



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	
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	

cisco.

ISE Self-Signed Identity Certificate & ISE pxGrid Configuration	44
WSA and ISE pxGrid node Configuration	
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: <u>http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf</u>

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 he 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 <u>http://www.cisco.com/c/en/us/td/docs/security/ise/1-4/compatibility/ise_sdt.html</u> 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 endusers 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 polices. 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 umber and description

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

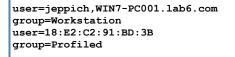
• EndpointProfileMetadata, providing ISE endpoint policy information such as changes/modifications to the ISE profiling policy

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

- 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

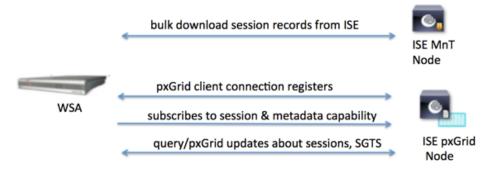
```
session (ip=192.168.1.14, Audit Session Id=0A030103000001E00FEBAD7, User Name=jsmith, Domain=lab4.com,
Calling station id=00:0C:29:77:A8:C7, Session state= STARTED, Epsstatus=null,Security Group=Engineering,
Endpoint Profile=Microsoft-Workstation, NAS IP=192.168.1.2, NAS Port=GigabitEthernet1/0/9, 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.



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. Endusers 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.

SECURE ACCESS HOW-TO GUIDES

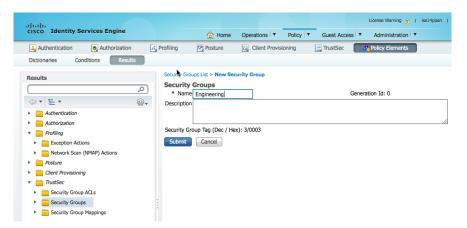


😵 System	A Identity	y Manag	gement	Network	Resources	🛃 Device I	Portal Manageme	ent 🔳	pxGrid Services	Feed Se	ervice	tity Mappir	ng				
lients Liv	e Log											⊖En	able Auto	-Registrat	tion Disa	view By	
Enable ⊘ Disa		oprove	😝 Group	👎 Decline	🔞 Delete 🔻	🛞 Refresh	Total Pending A	pproval(0)	•		1 - 7 of 7	Show	25 * F	per page	Page	1 🔹	of 1
Client Name	e		Clier	nt Description		Capabilities	s		Status		Client Group		Log				
ise-admin-i	se14smnt					Capabilities	s(0 Pub, 0 Sub)		Online		Administrator		View				
ise-mnt-ise	14smnt					Capabilities	s(2 Pub, 0 Sub)		Online		Administrator		View				
ise-admin-is	se14pmnt					Capabilities	s(0 Pub, 0 Sub)		Online		Administrator		View				
ise-mnt-ise	14pmnt					Capabilities	s(2 Pub, 0 Sub)		Online		Administrator		View				
Ise-admin-is	se14ppan					Capabilities	s(2 Pub, 1 Sub)		Online		Administrator		View				
▼ ironport.ex	ample.com-	pxgrid_	client pxGr	rid Connection	from WSA	Capabilities	s(0 Pub, 2 Sub)		Online		Session		View				
	Ca	pability	y Detail							1 - 2 of 2	Show 25 + per page	Page 1	*	of 1			
		Capa	bility Name		Capabili	ty Version		Messaging	Role	Message	e Filter						
	0	Sessi	ionDirectory		1.0			Sub									
	0	Trust	SecMetaData	а	1.0			Sub									

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

ahaha cisco Ide	entity Services Engine	<u>^</u>	Home Operations	Policy V Guest Access		P
💄 Authenti	cation 🥑 Authorization	Profiling 💽 Pos	sture 😡 Client Provisio	ning 📄 TrustSec	🔑 Policy Elements	
Authorizatio	on Policy					
	orization Policy by configuring rules t go to Administration > System >			I drop rules to change the o	order.	
First Matched R		backup & Restore > Policy E	xport rage			
Exception	ıs (0)					
Standard						
Status	Rule Name	Conditions (id	lentity groups and other condit	ions)	Permissions	
	Wireless Black List Default	if Blacklist AN	D Wireless_Access		then Blackhole_Wireless_Access	
	Engineering_Groups	if pxGrid_Users	ExternalGroups EQUALS lab6.	com/Users/Domain Users	then Engineering AND PermitAccess	
	Profiled Cisco IP Phones	if Cisco-IP-Ph	ione		then Cisco_IP_Phones	
	Profiled Non Cisco IP Phones	if Non_Cisco_P	rofiled_Phones		then Non_Cisco_IP_Phones	
	Basic_Authenticated_Access	if Network_Acc	ess_Authentication_Passed		then PermitAccess	
	Default	if no matches, th	en DenyAccess			
Save	eset					

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

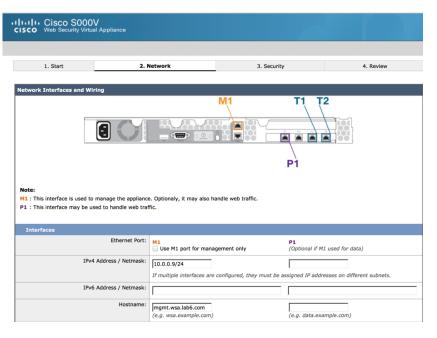
CISCO Web Security Virtual Appliance	•			
1. Start	2.	Network	3. Security	4. Review
System Settings				
Def	ault System Hostname: 🕐	wsa.lab6.com e.g. proxy.company.com		
	DNS Server(s):	Use the Internet's Root DNS Ser Use these DNS Servers: 10.0.0.26 75.75.76.76	(optional) (optional)	
	NTP Server:	time.sco.cisco.com		
	Time Zone:	Region: GMT Off: Country: GMT : Time Zone / GMT Offset: GMT		
Appliance Mode				
Α;	pliance Mode of Operation	Cloud Web Security Connector	n-premise policy enforcement (Standard Web Securit arily to direct traffic to Cisco Cloud Web Security for installation).	

Step 3 Select->Next

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

SCO Web Security Virtual Ap	bliance		
1. Start	2. Network	3. Security	4. Review
etwork Context			
Is there another web proxy in y	our network? o Wizard, you will have the option to define additional		
Proxy Group Name:	o wizaro, you will have the option to denne additional	upstream proxies.	
Address:			
Port:	e.g. 10.1.1.1, 2001:420:80:1::5, example.com		
another web proxy is present, th	e Cisco Web Security Appliance is recommended to be	placed downstream of the existing proxy (cl	oser to the client), as illustrated below
IRONPORT S-SER	LES ANOTHER AND FIREWALL INTERNET		
Prev Cancel			Next

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



- Step 6 Click->Next
- **Step 7** In this document, Simplex TAP is set

Cisco S000V	ppliance		
1. Start	2. Network	3. Security	4. Review
ayer 4 Traffic Monitor Wiring		M1 T1 T	2
in addition, web proxy interfaces	d for the L4 Traffic Monitor. (M1, P1 or P2) may be used for L4TM bloc	king.	
Interfaces	Wiring Type: Duplex TAP: T1 (In/Out) Simplex TAP: T1 (In) and T2 (O	ut)	



Step 9 Enter the network routes

1. Start	2. 1	Network	3. Security	4. Review
IPv4 Routes for Management a	nd Data Traffic	(Interface M1: 10.0.0.9)		
D	efault Gateway:	10.0.0.1 This will be the default route for external	al traffic as well as internal tra	offic with no static route below.
Static Routes Table				
		s to the Cisco Web Security Appliance as w the Secure Web Proxy and optional blocking		on the appliance functions you
Name	Int	ernal Network	Internal Gateway	
	10	0.0.0/24	10.0.0.1	Û
Internal		v4 Address (such as 10.1.1.10) or CIDR	IPv4 Address	
Internal Identifying name for route		uch as 10.1.1.0/24)		

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

```
Note: PC client proxy settings are listed in the Appendices
```

CO Web Security Virtual Appliance			
1. Start	2. Network	3. Security	4. Review
nsparent Connection Settings		st be connected via a Layer 4 switch or WCC	Derester
Transparent Redirection D	Contemporate received and a contemporate received and	irection device is connected, only explicit for service ID: 0 web_cache (port 80) s: Separate multiple addresses with comm er security for this service ssword:	as or whitespace.

