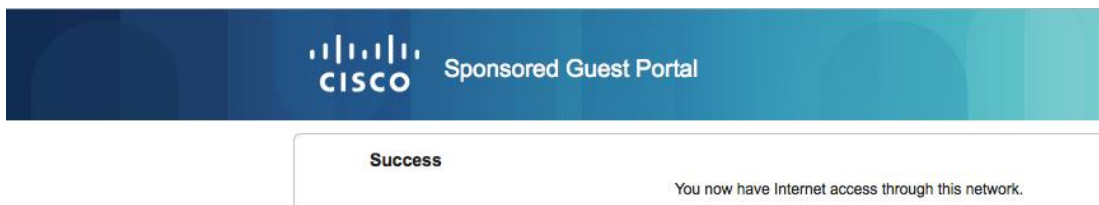
Step 5 Enter the user credentials, then Sign on



Step 6 Click->Sign On

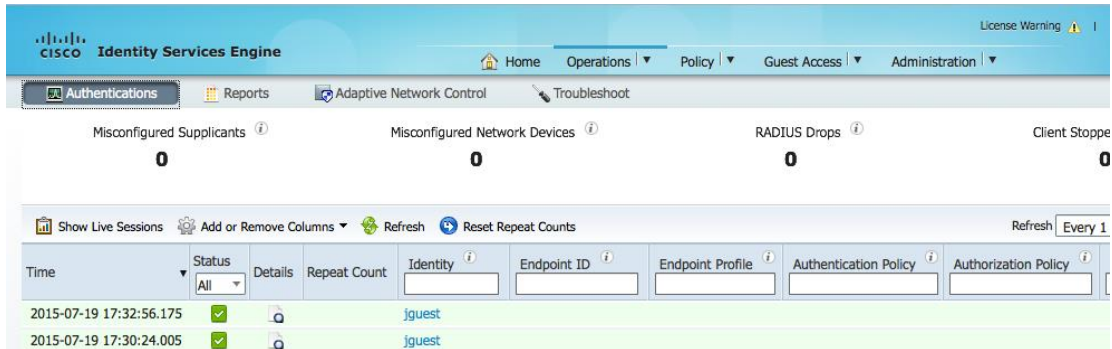


Step 7 Click->Continue



You should see that the user credentials have tested successfully

Step 8 Select->Operations->Authentications



Step 9 Follow the same procedure for testing JContractor

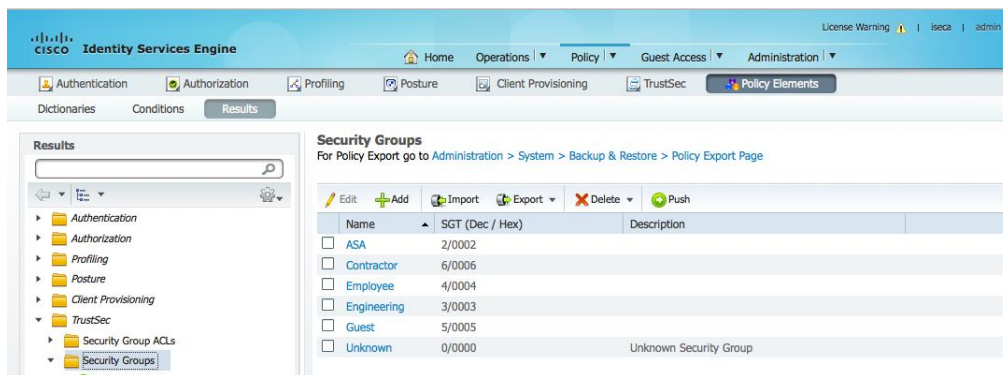
ISE Dynamic Tags, Authorization Profiles, and Authorization Policies

Create the security group tags for Employee, Contractor, and Guest. The authorization profile for CWA will be created and added to a Wired MAB condition rule in authorization policy. The security tag condition rules and associated security group tags will be applied to the authorization policy as well.

Dynamic Tags

Create Dynamic Tags for Employee, Guest and Contractor

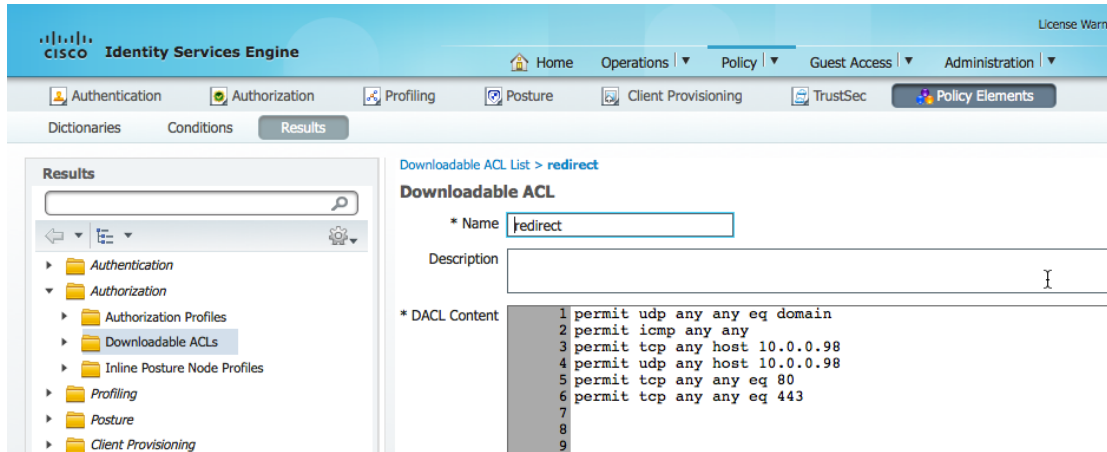
Step 1 Select –Policy->Policy Elements->results->Trustsec->Security Groups->add the additional tags for Employee, Guest, Contractor, then submit



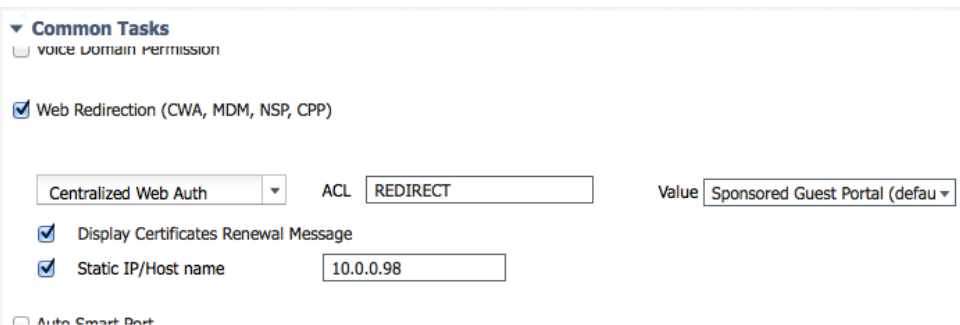
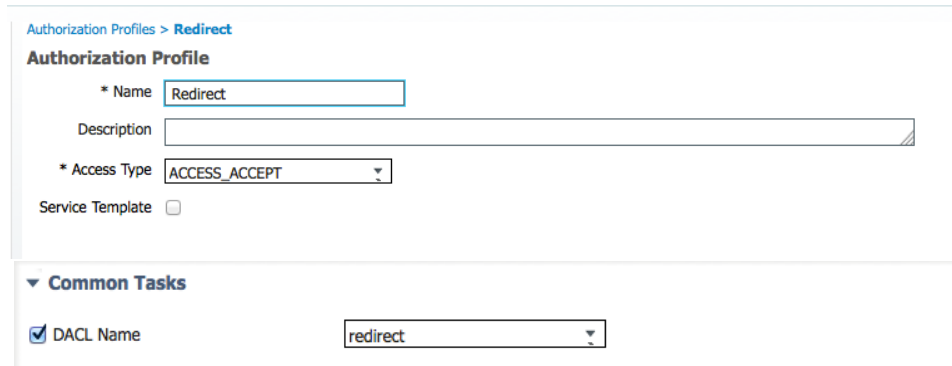
Authorization Profile and Downloadable ACL's for CWA

The downloadable DACLs will be pushed down to the switch to allow redirection back to ISE. This “redirect” DACL will be placed in the authorization profile for CWA.

Step 1 Select->Policy->Policy Elements->Results->Downloadable ACL's and Add the DACL content, then submit.



Step 2 Select->Policy->Policy Elements->Results->Authorization Profiles-Add Redirect for Name and add the redirect DACL and REDIRECT switch ACL, select the Sponsored Guest Portal The static IP address is the ISE node address in a stand-alone ISE deployment or the ISE PSN node in a distributed ISE node and is not required.