Step 11 Enter admin name, password, email address

1. Start	2. 1	Network	3	. Security		4. Review
Iministrative Settings						
Ad	ministrator Password:	Password: Confirm Password:	Must be 6 or more ch	aracters		
E	mail system alerts to:	jeppich@lab.com e.g. admin@compar	ny.com			
Send Email via SMTP Rela	ay Host (optional): 🕐	i.e., smtp.example.	com, 10.0.0.3	Port: ?	optional	
	AutoSupport:	Send system ale	rts and weekly status r	eports to Cisco	o Customer Suppo	rt
SensorBase Network Pa	rticipation					
	Network Participation:	identify and sto Participation Le	vel: Uimited - Su	mmary URL in		rt them to Cisco in order to Ided)

- Step 12 Click->Next
- **Step 13** In this document, all the defaults are set

Veb Security Virtual Appliance			
1. Start 2. 7	Vetwork	3. Security	4. Review
urity Settings			
Global Policy Default Action: 3	 Block all traffic If block all traffic is s 	c elected, the Global Access Policy will be initially PS, FTP over HTTP, and native FTP).	r configured to block all proxied
L4 Traffic Monitor	Action for Suspect Ma	alware Addresses 💿 Monitor only 🕞 Block	
Acceptable Use Controls: (?	Chapter Chapter	licy will be initially configured to monitor all pr	e-defined categories.
Reputation Filtering	Cildble	licy will be initially configured to use Web Repu	itation Filtering and Adaptive
Malware and Spyware Scanning	The Global Access Po actions configured be	Enable McAfee Enable Sophos Iry and Outbound Malware Scanning Policy will fow. ted Malware: Monitor only Block	I be initially configured to apply the
Cisco Data Security Filtering	The Global Cisco Data	a Security Policy will be initially configured to b d) and monitor all other uploads.	lock uploads based on Web

Step 14 Click->Next

Step 15 Review the settings

SECURE ACCESS HOW-TO GUIDES

CISCO SOOOV CISCO Web Security Virtual Appliance			
1. Start 2. N	etwork	3. Security	4. Review
Review Your Configuration			
lease review your configuration. If you need to ma	ke changes, click the	Previous button to return to the previous	Printable Page
Network Settings			Edit
Default System Hostname:	wsa.lab6.com		
DNS Servers:	10.0.0.26, 75.75.76	5.76	
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	1	
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	ve been defined.	
Transparent Connection Settings			Edit
Transparent Redirection Device Type:	Layer 4 Switch or N	o 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

	Web Security Manager	Security Services	Network	System Administrat	ion
Certificate I	Aanagement				
Success - Your	changes have been commit	ted.			
Certificate Lists					
Updates					
File Type		Last Updat		urrent Version	New Update
Cisco Trusted Root		Never Upda		.2	Not Available
Cisco Certificate Bla	ecklist	Never Upd	ated 1	.2	Not Available
Attention - Updates	in progress.				Update
	agement				
Certificate Mar				st	
Certificate Mar	Trust Root Certificates:	380 certificates in Cisco trus 1 custom certificates added		icate list	

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:

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-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 req Request box.

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	MSLUdrmDFsbk820gFzRHRet0At3xuySCYIPVT0TkK7 rDAAcYpOGa1+7bgXNoRjnueA32XP3pOb5ap6Hrt541 207dbnXGd9bblEkzbOKM7y9AVHEJBBEHr8fcfx+Mbvi AZ/X/wpsmnL01E91C88FrjcejHAVh5fGAwf5FMkAhyl 8/x29MNHAguYkoXH5JPMIEOC7H9X3GmRI85HOFt END CERTIFICATE REQUEST		
Certificate Templa	te:		
	pxGrid ¢		
Additional Attribu	tes:		
Attributes:			
Attibutes.			

- Step 1 Select-Submit
- Step 2 Download "base-64"

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

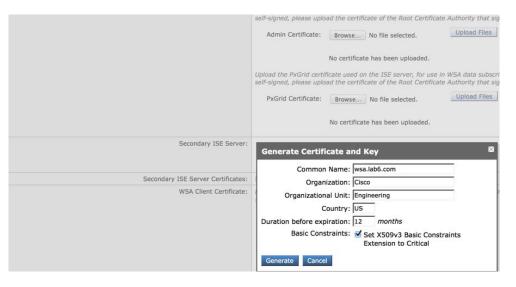
Creating WSA private key and CSR request from WSA (alternative)

Generate WSA CSR for pxGrid operation

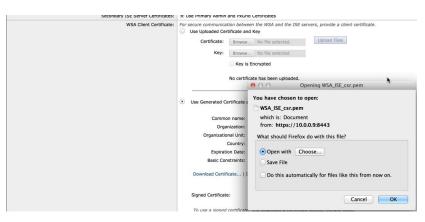
Step 1 Select->Network->Identification Service->Identity Service Engine->Edit Settings->WSA Client Certificate->Generate New Certificate and Key

WSA Client Certificate:	For secure communication between the WSA and the ISE servers, provide a client certificate. Use Uploaded Certificate and Key Certificate: Browse No file selected. Upload Files
	Key: Browse No file selected.
	Key is Encrypted
	No certificate has been uploaded.
	Use Generated Certificate and Key Generate New Certificate and Key
	No certificate has been generated.

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

SECURE ACCESS HOW-TO GUIDES

	00	WSA_ISE_csr.pem		
es	89:4f:55:3d:13:90:ae:e7:f 36:6c:ae:00:20:ac:30:00:7 84:63:9e:e7:80:df:65:cf:d 8f:fe:af:32:13:38:04:2f:c	d:17:ad:d0:0b:77:c6:ec:b9:19: 3:e1:59:88:37:5d:7b:72:8c:e1: 1:8a:4e:19:ad:7e:ed:b8:17:36: e:93:9b:e5:aa:7a:1e:bb:79:e0: 9:c4:5c:19:f2:51:cb:f2:45:d8: 8:49:33:6c:e2:8c:ef:2f:40:bc:		Styles AaBbt AaBbCcDdEc AaBbCcDdEc i. AaBbCcDc evel 1 Step_Level 1 Step_Level 2 Step_Level 3
	e1:54:e0:6a:60:25:2b:00:f 72:ce:d4:4f:75:0b:cf:05:a 07:d2:14:c9:00:87:22:16:3 4c:d4:11:06:68:f3:fc:76:f 28:25:3c:c9:44:38:2e:c6:1	f:1f:8c:6e:f2:d2:a0:94:26:1d: 9:c4:fc:01:9f:d7:ff:0a:6c:9a: e:37:1e:8c:70:15:87:97:c6:03: 1:5a:47:c9:9c:b4:8d:bf:57:76: 4:c3:47:02:0b:98:92:85:c7:21: 1:d2:b7:1a:64:65:f3:91:ce:17:		
MII VQC hki GUC 50a 0b7 dOF DQY M5L	dia:72:c4:33 =BGIN_CERTFLATE_REQUEST— CI_2:CACACADAYS_IELMAKADUEBINCY GUNTF hendpahru (n u.zzFVMBGAUEA IGSVBBACFAA0CADBAYLISIGACADEA IGSVBBACFAA0CADBA	VMXD1AMBgNVBAOTEUNG2XVMRQwEqTD WMG3NHLmNY1jv129tHT1B1AMBgKg BL85001Jv1jAE1tm5V00Ljc5XGsfcT4Y cya8b6/PR2YC+nTd5N03+M00rUSTh16 K11hz21LD524031b0Y1m6doy3NP2+4 DGKx653g5c5fTv0gAwh1KiMRDumn+VX th0ANu6g54JBv1Z3a1Cb1x2xH-31Ny1 Zr8KV1hK5u4Y3d5CcLWxwIDAQABAAM 20009reqs4bBr2MEg+81Acf1ugY241y		altalta cisco.
207 AZ/ 8/x	Act pucat Pucator Number 273 5005 7dbnMcd9bb1Exzb0KM7y9AvHE1BBEHr /X/wpsmnL0193C88EriceiHAVh5fcA x29MNHAguYkoXHISg1PM1E0C7IH9K3G END CERTIFICATE REQUEST	wfSFMkAhyIWMVpHyZy0jb9XdkzUEQZo		In the INSA and the ISS servers, provide a client certificate. Key No. The serverse. No. The serverse. No. The serverse.
207 AZ/ 8/x	7dbnNGd9bbiEkzb0KM7y9AvHEjBBEHr /X/wpsmnL01E91C88FrjcejHAVh5fGA x29MNHAguYkoXHISglPMlE0C7IH9K3G	wfSFMkAhyIWMVpHyZy0jb9XdkzUEQZo	No certi	No file selected. Upload Files.
207 AZ/ 8/x	7dbnNGd9bbiEkzb0KM7y9AvHEjBBEHr /X/wpsmnL01E91C88FrjcejHAVh5fGA x29MNHAguYkoXHISglPMlE0C7IH9K3G	wfSFMkAhyIWMVpHyZy0jb9XdkzUEQZo	Vie entre Use Generated Centhesis Organization Organization Control Regional Centhesis Control	I for The transmission of the second time of the

Step 6 Submit Advanced User request

Submit a Certif	icate Request or Renewal Request	
To submit a sav Request box.	ed request to the CA, paste a base-64-enco	ded CMC or PKCS #10 certificate request or PKCS #7 renewal rec
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	MŠLĮJofmDFsDk&ZogF2RIŤ&t0At3xuySGYIPVŤOTKKŤ rDAAcYpOGa1+7bgXNoRjnueA32XP3pObSap6Hr541 207dbnCdabbiEk2bOKMY9AVHEJBEHTRFCk+Mby AZ/XJwpsmnLO1E91C88FrjcejHAVh5fGAwfSFMkAhyl 8/x29MHAguYkcNHSgJMEGC7HByK3GmRI8SHOF END CERTIFICATE REQUEST	
Certificate Templa	te:	
	pxGrid ÷	
Additional Attribu	tes:	
Attributes:		

Submit >

- **Step 7** Select-Submit
- Step 8 Download "base-64 encoded"



- Step 9 Click->Submit
- **Step 10** Also download the root certificate in "base-64 encoded"

Step 11 Upload the WSA+pxGrid identity certificate



Se opioaded certificate and iter	
Certificate: Browse No file selected. Upload Files	
Key: Browse No file selected.	
Key is Encrypted	
No certificate has been uploaded.	
Use Generated Certificate and Key Generate New 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, uplaad it using the field below.	
Certificate: Browse wsa.cer Upload File	

ISE Service configuration on WSA

Step 1Create 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.

IIII Cise	CO SOOOV Security Virtual Appliance			
Reporting	Web Security Manager	Security Services	Network	System Administration
Edit Log S	ubscription			
Log Subscriptio	on			
	Log Type:	Access Logs		
	Log Name:	accesslogs		
		(will be used to name the log	g directory)	
	Rollover by File Size:	10G Maximum		
		(Add a trailing K or M to indi	cate size units)	
	Rollover by Time:	None ‡		
	Log Style:	• Squid		
		Apache		
		Squid Details		
	Custom Fields (optional):	%m		Custom Fields Reference
	File Name:	aclog		
	Log Compression:	Enable		
	Log Exclusions (Optional):			
		(Enter the HTTP status codes	s of transactions the	at should not be included in the Access Log)
	Retrieval Method:	• FTP on mgmt.wsa.lab6.co	m	
		Maximum	Number of Files:	10
		FTP on Remote Server		-

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 PPAN, 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.

C 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.
	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: Browse No file selected. Upload File
	Common name: lab6-WIN-49T17723UO8-CA
	Organization:
	Organizational Unit:
	Country:
	Expiration Date: May 18 02:38:28 2020 GMT
	Basic Constraints: Critical
	Download Certificate

Uploading secondary pxGrid node certificate

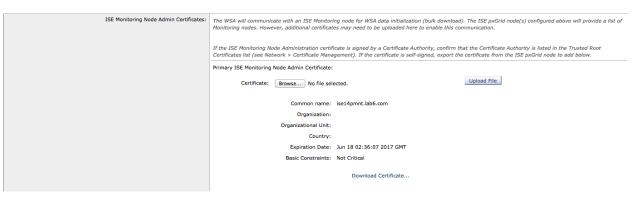
Step 1 Enter the pxGrid2 IP address or FQDN

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 optional.	l node to support WSA data subscription (ongoing u	odates). Specifying a secondary ISE pxGrid node (server) is
			•
	10.0.0.95 (Hostname or IPv4	4 address)	~
	ISE pxGrid Node Certificate:		
		Certificate Authority, confirm that the Certificate A tificate is self-signed, export the certificate from the	uthority is listed in the Trusted Root Certificates list (see ISE pxGrid node to add below.
	Certificate: Browse No file selected	ed. U	pload File
	Common name: lab	b6-WIN-49T17723UO8-CA	
	Organization:		
	Organizational Unit:		
	Country:		
	Expiration Date: Ma	ay 18 02:38:28 2020 GMT	
	Basic Constraints: Cri	itical	
		Download Certificate	

Uploading Primary Monitoring node certificate

Step 1 Upload the Primary MNT public certificate



Uploading Secondary Monitoring node certificate

Step 1 Upload the Secondary MNT public certificate

Secondary ISE Monitoring Node Admin Cert	ificate:	
Certificate: Browse No file sel	ected.	Upload File
Common name:	ise14smnt.lab6.com	
Organization:		
Organizational Unit:		
Country:		
Expiration Date:	Jun 18 02:46:19 2017 GMT	
Basic Constraints:	Not Critical	
	Download Certificate	

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 Use Uploaded Certificate and Key Certificate: Browse No file select	Indeed Eller
	Key: Browse No file selec	red.
	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
		Download Certificate

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: ise14pmnt.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

SECURE ACCESS HOW-TO GUIDES

Enable ISE Service		
Primary ISE pxGrid Node	The WSA will communicate with the ISE pxGrid node to support WSA data subscription (angoing updates). A primary ISE pxGrid node (server) must be configured.	
	10.0.0.93 (Hostname or IPv4 address)	
	· · · · · · · · · · · · · · · · · · ·	
	ISE pxGrid Node Certificate:	
	If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.	
	Certificate: Browse No file selected.	
	Common name: lab6-WIN-49T17723UO8-CA	
	Organization:	
	Organizational Unit:	
	Country: Expiration Date: May 18 02:38:28 2020 GMT	
	Basic Constraints: Critical	
	Download Certificate	
Secondary ISE pxGrid Node (optional): The IVSA will communicate with the JSE pxGrid node to support WSA data subscription (ongoing updates). Specifying a secondary JSE pxGrid node optional.		
	10.0.0.95 (Hostname or IPv4 address)	
	ISE pxGrid Node Certificate:	
	If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.	
	Certificate: Browse No file selected.	
	Common name: lab6-WIN-49T17723UO8-CA	
	Organization:	
	Organizational Unit:	
	Basic Constraints: Critical	
	Download Certificate	
	Organization: Organizational Unit: Country: Expiration Date: May 18 02:38:28 2020 GMT	



Step 2 Select->Commit changes twice

......

CISCO

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

🔆 System	🚰 Iden	tity Ma	anagement	Network	Resources	🛃 Device	Portal Manageme	ent 🔳	👿 pxGrid Services	S Feed Se	ervice	💵 pxGrid Identi	y Mappin	g		
Clients Li	ve Log												⊖Ena	ible Auto-Registr		o-Registi By Capat
Enable ⊘ De	sable 😪	Approv	ve 😝 Group	👎 Decline	😧 Delete 👻	🛞 Refresh	Total Pending A	opproval(0)	•			1 - 7 of 7	Show	25 👻 per page	Page 1 🗘	of 1
Client Nar	ne		Clie	ent Description		Capabilitie	s		Status		Client G	roup		Log		
ise-admin	-ise14smnt					Capabilitie	s(0 Pub, 0 Sub)		Online		Adminis	trator		View		
Ise-mnt-is	e14smnt					Capabilitie	s(2 Pub, 0 Sub)		Online		Adminis	trator		View		
ise-admin	-ise14pmnt					Capabilitie	s(0 Pub, 0 Sub)		Online		Adminis	trator	1	View		
ise-mnt-is	e14pmnt					Capabilitie	s(2 Pub, 0 Sub)		Online		Adminis	trator	1	View		
ise-admin	-ise14ppan					Capabilitie	s(2 Pub, 1 Sub)		Online		Adminis	trator	1	View		
▼ ironport.e	xample.com	m-pxgri	id_client pxG	Grid Connection	from WSA	Capabilitie	s(0 Pub, 2 Sub)		Online		Session		1	View		
	c	Capabi	ility Detail							1 - 2 of 2	Show	25 👻 per page	Page 1	\$ of 1		
		C	apability Name	3	Capabil	ity Version		Messaging	g Role	Message	e Filter					
		O Se	essionDirectory	y	1.0			Sub								
		O Tr	rustSecMetaDa	ita	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	
Senable Identification Profile	
Name: ?	ISE (e.g. my IT Profile)
Description:	
Insert Above:	1 (Global Profile) 🗘
User Identification Method	
Identification and Authentication: ?	Transparently identify users with ISE +
Fallback to Authentication Realm or Guest Privileges: ?	If user information is not available from the Identity Services Engine: Support Guest Privileges +
	Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).