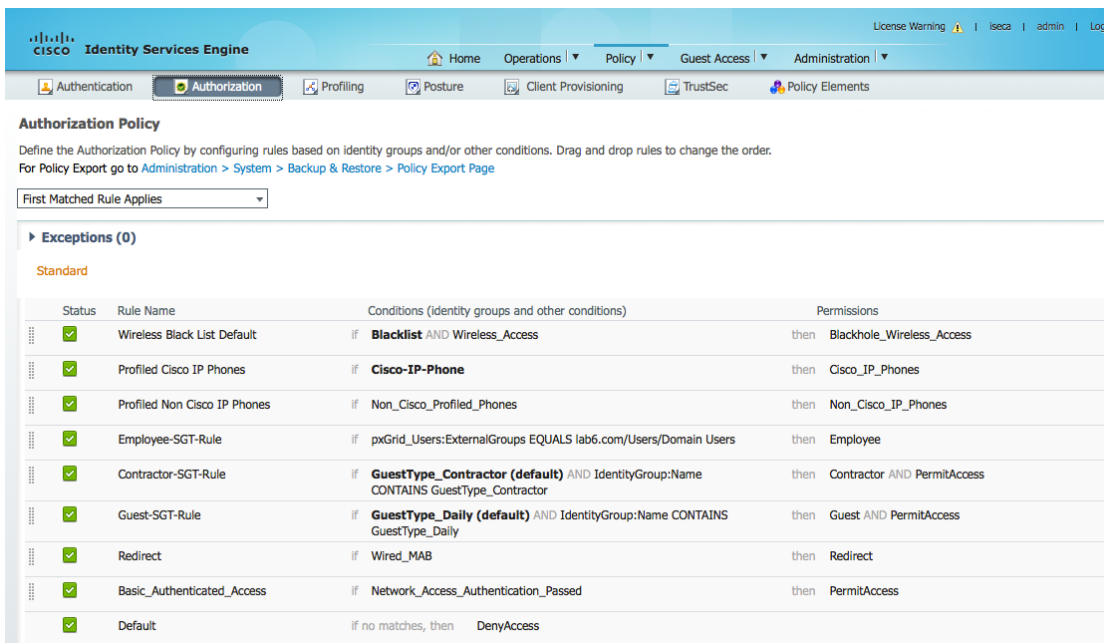


Authorization Policy

The authorization policy has been updated to include the Employee, Contractor, Guest SGT and wired MAB rules.

Step 1 Select->Policy->Authorization->add Employee-SGT Rule, Contractor-SGT Rule, and Guest-SGT rules:

- Employee SGT Rule – ExternalGroup/Domain/Users – Employee SGT
- Contractor SGT Rule – Identity Group: GuestType_Contractor (default)
IdentityGroup:Name contains GuestType_Contractor
Contractor-SGT and Permit Access
- Guest SGT Rule – Identity Group: GuestType_Daily (default)
IdentityGroup:Name contains GuestType_Daily
Guest-SGT and Permit Access



Step 2 Add the CWA redirect rule:
Redirect Rule ->Wired MAB condition from library.>Redirect authorization profile

Step 3 Select->Save

Employee

The WSA Identification Profile and the Web access policies for Employee is created. The web access policy is to allow Box.com access and deny Facebook Access.

Identification Profile and Web Access Policy

Step 1 Select->Web Security Manager->Web Policies->Web Access Policies->and create the Employee Identification Profile by clicking on “Secure Group Tags; No Users Entered” and select the “Employee” Security Group Tag Name

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.

Search

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"/>

Step 2 Click->Done

Step 3 You will see the following:

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

- Step 4** Click on Submit and Commit Changes twice
- Step 5** Under URL Filtering click on “Monitoring”
- Step 6** By default, File Transfer Services is set to Monitoring to allow Box.com access

Note: A custom defined URL category for www.box.com can also have been created under Web Security->Custom categories. This would have been present here under URL categories.

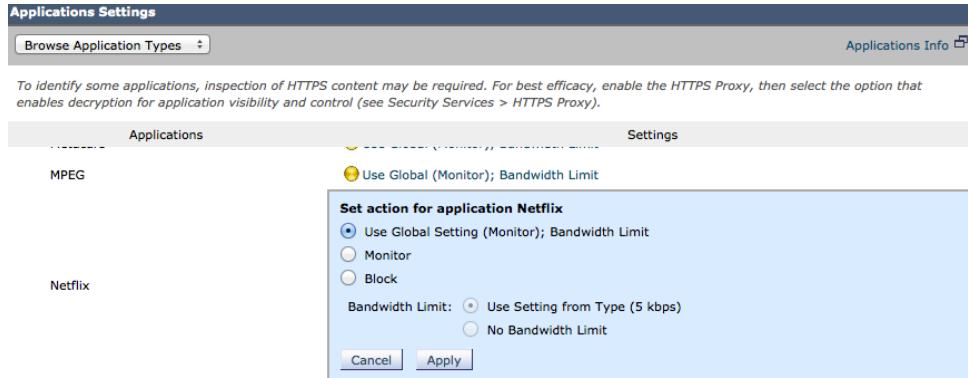
- Step 7** Proceed to “Block” Social Networking for Facebook.
- Step 8** Submit and Commit Changes twice

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 <small>⊘</small>	Monitor <small>⊕</small>	Warn <small>⚠</small>	Quota-Based <small>⚙</small>	Time-Based <small>⌚</small>
<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 checked="" type="checkbox"/> Social Science	✓				-	-

- Step 9** Under Applications, select monitoring->Edit->Application Settings->Define Applications Custom Settings
- Step 10** Under Media, click on “no bandwidth limit” and set the bandwidth limit, then Apply, this will be applicable to all media types.
- Step 11** Click on Media to ensure, “Netflix” is selected

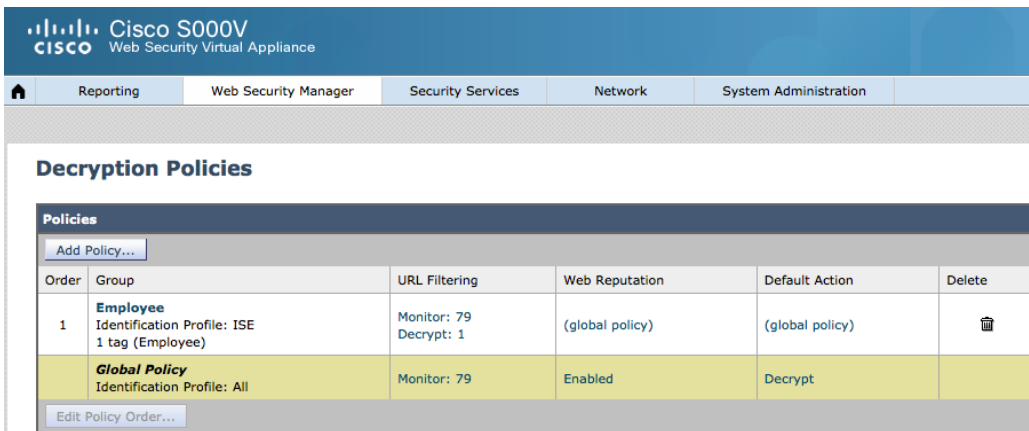


Step 12 Click->Submit->Commit Changes twice

Step 13 You should see the following:

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

Step 14 A decryption policy for Facebook will be created for Employees. See **Application Decryption**.

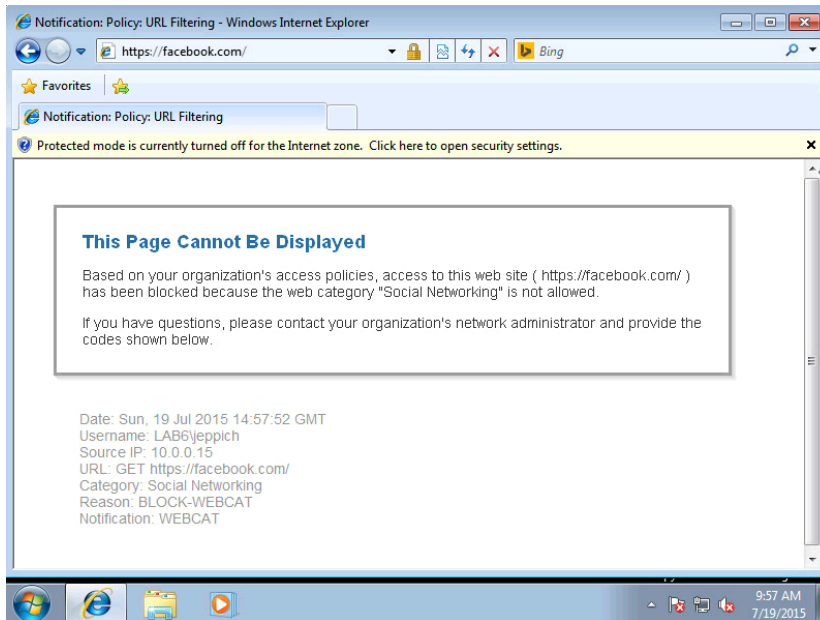


Testing

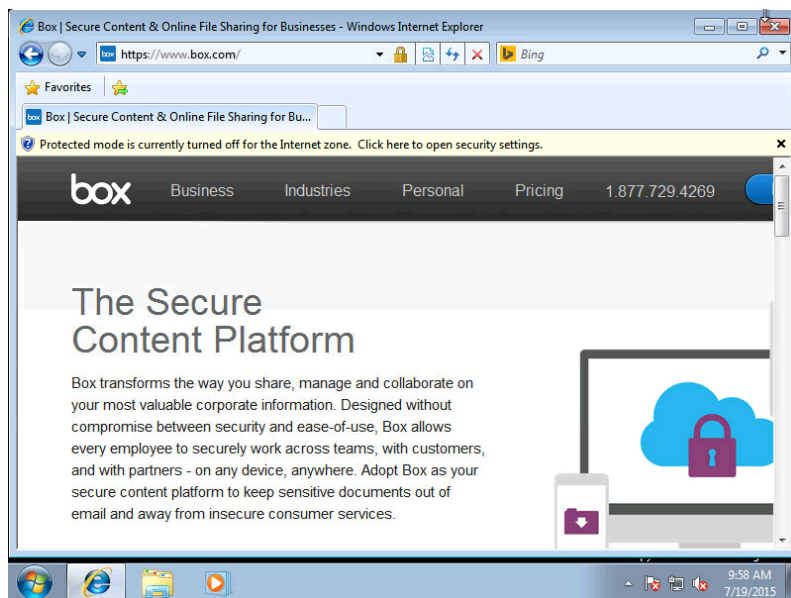
The employee will authenticate successfully and receive an employee security group tag and denied Facebook access,

allowed box.com access, and restricted Netflix access.

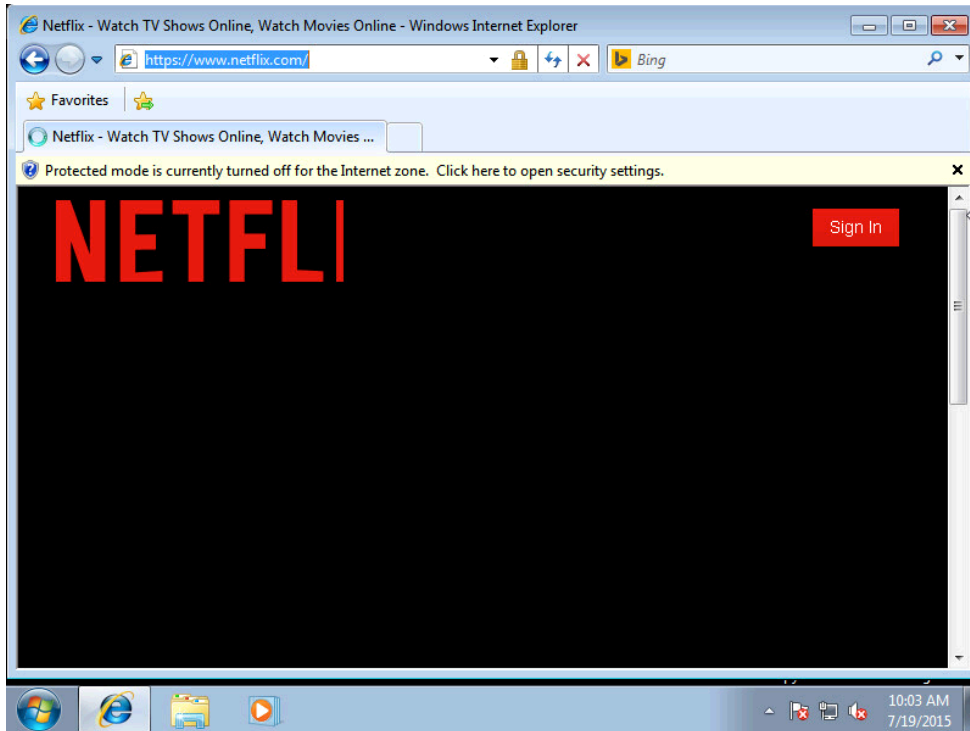
- Step 1** The employee successfully authenticates via 802.1X and receives an employee security group tag and is denied Facebook access



- Step 2** The employee is able to access Box.com



- Step 3** When the employee accesses Netflix, they will notice the slow screen painting for the streaming media bandwidth restrictions



Step 4 “ISEDATA” is run on the WSA to obtain the SGT-IP mappings for employee LAB6\jeppich

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

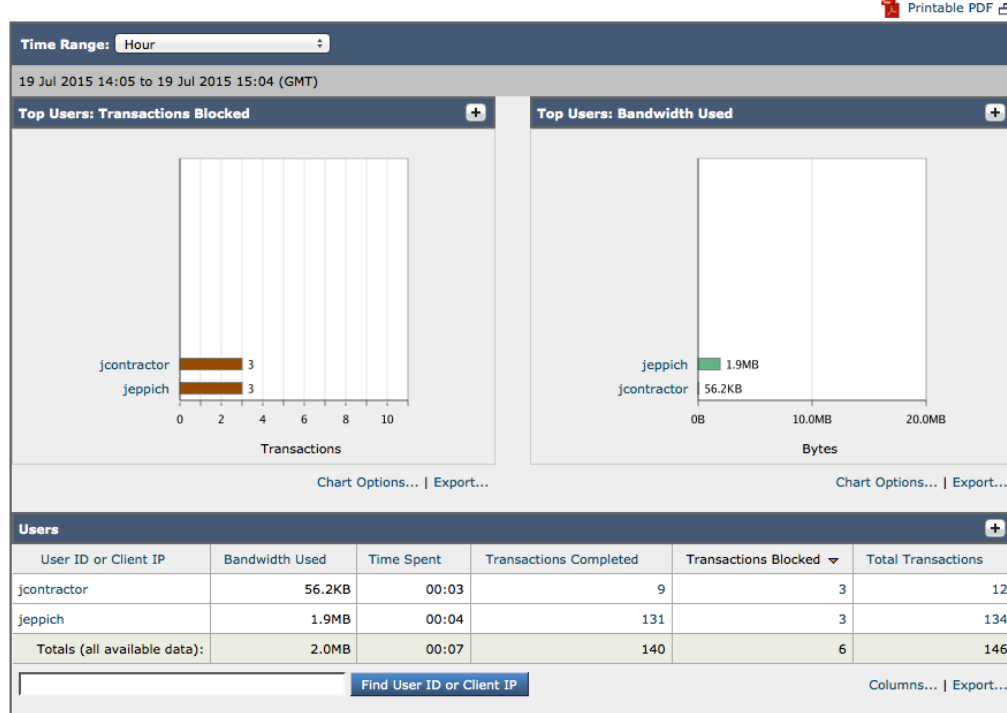
```
Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[]> SHOW
```