Membership Definition	
Membership is defined by any combination of the f	ollowing options. All criteria must be met for the policy to take effect.
Define Members by Subnet:	10.0.0.0/24 (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)
Define Members by Protocol:	 ✓ HTTP/HTTPS Native FTP
Advanced	Define additional group membership criteria.

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 a	dd Secure Group Tags. To remove Secu	re Group Tags from this policy, use the Delete option.	
0 Secure Group Tag(s) currently inc	luded in this policy.		
Secure Group Tag Name	SGT Number	SGT Description	Delete All
No Secure Group Tags selected.			
			11.
			Delete
Secure Group Tag Search			
	re Creur Tee come sumber es descrit	tion. Select one or more Secure Group Tags from the l	ist and use the
Add button to add to this policy.	re Group Tag name, number, or descrip	tion. Select one or more Secure Group Tags from the li	ist and use the
Search	×		
	, A		
0 Secure Group Tag(s) selected	T TOF Add		Add
Secure Group Tag Name	SGT Number	SGT Description	Select All
Unknown	0	Unknown Security Group	
Engineering	3	NONE	
ASA	2	NONE	
ANY	65535	Any Security Group	

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 Sec Add button to add to this policy.	ure Group Tag name, number, or de	escription. Select one or more Secure Group Tags from the	list and use the
Search	x		
1 Secure Group Tag(s) selecte			Add
Secure Group Tag Name	SGT Number	SGT Description	Select All
Unknown	0	Unknown Security Group	
Engineering	3	NONE	Image: A start and a start
ASA	2	NONE	
ANY	65535	Any Security Group	

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

You should see the following:

tembership is defined by the combination of the following	options. All criteria must be met for the poli	icy to take effect.	
Identification Profiles and Users:	Select One or More Identification Profiles	•	
	Identification Profile	Authorized Users and Groups	Add Identification Profile
	ISE ‡	OAll Authenticated Users	
		 Selected Groups and Users ? ISE Secure Group Tags: Engineering Users: No users entered 	ŵ

- Step 5 Click->Done
- Step 6 Click->Submit
- **Step 7** Under "URL Filtering" select->Global Policy and set to the following:

	Use		0	verride Glob	al Settings	
	Global Settings	Block 3	Monitor	Warn ?	Quota-Based	Time-Based
Category	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
e Real Estate	×				-	-
\varTheta Reference	1				_	_
😔 Religion	✓				-	_
😔 SaaS and B2B	✓				-	-
😔 Safe for Kids	✓				-	-
I Science and Technology	✓				-	-
😔 Search Engines and Portals	✓				-	-
I Sex Education					-	-
I Shopping	✓				-	-
Social Networking		1			-	-
😔 Social Science	 ✓ 				-	-
⊖ Society and Culture	✓				-	-
😝 Software Updates	✓				-	-
😝 Sports and Recreation	✓				-	-
😝 Streaming Audio	✓				-	-
😝 Streaming Video	✓				-	-
😔 Tobacco	1				_	_

- 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

SECURE ACCESS HOW-TO GUIDES

Reporting	Web Security Manager	Security Services	Network	System Administration	
ccess Polic	ies: Applications V	isibility and Co	ntrol: Engin	eering	
dit Applications S	ettings				
Define Application	s Custom Settings ‡				
Applications Settin					
Applications Settin	gs				
Browse Application	Types 🗧				Applications In
Browse Application	plications, inspection of HTTPS c			le the HTTPS Proxy, then selec	
Browse Application				le the HTTPS Proxy, then selec	
Browse Application To identify some ap enables decryption	plications, inspection of HTTPS c	rol (see Security Services >	HTTPS Proxy).	le the HTTPS Proxy, then selec	
Browse Application To identify some ap enables decryption	plications, inspection of HTTPS c for application visibility and cont		HTTPS Proxy).		
Browse Application To identify some ap enables decryption	plications, inspection of HTTPS c for application visibility and cont	rol (see Security Services >	HTTPS Proxy).		
Browse Application To identify some ap enables decryption	plications, inspection of HTTPS c for application visibility and cont	rol (see Security Services >	HTTPS Proxy).		
Browse Application To identify some ap enables decryption A Collaboration	plications, inspection of HTTPS c for application visibility and cont pplications	rol (see Security Services > Edit all Ə 8 Monitor	HTTPS Proxy).		
Browse Application To identify some ap enables decryption A To Collaboration	plications, inspection of HTTPS c for application visibility and cont pplications	edit all B Monitor Edit all G 6 Monitor	HTTPS Proxy).		
Browse Application To identify some ap enables decryption A Collaboration Enterprise App	plications, inspection of HTTPS c for application visibility and cont pplications	rol (see Security Services > Edit all Ə 8 Monitor Edit all	HTTPS Proxy).		
Browse Application To identify some ap enables decryption A Collaboration Enterprise App	plications, inspection of HTTPS c for application visibility and cont pplications	rol (see Security Services > Edit all e 8 Monitor Edit all f 6 Monitor Edit all	HTTPS Proxy).		
Browse Application To identify some ap enables decryption A Collaboration Collaboration	plications, inspection of HTTPS c for application visibility and cont pplications	edit all edit all e 8 Monitor Edit all e 6 Monitor Edit all e 6 Monitor Edit all Bandwidth Limit: No Bandw	HTTPS Proxy).		

Step 11 Click->Submit and Commit Changes twice

You will see the following:

R	leporting	Web Secu	rity Manager	Security Servic	es Ne	twork Sy	stem Administration	
Acce	ss Policies	-						
ACCE	ss Funcies	>						
Succe	ss — Item was	s successfu	lly deleted.					
Policie								
Policie	25							
	Policy	-						
	-		Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delet
Add	Policy			URL Filtering Block: 1 Monitor: 78	Applications Block: 10 Monitor: 368	Objects (global policy)	Anti-Malware and Reputation (global policy)	Delet

......

CISCO.

Create WSA Decryption Application Policy

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

Decryption Policy: DecryptEngine	eering
Policy Settings	
Senable Policy	
Policy Name: 🕐	DecryptEngineering (e.g. my IT policy)
Description:	
Insert Above Policy:	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 follow	ing options. All criter	ia must be met for t	he policy to take effect.	
Identification Profiles and Users:	Select One or Mor	re Identification Prof	iles 🗘	
	Identification Profi	le	Authorized Users and Groups	Add Identification Profile
	ISE	\$	OAll Authenticated Users	
			Selected Groups and Users ? ISE Secure Group Tags: Engineering Users: No users entered	鎆
			Guests (users failing authentication)	
			available at HTTPS connection time. For trans unavailable for decryption policies.	parent
	Use the Advanced of Category), or User		edit membership by proxy port, subnet, Time	Range, destination (URL
	The following advar	nced membership cri	iteria have been defined:	
	Proxy Ports:	None Selected		
	Subnets:	None Selected		
	Time Range:	No Time Range De (see Web Security	finitions Available Manager > Defined Time Ranges)	
	URL Categories:	None Selected		
	User Agents:	None Selected		

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

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

	Use			Override 0	Slobal Settir	ngs	
	Global Settings	Pass Through	Monitor	Decrypt	Drop ?	Quota-Based	Time-Based
Category	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable
Pornography		1				-	-
Professional Networking		v				-	_
Real Estate		1				-	_
Reference		1				-	-
Religion		1				-	-
SaaS and B2B		1				-	-
Safe for Kids		1				-	-
Science and Technology		1				-	-
Search Engines and Portals		√				-	-
Sex Education		1				-	-
Shopping		1				-	-
🕙 Social Networking				1		-	-
Social Science		1				-	-
Society and Culture		 ✓ 				-	-
Software Updates		✓				-	-
Sports and Recreation		1				-	-
G Streaming Audio		1				-	_

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

ĸ	eporting	Web Security Manager	Security Services	Network	System Administration	
Decr	yption P	olicies				
Succe	ss — Item	was successfully deleted.				