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
[]> █
```

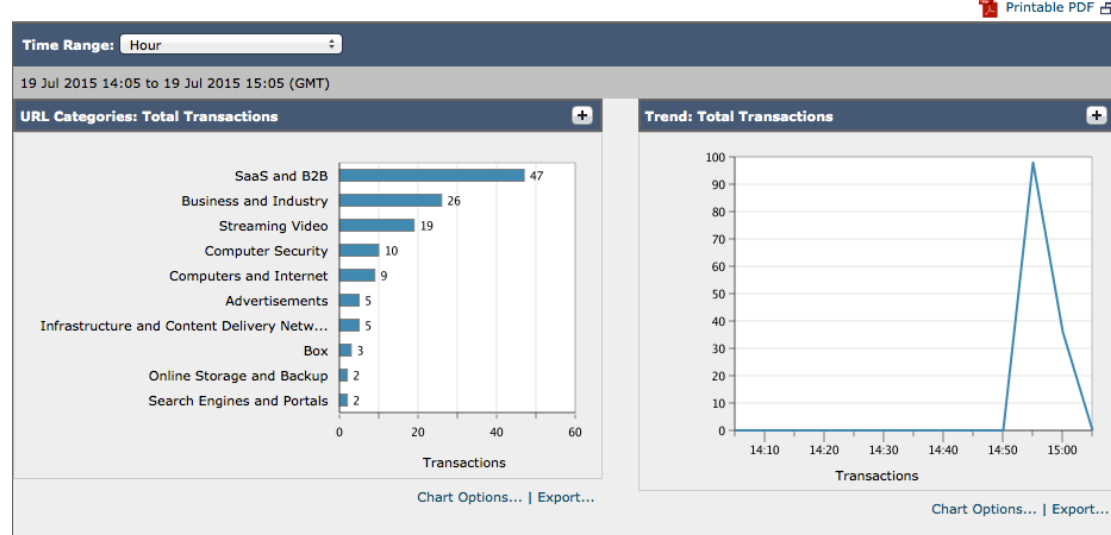
Step 5 Select->Reporting->Users report. Notice that jeppich has 3 blocked transactions, and has some bandwidth usage

Users



Step 6 Click->jeppich to drill down to see the Box transactions, blocked Facebook access, streaming media bandwidth and matched Web Access employee policy.

Users > LAB6\jeppich



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...

Step 7 Select->System Administrator->Policy Trace. Note the policy trace for Netflix and matching Employee Web Access policy

Destination	
URL:	<input type="text" value="www.netflix.com"/>
Transaction	
Client or User:	<i>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.</i>
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"/>
Advanced Find Policy Match	

Results
<p>User Information</p> <p>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</p> <p>URL Check</p> <p>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</p> <p>Policy Match</p> <p>Cisco Data Security policy: None Decryption policy: None Routing policy: Global Routing Policy Identification Profile: ISE Access policy: Employee</p>

Step 8 Note the policy trace for Box and matching Employee Web Access policy

Destination	
URL:	<input type="text" value="www.box.com"/>
Transaction	
Client or User:	<i>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.</i>
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"/>
Advanced 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

Step 9 Note the policy trace for Facebook and matching Employee Web Access policy and blocked transaction

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

Step 10 Select->Operations->Authentications to view the authenticated user and employee security group tag assignment

Time	Status	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device
2015-07-19 14:49:44.229	Success	0	LAB6\jeppich	00:0C:29:79:02:A8	VMWare-Device	Default >> Dot1X >> D..	Default >> Employee-S...	Employee	sw
2015-07-19 14:49:44.220	Success	0	LAB6\jeppich	00:0C:29:79:02:A8	VMWare-Device	Default >> Dot1X >> D..	Default >> Basic_Auth...	PermitAccess	sw

Guest

The WSA Identification Profile and the Web access policies for Guest is created. The web access policy is to deny Box access and allow Facebook Access.

Identification Profile and Web Access Policy

Step 1 Select->Web Security Manager->Web Policies->Web Access Policies->and create the Guest Identification Profile by clicking on “Secure Group Tags; No Users Entered” and select the “Guest ” Security Group Tag Name

Secure Group Tag Name	SGT Number	SGT Description	Delete
Guest	5	__NONE__	<input type="checkbox"/>

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 checked="" type="checkbox"/>
Employee	4	__NONE__	<input type="checkbox"/>
Contractor	6	__NONE__	<input type="checkbox"/>
ANY	65535	Any Security Group	<input type="checkbox"/>

- Step 2** Click->Done
- Step 3** You will see the following

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 ▾

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

- Step 4** Click on Submit and Commit Changes twice
- Step 5** Under URL Filtering click on “Monitoring”
- Step 6** Block File Transfer Services

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 <small>⊗</small>	Monitor <small>⚠</small>	Warn <small>?</small>	Quota-Based <small>⌚</small>	Time-Based <small>⬇</small>
	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
<small>⚠</small> Education	✓				-	-
<small>⚠</small> Entertainment	✓				-	-
<small>⚠</small> Extreme	✓				-	-
<small>⚠</small> Fashion	✓				-	-
<small>⊗</small> File Transfer Services		✓			-	-
<small>⚠</small> Filter Avoidance	✓				-	-

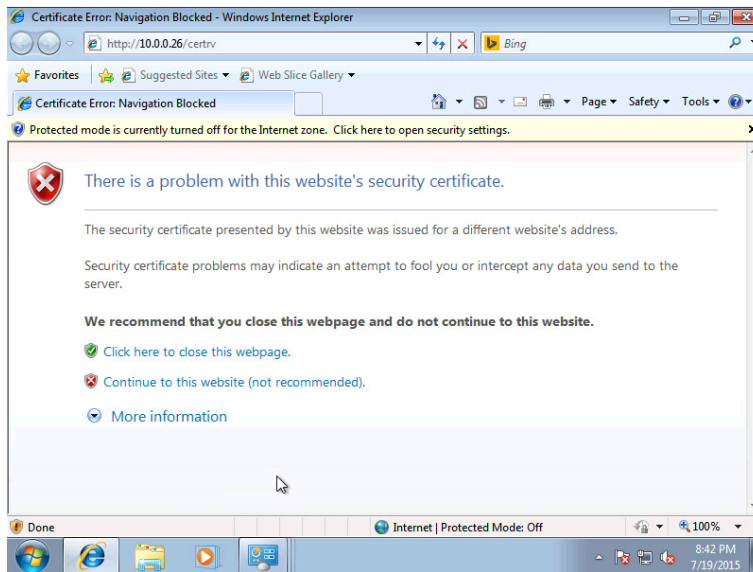
- Step 7** Set the BOX URL policy as monitoring or allow
- Step 8** Submit and Commit Changes twice

Testing

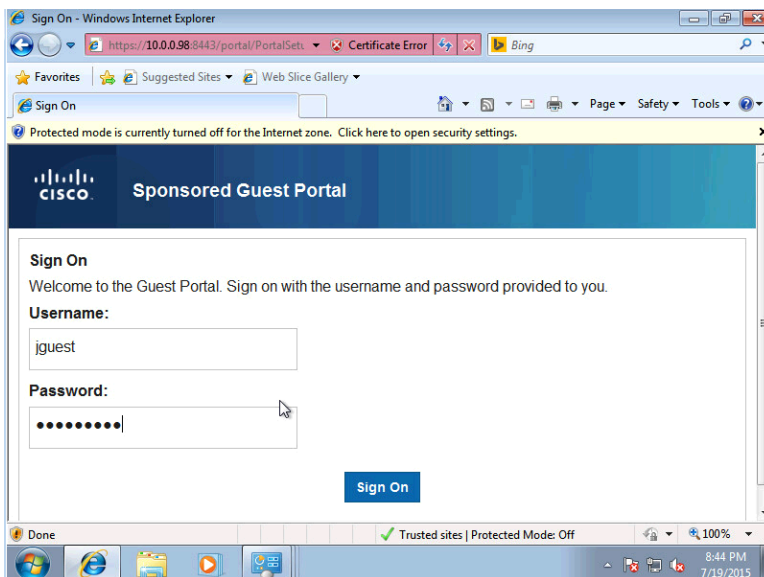
The guest user opens their browser, to an internal web server, and will get redirected access the sponsored guest portal.

Note: The certificate error message is due to not using the FQDN for the ISE node redirection. Instead just the IP address was used causing the below error message. Also 10.0.0.26 was internal web server used for ISE redirection. It is better to use <http://1.1.1.1> instead. This is noted in the Proxy Settings in the Appendices.

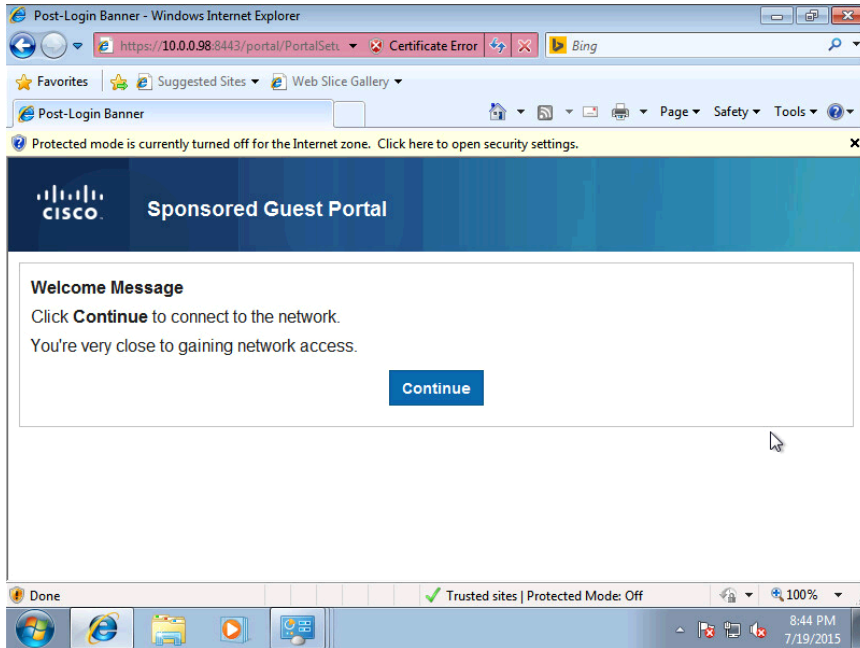
Step 1 The guest user will be redirected ISE when accessing <http://10.0.0.26/certsrv>



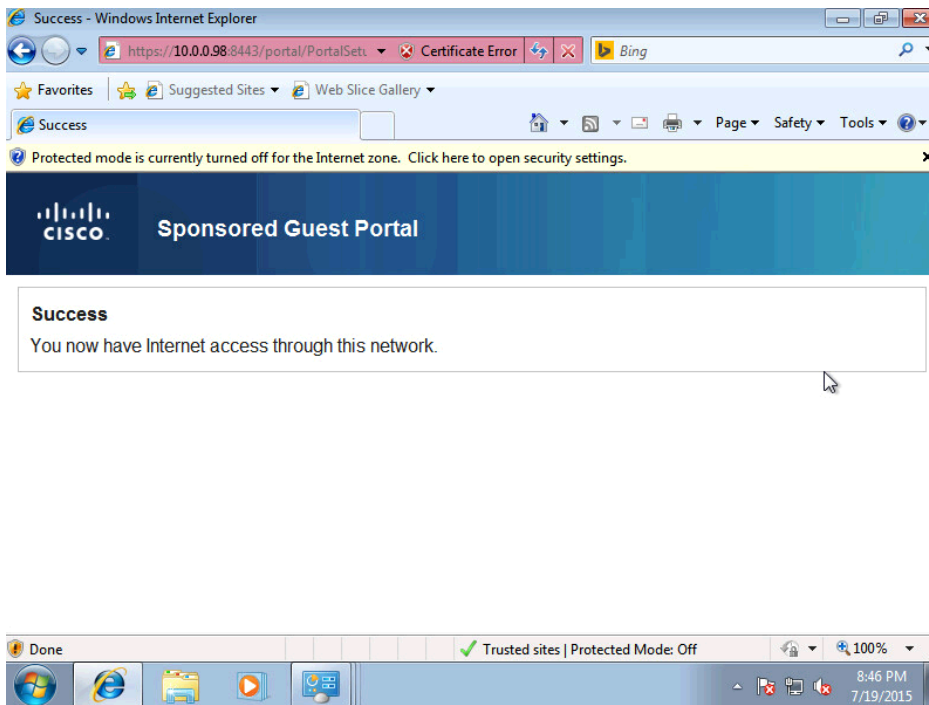
Step 2 The guest user will enter their credentials and then Sign On



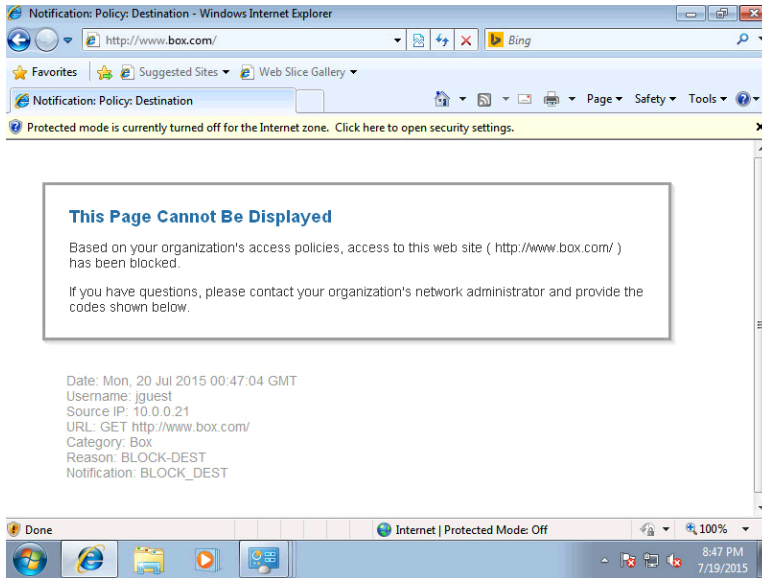
Step 3 Select Continue



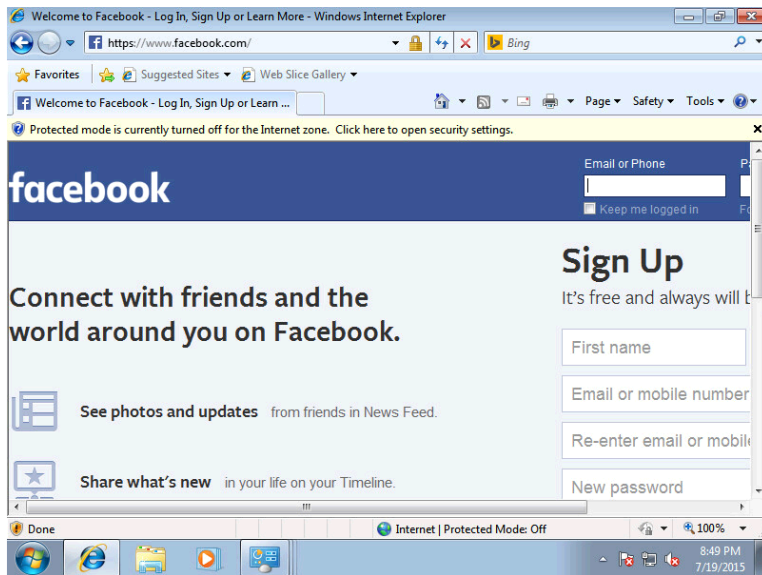
Step 4 Jguest has logged on successfully



Step 5 Box.com has been denied



Step 6 Facebook has been allowed



Step 7 Notice SGT-IP Mappings for Guest

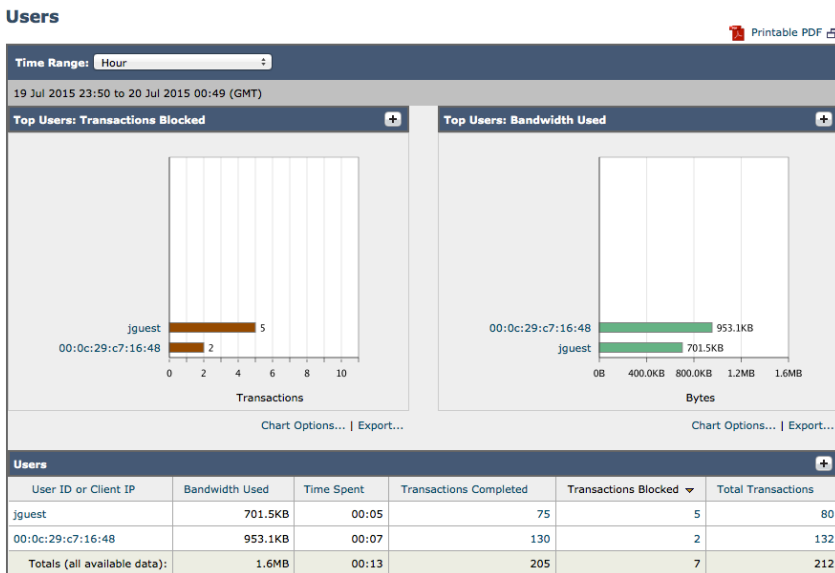
```
- CACHE - Show the ISE cache or check an IP address.
- SGTs - Show the ISE Secure Group Tag (SGT) table.
[]> CACHE
```

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

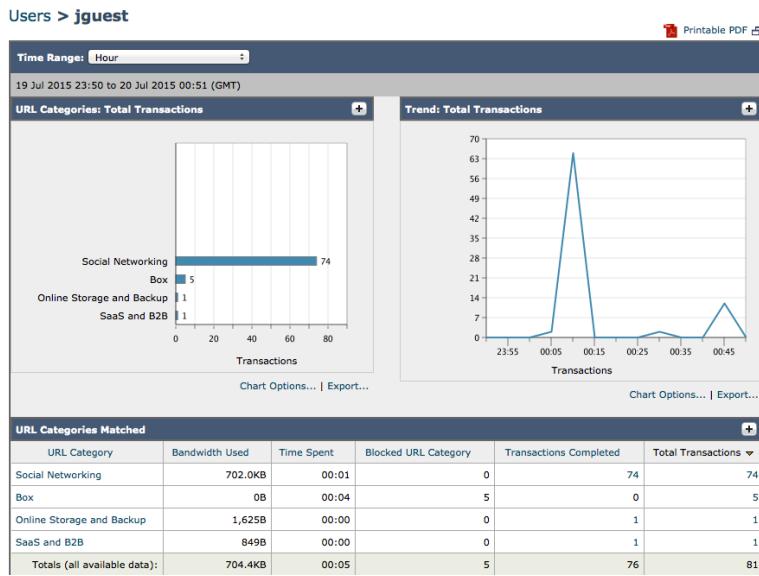
IP	Name	SGT#
10.0.0.15	LAB6\jeppich	4
10.0.0.98	00:0C:29:35:48:2A	0
169.254.57.162	00:0C:29:C7:16:48	0
10.0.0.22	00:0C:29:CA:A3:8F	0
10.0.0.33	68:05:CA:12:7C:78	0
10.0.0.21	jguest	5
10.0.0.3	18:E7:28:2E:29:CC	0

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

Step 8 Note the Users report for jguest, he has 2 blocked transactions



Step 9 Click on jguest to see the blocked transactions for Box



Step 10 Jguest has been denied access for Box and allowed access for Facebook

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
snapengage.com	849B	00:00	1	0	1

Step 11 The application matches provide more visibility

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

Step 12 Select->Administrator->Policy Trace and review the policy trace for Box

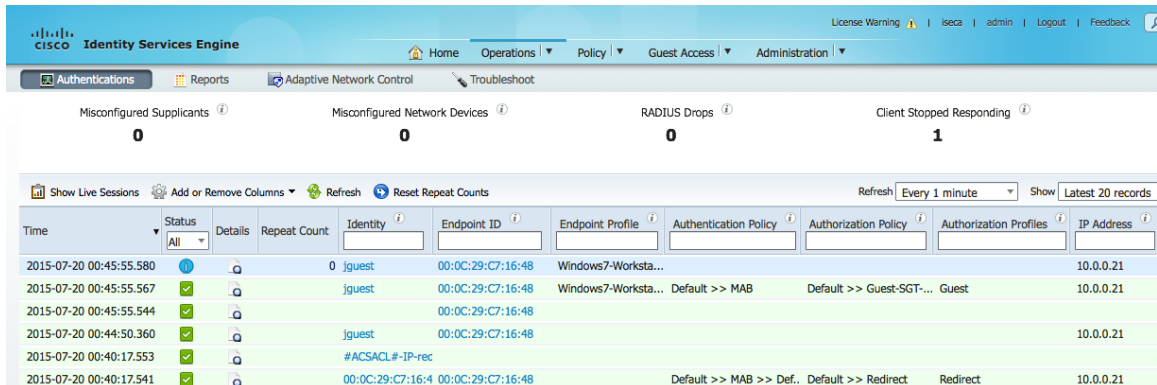
Destination	
URL:	www.box.com
Transaction	