Policie						
POLICIE	15					
	Policy		_			
	Policy		URL Filtering	Web Reputation	Default Action	Delete
Add	Policy	Profile: ISE	URL Filtering Pass Through: 77 Monitor: 1 Decrypt: 1	Web Reputation	Default Action	Delete



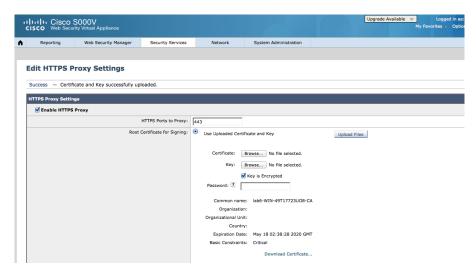
Application Decryption

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.

•	IIII Cisco	S000V urity Virtual Appliance	Upgrade Available Upgrade Available Upgrade Available.com My Favorites - Options - Support and Help						
	Reporting	Web Security Manager	Security Services	Network	System Administration				
									No Changes Providing
E	dit HTTPS I	Proxy Settings							
1	ITTPS Proxy Setti	nos							
1	Enable HTTP								
			HTTPS Ports to Proxy:	443					
		Root	Certificate for Signing:	Use Uploaded C	ertificate and Key	Upload Files			
				Certificate:					
				Kev:	Browse rootcert.cer Browse rootkey.cer				
					Key is Encrypted				
				Password: ?					
					as been uploaded.				
				No ceroncate n	as been uploaded.				

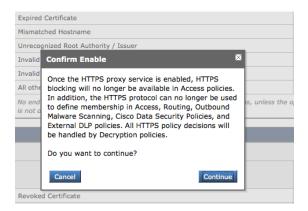
Step 5 Select->Upload Files, you should see they have been successfully uploaded



Step 6 Under "Decrypt for Application Detection", enable "Enable decryption for enhanced application visibility..."

Decryption Options				
Decrypt for Authentication: (?)	Senable decryption for authentication			
	If the user has not been authenticated prior to the HTTPS transaction, the request will be denied if not decrypted.			
Decrypt for End-User Notification: ⑦	Search and the second s			
	Decryption is necessary to display an end-user notification page in the event of a policy block.			
Decrypt for End-User Acknowledgement: ?	Seable decryption for display of the end-user acknowledgement page			
	If the user has not acknowledged the web proxy prior to the HTTPS transaction, the acknowledgement page cannot be di the request will be denied.			
Decrypt for Application Detection: ?	Search and the second application visibility and control			
	Enabling this option will improve the efficacy of detection for some HTTPS applications. However, fecryption may cause ot unless the root certificate for signing is installed on the client.			
Invalid Certificate Options				

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



- Step 8Click 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 Certif	icate:					
	Common name: lab6-WIN-49T17723UO8-CA						
	Organization:						
	Organizational Unit:						
	Country:						
	Expiration Date:	May 18 02:38:28 202	0 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				
	N	lismatched Hostname:	Monitor				
	Unrecognized I	Root Authority / Issuer	Drop				
	Inv	alid Signing Certificate	Drop				
		Invalid Leaf Certificate	Drop				
		All other error types:	Drop				

Obtaining root public/private key pair

Step 1Backup 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

Certification Authority (Local)\\ah6-WIN-49T17723U08-CA1	×						
Select a Password							
E This password is required to gain access to the private key and the CA certificate file.	This password is required to gain access to the private key and the CA certificate file.						
Password:							
Confirm password:							
To maintain private key security, do not share your password.							
< Back Next > Cancel Help							

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

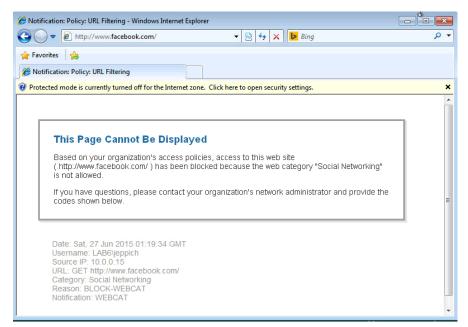
openssl pkcs12 -in lab6-WIN-49T17723U08-CA.p12 -clcerts -nokeys -out rootcert.cer Enter Import Password: MAC verified OK

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 <u>https://facebook.com</u> in browser. Internet Explorer proxy settings can be found in the Appendices.

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



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

🟉 Notification: Policy	URL Filtering - Windows Internet Explorer		
😋 🔾 🗢 🙋 http	os://facebook.com/	🚹 🗟 😽 🗙 🕨 Bing	+ ۹
🔶 Favorites 🛛 🚖	Website Identification	×	
Protected mode is	lab6-WIN-49T17723UO8-CA has identified this site as:	o open security settings.	×
	facebook.com		- î
	This connection to the server is encrypted.		_
This P	Should I trust this site?		
Based or	View certificates	to this web site (https://facebook.com/)	
has beer	DIOCREA DECADO INE WED CALEGOLY OUC	- Networking" is not allowed.	
	/e questions, please contact your organiz: own below	ation's network administrator and provide the	
codes si	Swir Below.		=
Username Source IF URL: GET Category Reason: I	, 27 Jun 2015 00:33:47 GMT :: LAB6\jeppich : 10.0.0.15 Thttps://facebook.com/ : Social Networking BLOCK-WEBCAT in: WEBCAT		
		17	
		- 🍡 📷	8:15 PM

SECURE ACCESS HOW-TO GUIDES



Step 3 On the virtual WSA, type:

isedata
CACHE
isedata CACHE SHOW

🖉 WSAv on ucs2.lab	5.com	
File View VM		
🔳 🔢 🕨 🤻		
	eration you want to perform:	
	- Show the ISE server status and ISE statistics.	
	w the ISE cache or check an IP address. the ISE Secure Group Tag (SGT) table.	
[]> CACHE	the 13£ Secure droup ray (301) table.	
	eration you want to perform:	
	the ISE ID cache.	
	uery the local ISE cache for an IP address	
[]> SHOM		
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
	68:05:CA:12:7C:78	0
10.0.0.3	18:E7:28:2E:29:CB	0
Choose the en	eration you want to perform:	
	the ISE ID cache.	
	uery the local ISE cache for an IP address	
[]>		

Note the SG-IP mapping for the authenticated user

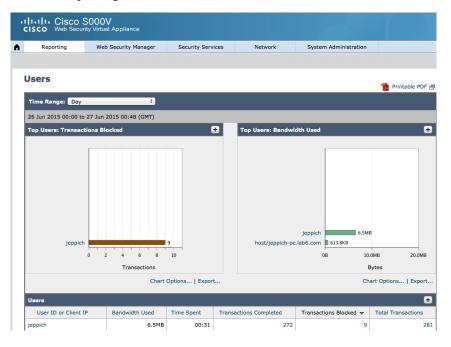
Isedata provides ISE operational statistics on downloaded tags and provide a display of IP-SGT username mappings



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

Reporting	Web Security Manager	Security Services	Network	System Administra	tion	
Web Tracking						
Web Hacking						
Search						
Proxy Services	L4 Traffic Monitor SOCK	S Proxy				
Available: 24 Jun 201	15 03:48 to 27 Jun 2015 00:37	(GMT +00:00)				
	Time Range:	Day	\$			
	User/Client IPv4 or IPv6: ?	LAB6\jeppich (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:			r 2001:420:80:1::5	
	Website:	[(e.g. google.com)		
	Transaction Type:	Blocked ‡				
	Advanced	Search transactions usin	ng advanced criteria.			
Clear						Search
Generated: 27 Jun 2015	01-02 (CMT)					Printable Downl
Results	01:02 (GMT)					
Displaying 1 - 8 of 8 ite	ume					
		te (count)	Display All Details	Disposition	Bandwidth	User / Client IP
Time (GMT +00:00) 27 Jun 2015 00:33:47	https://facebook.com:44	3		Block - URL Cat	OB	jeppich 10.0.0.