Client or User:	To represent a client by IP address, choose "No authentication or Identification" and enter the IP address below. To represent a user identified through ISE, choose "Identity Services Engine (ISE)" and enter an IP address.
Authentication / Identification:	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	

Step 13 Review the Facebook policy trace as well.

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	
WBSR 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	

Step 14 Select->Operations->Authentication, and note that Guest security group tag has been applied to jguest



The screenshot shows the Cisco Identity Services Engine (ISE) Operations page. At the top, there are navigation tabs for Home, Operations, Policy, Guest Access, and Administration. Below the navigation, there are four summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), and Client Stopped Responding (1). The main content area displays a table of live sessions. The table has columns for Time, Status, Details, Repeat Count, Identity, Endpoint ID, Endpoint Profile, Authentication Policy, Authorization Policy, Authorization Profiles, and IP Address. The table shows several sessions for the identity 'jguest' with a status of 'Success' (green checkmark) and an IP address of 10.0.0.21. The authentication policy is 'Default >> MAB' and the authorization policy is 'Default >> Guest-SGT...'. The authorization profiles are 'Guest'.

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	Success		0	jguest	00:0C:29:C7:16:48	Windows7-Worksta...	Default >> MAB	Default >> Guest-SGT...	Guest	10.0.0.21
2015-07-20 00:45:55.567	Success			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	Success			jguest	00:0C:29:C7:16:48					10.0.0.21
2015-07-20 00:44:50.360	Success			#ACSACL#-IP-rec						10.0.0.21
2015-07-20 00:40:17.553	Success									
2015-07-20 00:40:17.541	Success				00:0C:29:C7:16:4 00:0C:29:C7:16:48		Default >> MAB >> Def.	Default >> Redirect	Redirect	10.0.0.21

Contractor

The Contractor Identification Profile and the Web access policies for Contractor is created. The web access policy is to deny Box access and allow Facebook Access.

Identification Profile and Web Access Policy

Step 1 Select->Web Security Manager->Web Policies->Web Access Policies->and create the Guest Identification Profile by clicking on “Secure Group Tags; No Users Entered” and select the “Guest ” Security Group Tag Name

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 <input type="checkbox"/>
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 <input type="checkbox"/> All <input type="checkbox"/>
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"/>

- Step 2 Click->Done
- Step 3 You will see the following

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

- Step 4 Click on Submit and Commit Changes twice
- Step 5 Under URL Filtering click on "Monitoring"
- Step 6 Block File Transfer Services

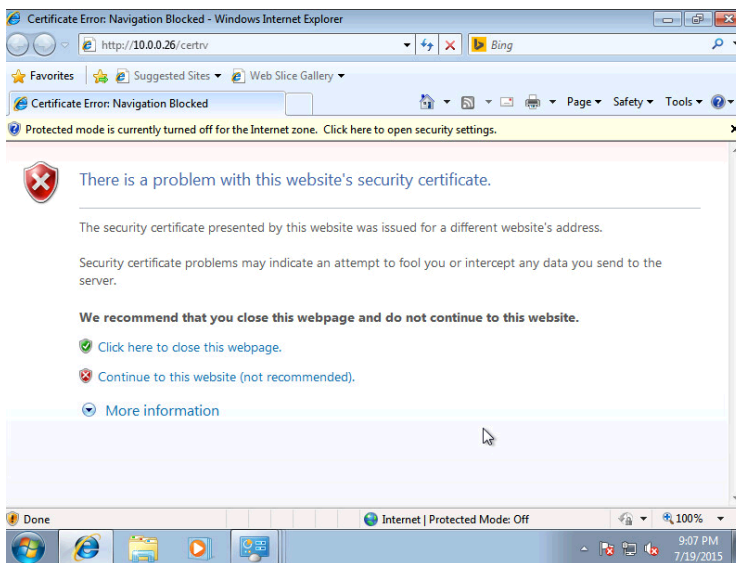
Predefined URL Category Filtering						
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.						
Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn	Quota-Based	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Education	<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"/>	<input checked="" type="checkbox"/>			–	–
Filter Avoidance	<input checked="" type="checkbox"/>				–	–

Step 7 Submit and Commit Changes twice

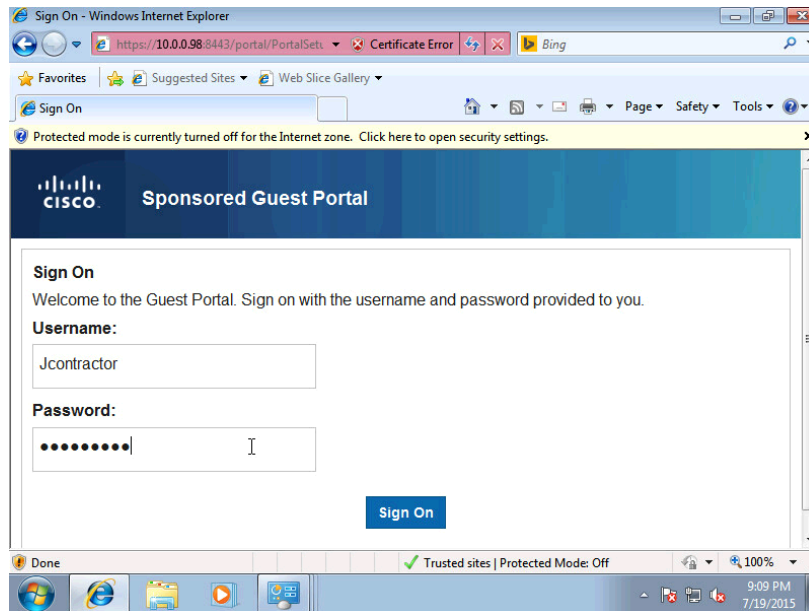
Testing

Step 1 Contractor opens their browser, continues to website

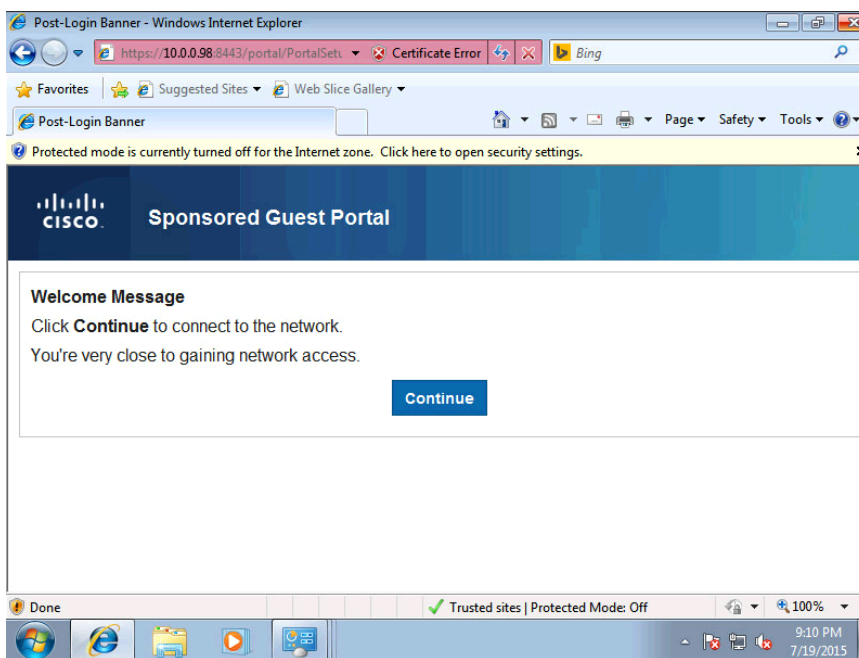
Note: The reason for the certificate error message is the URL is the IP address of the server, if this were the FQDN you would not see this error message.



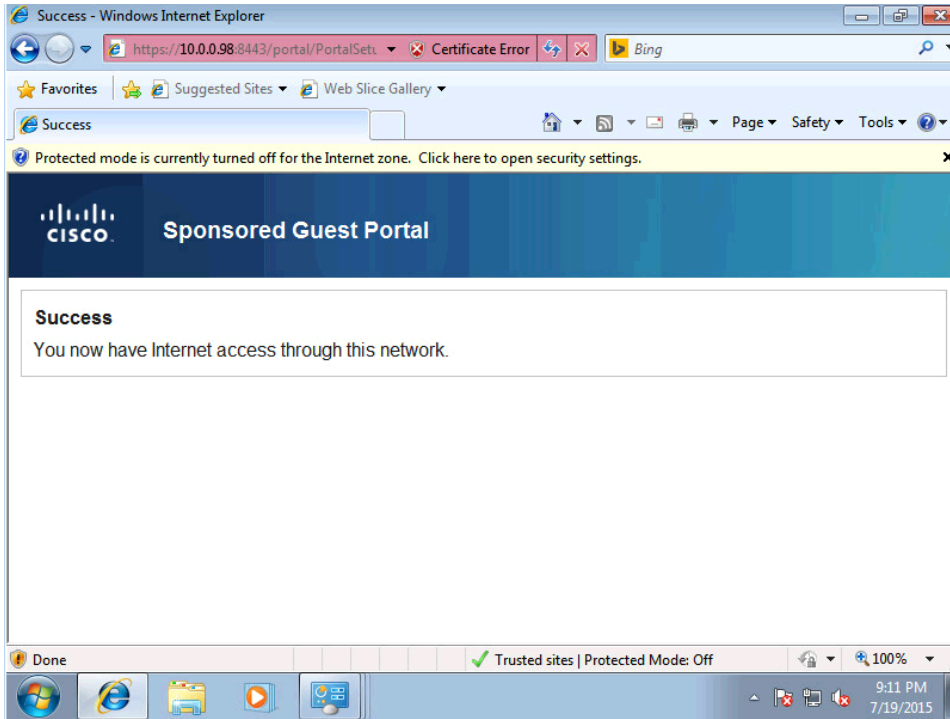
Step 2 Contractor enters their credentials as defined earlier for internal users in ISE



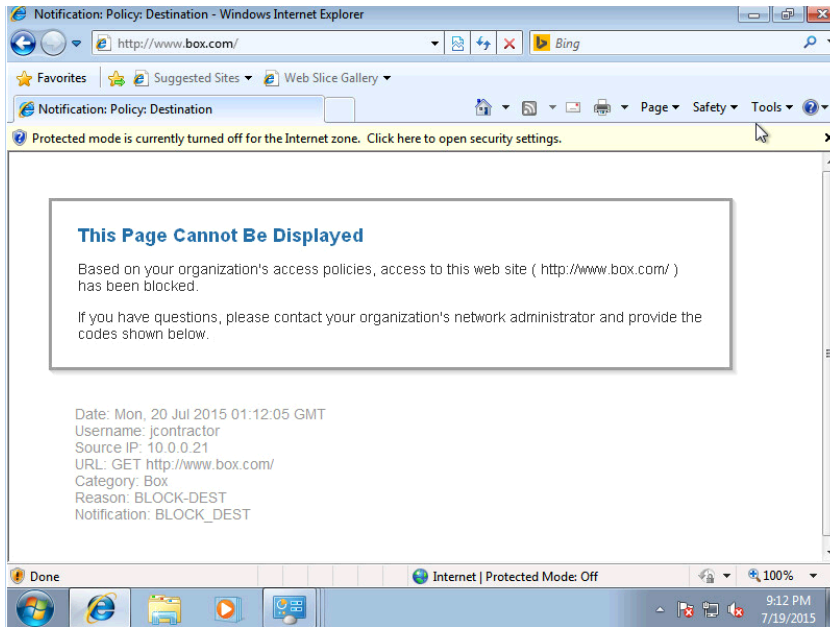
Step 3 Contractor selects continue



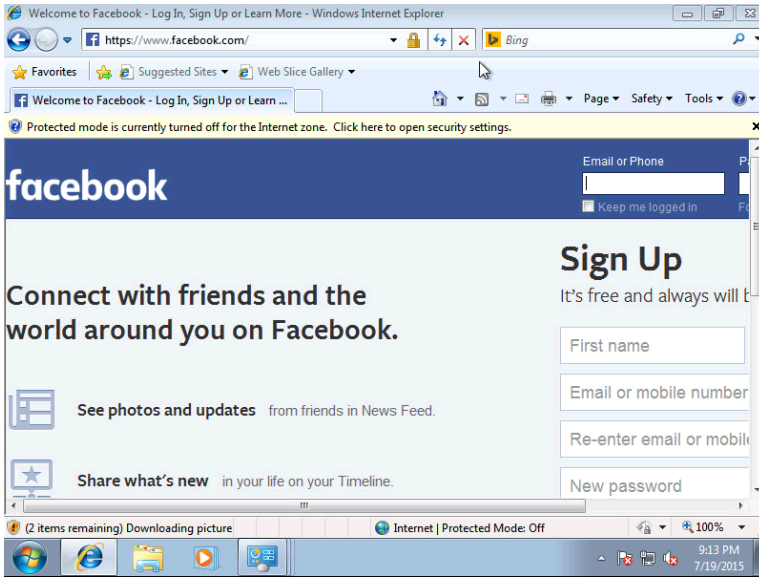
Step 4 Contractor has successfully logged into the Sponsored Guest Portal



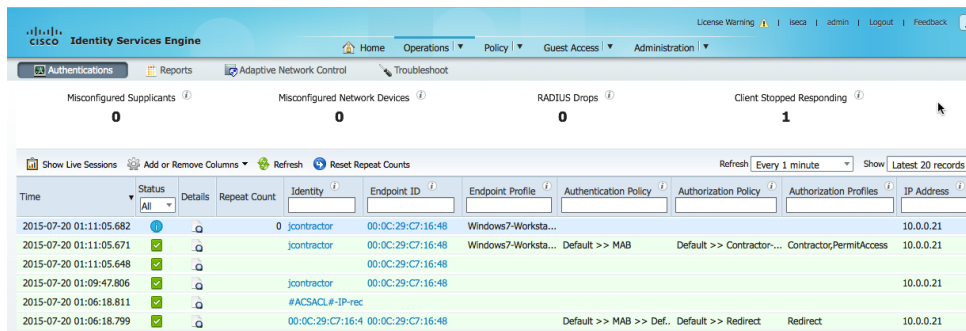
Step 5 Contractor accesses Box.com and is denied



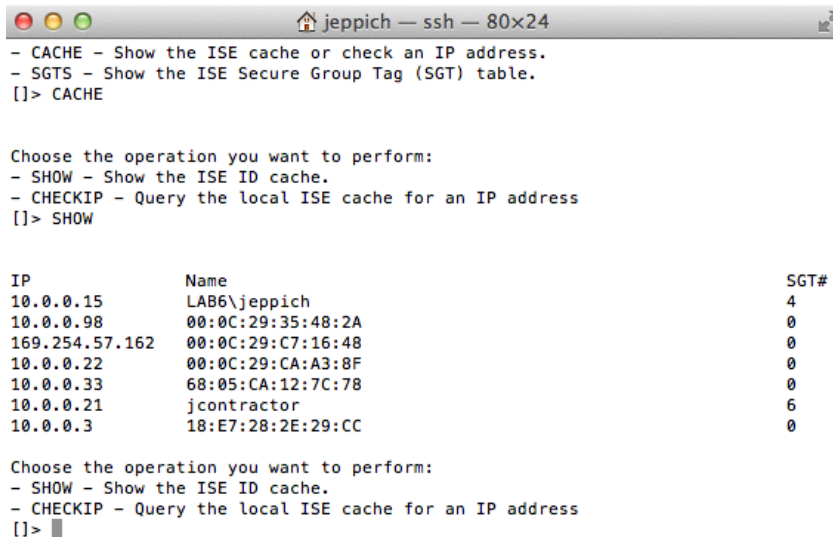
Step 6 Contractor accesses Facebook



Step 7 Select->Operations View in ISE to view that Jcontractor has been assigned a Contractor SGT

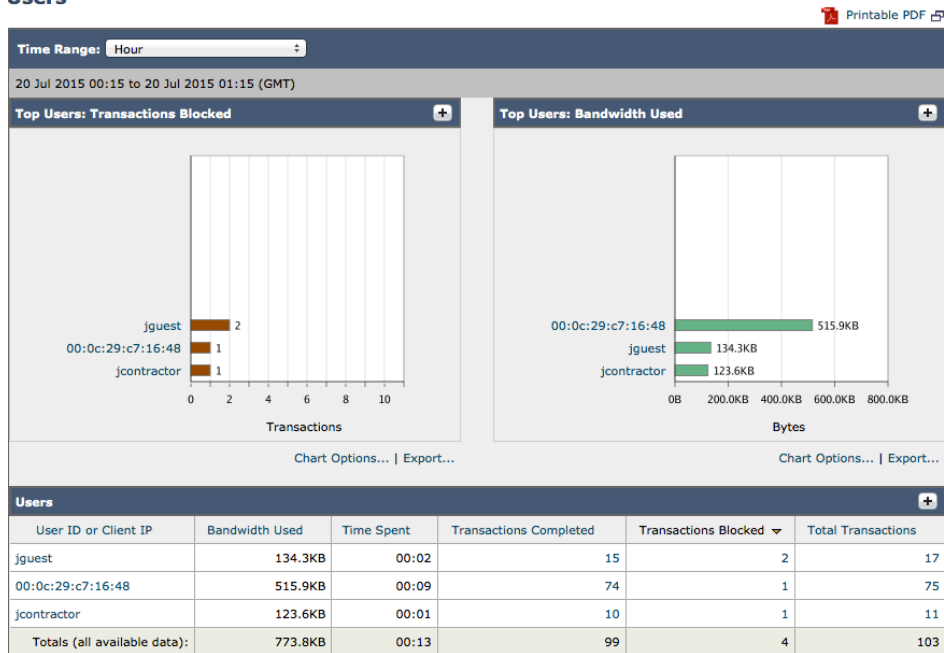


Step 8 On the WSA console, type in “isedata” to view the IP-SGT mappings for jcontractor



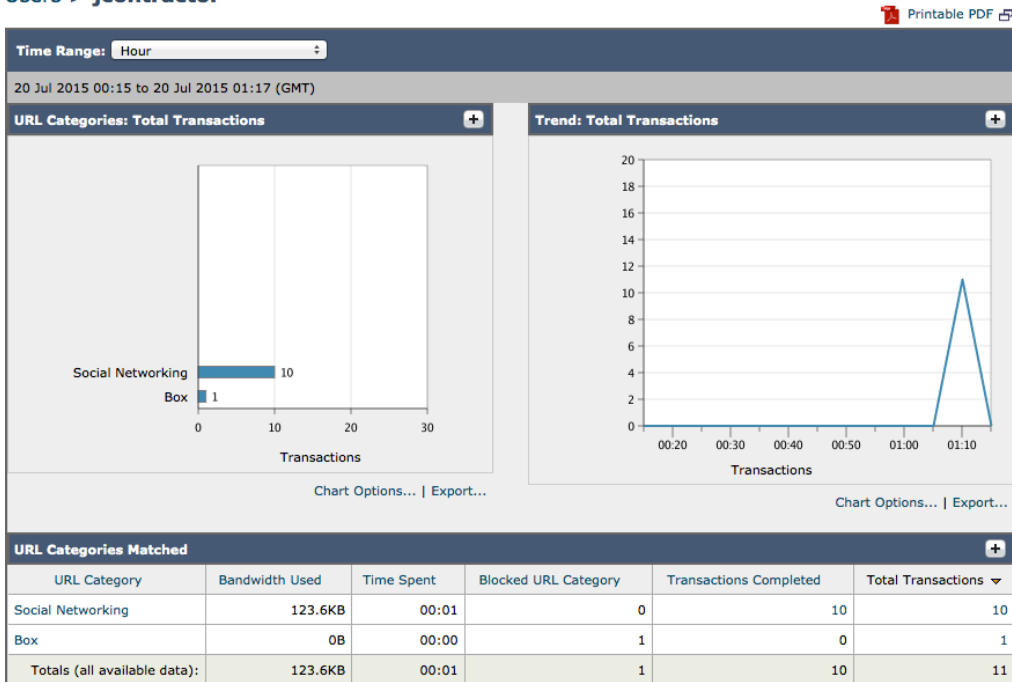
Step 9 On the WSA GUI, select Reports->Users, to view a summary of blocked transactions

Users



Step 10 Select Jcontractor, to view the blocked transactions

Users > jcontractor



Step 11 Notice that box.com has been blocked and Facebook has been allowed

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

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

Step 12 Here is the matched policy for Jcontractor

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

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

Step 13 Select->Administrator->Policy Trace to provide more visibility details on Box

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:

Find Policy Match

Results

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

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

Final Result
Request blocked
Details: Request blocked based on custom URL category
Trace session complete

Step 14 Select->Administrator->Policy Trace to provide more visibility details on Facebook

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:

Find Policy Match

Results**User Information**

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

URL Check

WBSR 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

Troubleshooting

Always use the “tail ise_service_log” on the WSA when configuring the WSA and ISE pxGrid node integration. You will want to verify that you see the following to verify a successful connection:

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

Restful ISE Node Failures