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

Reporting	Web Security Manager	Security Services	Network	System Administration	
olicy Trace					
estination					
	URL:	https://facebook.com			
ransaction					
ransaction	Client or User:		resent a user identii	authentication or Identification" ied through ISE, choose "Identit	
ransaction	Client or User:	the IP address below. To rep	resent a user identii ss.		
fransaction	Client or User:	the IP address below. To rep (ISE)" and enter an IP addre	resent a user identii ss. ation: Identity Se	ied through ISE, choose "Identit	

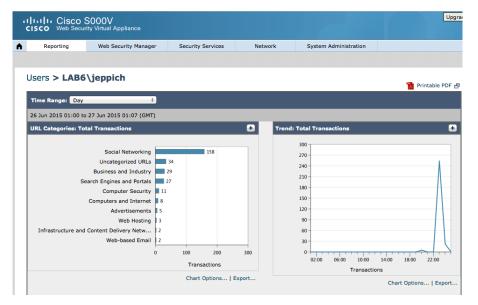
You should see the following policy trace

Note the Decryption Policy and the Access policy

Results	Results					
User Information						
User Name: None Authentication Realm Group Membership: None Secure Group Tag Membership: Engineering User-Agent: Mozilla/S.0 (Macintosh; Intel Mac OS X 10.8; rv:38.0) Gecko/20100101 Firefox/38.0						
URL Check						
WBRS 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



				Iten	ns 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	21
Computer Security	19.1KB	00:00	0	11	11
Computers and Internet	125.0KB	00:01	0	8	ε
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

				I	tems Displayed 10 +
Domain or IP	Bandwidth Used	Time Spent 1	Fransactions Completed	Transactions Blocked	Total Transactions 🔻
akamaihd.net	4.5MB	00:10	117	0	11
facebook.com	323.4KB	00:10	33	8	4
10.0.26	351.8KB 00:05		34	0	3
doubleverify.com	109.0KB 00:00		10	0	1
live.com	196.7KB	00:00	10	0	1
omniroot.com	21.9KB 00:00		9	0	
yimg.com	591.2KB	00:00	8	0	
digicert.com	7,352B	00:00	6	0	1
yahoo.com	128.6KB	00:00	6	0	1
google.com	10,130B	00:00	5	0	
	Find Domain or IP				Columns Export
Applications Matched					æ
Application	Application Type	Bandwidth Used	Transactions Completed	Other Blocked Transactions	Total Transactions 🗢
Facebook General	Facebook	4.8MB	150	C	15
Outlook.com	Webmail	88.5KB	5	C)
Windows Update	Software Updates	6728	1	C	
Totals (all available da	ta):	4.9MB	156	C	15

the sala mas round in the selecti	ted time range				
Malware Threats Detected					
No data was found in the select	ed time range				
Policies Matched					+
Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions 🗢
DefaultGroup	Decryption	3.1MB	111	0	111
	Decryption Access	3.1MB 367.5KB	111 65	0	
Engineering					74
Engineering Engineering	Access	367.5KB	65	9	74
Engineering Engineering ExemptEngineering	Access Decryption	367.5KB 2.0MB	65	9 0	74 61 28
Engineering Engineering ExemptEngineering DefaultGroup	Access Decryption Decryption	367.5KB 2.0MB 1.0MB	65 61 28	9 0 0	74 61 28
DefaultGroup Engineering Engineering ExemptEngineering DefaultGroup DecryptEngineering Totals (all available data):	Access Decryption Decryption Access Decryption	367.5KB 2.0MB 1.0MB 54.5KB	65 61 28 6	9 0 0	111 74 61 26 6 6 1 28

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 standalone 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

cisco Identity Services Engine	License Warning 🚖 ise14 admin
CISCO Identity Services Engine	Home Operations ▼ Policy ▼ Guest Access ▼ Administration ▼
System 🏾 🌺 Identity Management	📷 Network Resources 🛛 🛃 Device Portal Management 🕞 pxGrid Services 🕞 Feed Service 💵 pxGrid Ide
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	System Certificates 🔺 For disaster recovery it is recommended to export certificate and private key pairs of all system certificate
Overview	Edit Generate Self Signed Certificate Finport Export X Delete P View
System Certificates	Friendly Name Used By Portal group tag Issued To Issued By Fise14 Export Certificate 'Default self-signed server certificate'
Endpoint Certificates	Defa certit
Trusted Certificates	Export Certificate and Private Key
OCSP Client Profile	*Private Key Password
Certificate Signing Requests	*Confirm Password Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.
Certificate Authority	Export Cancel

- **Step 2** Save the defaultsignedservercerti.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

cisco

dialia cisco Identity Services Engine	Administration ▼ Policy ▼ Guest Access ▼ Administration ▼
🔆 System 🏾 👰 Identity Management	🎬 Network Resources 🛛 🛃 Device Portal Management 🕞 pxGrid Services 🕞 Feed Service 💵 🔩 pxGrid Identity Mappir
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	Import a new Certificate into the Certificate Store
Overview	* Certificate File Browse ise14.pem Friendly Name
System Certificates	Trusted For: ()
Endpoint Certificates	✓ Trust for authentication within ISE
	Trust for client authentication and Syslog
Trusted Certificates	Trust for authentication of Cisco Services
OCSP Client Profile	Validate Certificate Extensions
Certificate Signing Requests	Description
Costilianto Authority	Submit Cancel

Step 4 Click->Submit

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

սիսիս	License Warning 👔 ise14 admin Logout Fr
CISCO Identity Services Engine	Home Operations Policy Guest Access Administration Administration
System 🏼 🐉 Identity Management	Network Resources 🛃 Device Portal Management 🗒 pxGrid Services 📓 Feed Service 🔩 pxGrid Identity Mapping
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Deployment ↓ F + Deployment ↓ PAN Failover	General Settings Profiling Configuration Hostname ise14 FQDN ise14.ia96.com FP Address 100.0.21 Node Type Identity Services Engine (ISE) Personas Administration Role STANDALONE Make Primary Monitoring Role PRIMARY • Other Monitoring Node Policy Service Enable Session Services 0 Include Node in Node Group None • 0
	Include Hode In Hode Biology Reviee

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

cisco Ider	ntity Services Engin			<u>(</u>) H	Home Oper	rations V Policy V	Guest Access	Administration V		
🔆 System	Identity Manage	ement	Network	Resources	🛃 Device I	Portal Management	pxGrid Services	Feed Service	2 pxGrid Identity	Mapping
										Disable Au
										- Disable rv
Clients	Live Log									
		😝 Group	👎 Decline	🐼 Delete 👻	🛞 Refresh	Total Pending Approval(0)) •		1 - 2 of 2	Show 25 +
	Disable 😪 Approve	-	Decline Description	🐼 Delete 👻	Refresh Capabilities		I) 👻 Status	Client G		
/ Enable ⊘	Disable 😪 Approve ame	-		🛞 Delete 👻	Capabilities			Client G Adminis	roup	Show 25 ¥

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

Reporting	Web Security Manager	Security Services	Network	System Administration	
Reporting	web security Manager	Security Services	Network	System Administration	
Annago Truc	ted Root Certifica	toc			
nallaye mus		les			
Custom Trusted Ro	ot Certificates				
Custom Trusted Ro Import	ot Certificates				
Import		they (TTTPC sites/ size is			
Import Trusted root certifica	tes are used to determine whet			sted based on their chain of cert this list in order to trust certific	
Import Trusted root certifica authorities. Certifica	tes are used to determine whet			sted based on their chain of cert this list in order to trust certifica	
Import Trusted root certifica authorities. Certifica	ites are used to determine whet tes imported here are added to	the trusted root certificate		this list in order to trust certifica	
Import Trusted root certifica authorities. Certifica signing authorities n Certificate	ites are used to determine whet tes imported here are added to	the trusted root certificate Expiration Date	list. Add certificates to	this list in order to trust certification On Cisco List	Delete
Import Trusted root certifica authorities. Certifica signing authorities n	ites are used to determine whet tes imported here are added to	the trusted root certificate	list. Add certificates to	this list in order to trust certifica	ates with

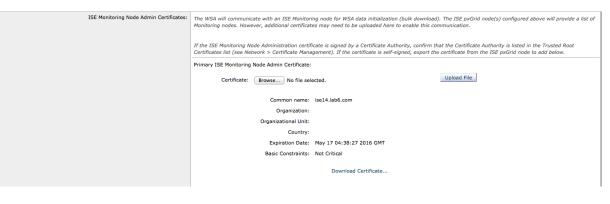
Step 2Upload ISE Identity Certificate pem file to the WSA
Select->Network->Identification Services->Identity Services Engine->Enable ISE Service, provide the
ISE+pxGrid IP address or FQDN->upload the ISE identity certificate

Edit Identity Services Engine Settings	
C Enable ISE Service	
Primary ISE pxGrid Node:	The WSA will communicate with the ISE pxGrid node to support WSA data subscription (ongoing updates). A primary ISE pxGrid node (server) must be configured.
	10.0.0.21 (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: Browse No file selected. Upload File
	Common name: ise14.lab6.com
	Organization:
	Organizational Unit:
	Country:
	Expiration Date: May 17 04:38:27 2016 GMT
	Basic Constraints: Not Critical
	Download Certificate

Step 3 Leave the secondary ISE+pxGrid node blank

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

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



Step 5 Leave the secondary MNT node blank

Secondary ISE Monitoring Node Admin Certificate:	
Certificate: Browse No file selected.	Upload File
No certificate has been uploaded. If a secondary ISE Monitoring nod 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

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: Browse No file selected. Upload Files
Key: Browse 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
Download Certificate
Use Generated Certificate and Key Generate New 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:		
Primary ISE Server Certificates:	Admin Certificate:	
	Common name:	ise14.lab6.com
	Organization:	
	Organizational Unit:	
	Country:	
		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 configur	red
Secondary ISE Server Certificates:	Use Primary Admin a	nd PxGrid Certificates
WSA Client Certificate:	Using Uploaded Certif	ficate:
	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



System Aldentity Management	🖬 Network Resources 🛛 🔣 Device Portal Management 🗔 pxGrid Services 🗔 Feed Service 💵 pxGrid Identity Mapp
Deployment Licensing Certificat	
Certificate Management	Import a new Certificate into the Certificate Store
Overview	* Certificate File Browse wsa_self.cer Friendly Name
System Certificates	Trusted For: ()
Endpoint Certificates	Trust for authentication within ISE
Trusted Certificates	Trust for client authentication and Syslog Trust for authentication of Cisco Services
OCSP Client Profile	Validate Certificate Extensions
Certificate Signing Requests	Description
Certificate Authority	Submit Cancel

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

	IIIII Cisco S Cisco Web Securi					
٨	Reporting	Web Security Manager	Security Service	s Network	System Administration	
	HTTPS Proxy					
	HTTPS Proxy Setting	IS				
		HTTPS Proxy:	Enabled			
		HTTPS Ports to Proxy:	443			
	Root Cert	ificate and Key for Signing:	Using Uploaded Certif	icate:		
			Common name:			
			Organization:	Internet Widgits Pty Lt	d	
			Organizational Unit:			
			Country:	AU		
			Expiration Date:	Jun 26 19:56:00 2016	GMT	
			Basic Constraints:	Not Critical		

Step 12 Enable decryption for enhanced visibility and security

Decrypt for Application Detection: ?	Enable decryption for enhanced application visibility and control
	Enabling this option will improve the efficacy of detection for some HTTPS applications. However, decryption may cause other HTTPS applications to fail unless the root certificate for signing is installed on the client.

- Step 13 Click->Submit->
- **Step 14** You should see the following

ITTPS 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	
OCSP Result Handling:	Revoked Certificate: Drop
	Unknown Certificate: Monitor
	OCSP 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 and 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

ababa						License Warning 🔥	ise14 admin Logout	Feedback	
cisco Identity Services E	Engine	🛕 Hon	ne Operations 🔻	Policy 🔻 Gues	t Access 🔻 Administr	ation 🔻			Setup Assistan
Authentications	eports 🛛 🔯 A	daptive Network Control	💊 Troubleshoot						
Misconfigured Supplicant	its (i)	Misconfigured Network	Devices (i)	RADIU	IS Drops (1)	Client Stopp	ed Responding (i)	Re	peat Counter ①
0		0		0)		0		4
		. <u>A</u>				Defeat a	charles - Charles		
Show Live Sessions Add or	Details Repeat	Televille ()		Endpoint Profile	Authentication Policy	Refresh Every	1 minute Show L Authorization Profiles	Network Device	within Last 24 hours
Status	Details Repeat	Televille ()	indpoint ID	Endpoint Profile ()	Authentication Policy ()				within Last 24 hours Device Port
Time Status	Details Repeat	t Count	indpoint ID () E B:E7:28:2E:29:CC C	üsco-Device			Authorization Profiles (1)		
Time Status All 2015-06-30 12:44:43.820	Details Repeat	t Count Identity () E 0 18:E7:28:2E:29:C 18 18:E7:28:2E:29:C 18	indpoint ID () E 3:E7:28:2E:29:CC C 3:E7:28:2E:29:CC C	üsco-Device		Authorization Policy	Authorization Profiles (1)	Network Device	Device Port

Step 2 User enters their proxy information proxy information

ial-up and Virtual Private Network settings		en security settings.
	Add	Local Area Network (LAN) Settings
	Add VPN	Automatic configuration
	Remove	Automatic configuration may override manual settings. To ensu use of manual settings, disable automatic configuration.
Choose Settings if you need to configure a proxy server for a connection.	Settings	Automatically detect settings Use automatic configuration script
Never dial a connection		Address
 Dial whenever a network connection is not pro Always dial my default connection 	esent	Proxy server
Current None	Set default	Use a proxy server for your LAN (These settings will not app dial-up or VPN connections).
ocal Area Network (LAN) settings		Address: 10.0.0.7 Port: 3128 Advan
LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.	LAN settings	Bypass proxy server for local addresses

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

6 Notification: Policy: U	JRL Filtering - Windows Internet Explorer		
🚱 🔾 🗢 🙋 https	://facebook.com/ 👻 🔒	🗟 😽 🗙 🕨 Bing	+ ۹
🔶 Favorites 🛛 👍	x Website Identification		
Protected mode is	Internet Widgits Pty Ltd has identified this site as: facebook.com This connection to the server is encrypted. Should I trust this site?	o open security settings.	×
		to this web site (https://facebook.com/) Networking" is not allowed. on's network administrator and provide the	ш
Username: Source IP: URL: GET Category:	https://facebook.com/ Social Networking LOCK-WEBCAT		

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

alialo						License V	Warning 🔥 iseca admin	Logout Feedback	
cisco Identity Services Engine	<u> </u>	Home Operations	Policy	Guest	Access 🔻 🖌	Administration			Setup Assistant
🔆 System 🛛 💆 Identity Management	Network Resources	🛃 Device Portal Ma	anagement	😡 pxGri	d Services	Feed Service	💵 pxGrid Identity Mappi	ng	
Identities Groups External Identity Sou	urces Identity Sourc	e Sequences Se	ttings						k
Identities Network Access Users									
	🖊 Edit 🕂 Add	🔃 Change Status 👻	Import	🔁 Export 👻	🗙 Delete 🔻	Duplicate		Show All	*
	Status	Name 🔺 I	Description		First Name	Last Name	Email Address	User Identity Groups	Admin
	🗌 🗹 Enabled	👤 JContractor			Joe	Contractor	jcontractor@lab6.com	GuestType_Contractor (default)	
Endpoints Latest Manual Network Scan Results	🗌 🧧 Enabled	👤 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

CISCO Sponsored Guest Portal
Sign On Welcome to the Guest Portal. Sign on with the username and password provided to you.
Username:
JGuest
Password:
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

cisco Identity Ser			<u>ا</u> ش	Home Operations	Policy G	uest Access	Administration 🔻	
Authentications	Peports	Adaptive I	Network Control	💊 Troubleshoot				
Misconfigured S	Supplicants (i)	r	Misconfigured Netwo	ork Devices (i)	RAL	DIUS Drops (i)		Client Stop
0			0			0		
Show Live Sessions	Add or Remov	e Columns 🔻 🛞 Re	efresh 💿 Reset Re	peat Counts			F	efresh Every
Show Live Sessions 1								
-	Status All T	ails Repeat Count	Identity ()	Endpoint ID	Endpoint Profile	Authentication	Policy i Authorizati	on Policy 🕐
ime 2015-07-19 17:32:56.175	All 🔻 Det	ails Repeat Count	Identity (i)	Endpoint ID	Endpoint Profile	Authentication	Policy (i) Authorizati	on Policy (i)

Step 9 Follow the same procedure for tesing 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.