- Resolution: run “tail ise_service_log”. If you see “cannot resolve hostname” errors, verify that all the ISE nodes and the WSA are DNS resolvable.
- If you still see “cannot resolve hostname” errors, and the WSA and the ISE node are DNS resolvable, delete the WSA pxGrid client connection, and restart the WSA. After the WSA restart, verify that you see the WSA subscribed to the SessionDirectory and TrustsecMetadata Capability of the ISE pxGrid node. Run “tail ise_service_log” to verify that you see the download SGT tags. You may also have to reboot the ISE pxGrid node if you still see errors.
- Verify that the CA root certificate is installed for the ISE Monitoring node admin certificate on the WSA for a CA-signed environment.
- Verify that the ISE self-signed certificate is installed for the ISE Monitoring node admin certificate on the WSA for a in an ISE Stand-alone environment if running self-signed certificates.
- The WSA upon initial boot, will use the ISE RESTful API to download bulk session records from the ISE MnT node. The WSA will use the ISE Admin node certificate to query the available ISE MnT nodes.

ISE pxGrid client Connectivity Issues

- In an ISE stand-alone environment, by default, pxGrid node auto registration is disabled. This is fine, make sure the ISE admin approves the pending pxGrid client request. You can change auto registration to enabled to avoid pending requests.

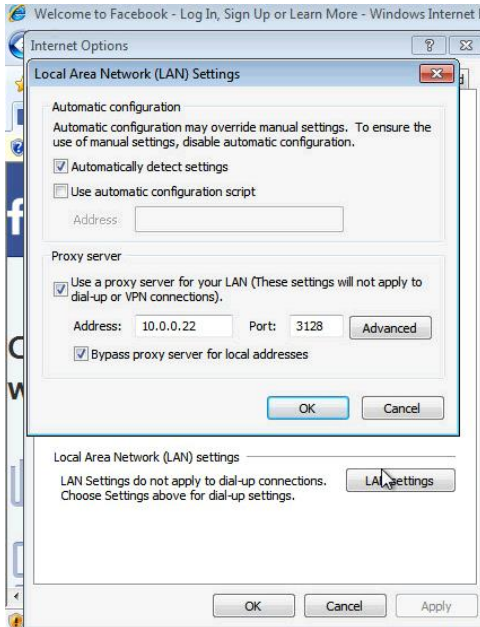
CPU RAM utilization 100% on WSA Virtual

Resolution: run “tail ise_service_logs”. If you see multiple WSA re-starts, increase the CPU to 2, and RAM size to 8 GBs of RAM.

Appendices

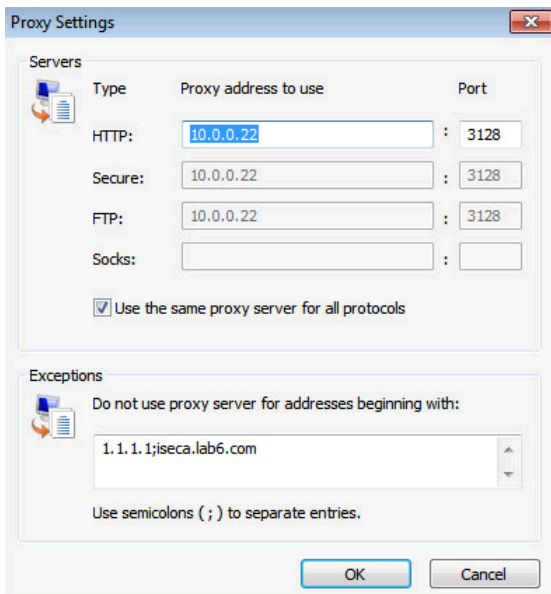
Internet Explorer Proxy Settings

The address and port represent the WSA and port number



The exceptions below represent bypass the WSA proxy settings to allow the redirection to the ISE node for CWA access. The 1.1.1.1 is an IP address which will trigger a redirection to the ISE node, iseca.lab.com.

Note: This will be the IP address of the ISE PSN node in a Distributed ISE Deployment



Switch and redirect ACL Settings for CWA

This will very pending customer deployments, the basics are below and highlighted. A Catalyst 3850 switch was used for this document.

Redirect 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 Switch Settings

Additional settings can be found: http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_sw_cfg.html

```
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)
```

References

How to: Configuring pxGrid in a Distributed ISE Environment:

http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf

Deploying certificates with pxGrid: using self-signed certificates with ISE pxGrid node and pxGrid client:

http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-Self_signed_pxGridClient_selfsigned_pxGrid.pdf

Deploying certificates with pxGrid: using CA-signed ISE pxGrid node and CA- signed pxGrid client:

http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-Self_signed_pxGridClient_selfsigned_pxGrid.pdf