SECURE ACCESS HOW-TO GUIDES



սիսիս						Lice	nse Warni
cisco Identity Services Engine	企	Home Opera	ations 🛛 🔻	Policy 🛛 🔻	Guest Access	Administration	
🛃 Authentication 🛛 👩 Authorization	Profiling 💽 Pos	sture 🗔 C	Client Provisio	ning [TrustSec	🔒 Policy Elements	
Dictionaries Conditions Results							
Results ↓ <th>Downloadable ACL Lis Downloadable ACL Lis * Name re Description</th> <th>ACL</th> <th></th> <th></th> <th></th> <th>Ť</th> <th></th>	Downloadable ACL Lis Downloadable ACL Lis * Name re Description	ACL				Ť	
	* DACL Content	2 permit 3 permit 4 permit 5 permit	udp any a icmp any t tcp any t udp any t tcp any a tcp any a	any host 10.0 host 10.0 any eq 80	.0.98	1	

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 Profiles	> Redirect
Authorization F	Profile
* Name	Redirect
Description	
* Access Type	ACCESS_ACCEPT T
Service Template	
▼ Common Ta	sks
JACL Name	redirect
Common Task voice Domain Pe	-
Web Redirection	(CWA, MDM, NSP, CPP)
Centralized We	Act REDIRECT Value Sponsored Guest Portal (defau -
Display Cer	rtificates Renewal Message
Static IP/H	ost name 10.0.0.98
Auto Cmart Dort	

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

	սիս								License Warning 🔥 iseca admin Lo
	sco Ide	ntity Services Engine		🟠 Home	Operations •	Policy	Guest Access	Adm	inistration 💌
2	Authentic	ation	🛃 Profiling	💽 Posture	😡 Client Prov	isioning	🚍 TrustSec	🔒 Policy	Elements
Auth	orizatio	n Policy							
		rization Policy by configuring rules				and drop rule	s to change the orde	r.	
		go to Administration > System >	Backup & Restore >	Policy Export Page	2				
First	Matched Ru	Ile Applies 🔻							
►E	xception	s (0)							
St	andard								
	Status	Rule Name	Cond	ditions (identity gro	ups and other cor	nditions)		1	Permissions
		Wireless Black List Default	if Bla	cklist AND Wireles	s_Access			then	Blackhole_Wireless_Access
	~	Profiled Cisco IP Phones	if Cis	co-IP-Phone				then	Cisco_IP_Phones
		Profiled Non Cisco IP Phones	if Non	_Cisco_Profiled_Ph	ones			then	Non_Cisco_IP_Phones
	 Image: A start of the start of	Employee-SGT-Rule	if pxG	rid_Users:External	Groups EQUALS la	b6.com/User	/Domain Users	then	Employee
1	 Image: A set of the set of the	Contractor-SGT-Rule		estType_Contract		D IdentityGro	up:Name	then	Contractor AND PermitAccess
		Guest-SGT-Rule		stType_Daily (de	efault) AND Iden	tityGroup:Na	ne CONTAINS	then	Guest AND PermitAccess
		Redirect	if Wire	ed_MAB				then	Redirect
		Basic_Authenticated_Access	if Net	work_Access_Authe	entication_Passed			then	PermitAccess
	~	Default	if no ma	tches, then De	nyAccess				

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 ad	d Secure Group Tags. To remove Secu	re Group Tags from this policy, use the Delete option.	
		e oroup rugs nom ans policy, use the belete option.	
1 Secure Group Tag(s) currently inclu	uded in this policy.		
Secure Group Tag Name	SGT Number	SGT Description	Delete All
Employee	4	NONE	
			Delete
			Delete
Secure Group Tag Search			
Enter any text to search for a Secur	e Group Tag name, number, or descrip	tion. Select one or more Secure Group Tags from the list and use	the
Add button to add to this policy.	e oroup rug name, number, or descrip	tion. Sciect one of more Secure Group rags from the list and as	, the
Search	×		
-			
0 Secure Group Tag(s) selected	for Add		Add
			O de la cel
Secure Group Tag Name	SGT Number	SGT Description	Select
Secure Group Tag Name		SGT Description	AII
Unknown	0	Unknown Security Group	
Engineering	3	_NONE_	
ASA	2	NONE	
Guest	5	NONE	
Employee	4	NONE	
Contractor	6	NONE	
ANY	65535	Any Security Group	
(ALL)	00000	ring becang bloch	

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

SECURE ACCESS HOW-TO GUIDES

Policy Settings			
🗹 Enable Policy			
Policy Name: ?	Employee		
	(e.g. my IT policy)		
Description:			
Insert Above Policy:	2 (Guest) ‡		
Policy Member Definition			
Membership is defined by the combination of the following	options. All criteria must be met for the p	olicy to take effect.	
Identification Profiles and Users:	Select One or More Identification Profil	es 🗘	
	Identification Profile	Authorized Users and Groups	Add Identification Profile
	ISE ÷	OAll Authenticated Users	
		•Selected Groups and Users ? ISE Secure Group Tags: Employee Users: No users entered Guests (users failing authentication)	â

- **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

<u>Note:</u> A custom defined URL category for <u>www.box.com</u> 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

These URL Categories are defined as group membership criteria. Al		ble for this	,			
	Use		0	verride Glob	al Settings	
	Global Settings	Block	Monitor	Warn ?	Quota-Based	Time-Based
Category	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
😔 Search Engines and Portals	✓				-	-
I Sex Education	1				-	-
😔 Shopping	1				_	_
3 Social Networking		1			-	_
😔 Social Science	1				-	-

- **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

Applications Settings Browse Application Types	Applications Info 🗗
To identify some applications, inspect	 tion of HTTPS content may be required. For best efficacy, enable the HTTPS Proxy, then select the option that ibility and control (see Security Services > HTTPS Proxy).
Applications	Settings
MPEG	😝 Use Global (Monitor); Bandwidth Limit
Netflix	Set action for application Netflix Use Global Setting (Monitor); Bandwidth Limit Monitor Block Bandwidth Limit: Use Setting from Type (5 kbps) No Bandwidth Limit Cancel Apply

- 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)	Ŵ
---	---	-----------------	-------------------------	--	-----------------	-----------------	---

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

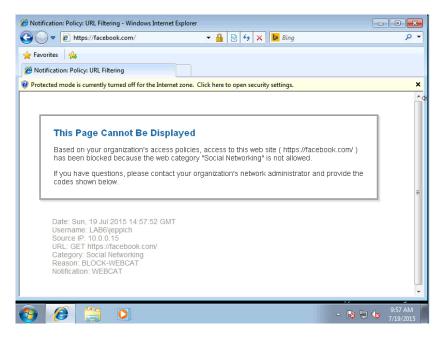
isco	Cisco S Web Secur	ity Virtual Appliance				
R	eporting	Web Security Manager	Security Services	Network	System Administration	
Decr	yption P	olicies				
Policie						
	1					
Add	Policy					
_			URL Filtering	Web Reputation	Default Action	Delete
Order	Group		ORETHREINIG	web Reputation	Deladic Action	Delete
Order 1	Group Employee Identification 1 tag (Employ		Monitor: 79 Decrypt: 1	(global policy)	(global policy)	Delete

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

C Netflix - Watch TV Shows Online, Watch Movies Online - Windows Internet Explorer	
CO V Inttps://www.netflix.com/ V A Integration Bing	+ م
🖕 Favorites 🛛 🖕	
O Netflix - Watch TV Shows Online, Watch Movies	
😢 Protected mode is currently turned off for the Internet zone. Click here to open security settings.	×
NETFLI	Sign In
	*
 (a) (b) (c) (c)	← 💽 🐏 🏎 10:03 AM 7/19/2015

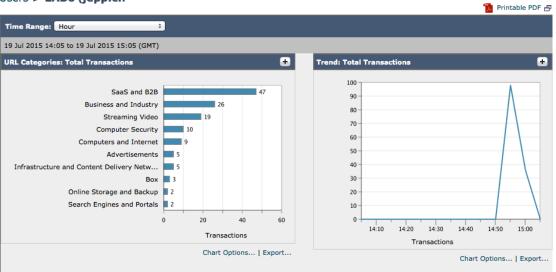
Step 4 "ISEDATA" is run on the WSA to obtain the SGT-IP mappings for employee LAB6\jeppich

```
- 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
                                                                                 SGT#
IP
                  Name
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
                  18:E7:28:2E:29:CC
10.0.0.3
                                                                                  Ø
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							🏗 Printable PDF 🗗
Time Range: Hour	\$						
19 Jul 2015 14:05 to 19 Jul 2	015 15:04 (GMT)						
Top Users: Transactions Bl	ocked		+ Top User	rs: Bandwie	dth Used		Ð
jcontractor jeppich 0	3 3 2 4 6 8 Transactions Chart	0 0 0 0 0 0 0	t	jeppi jcontract	or 56.2KB	0.0MB Bytes Ch	20.0MB art Options Export
Users							÷
User ID or Client IP	Bandwidth Used	Time Spent	Transactions Com	pleted	Transactions Bloc	ked 🔻	Total Transactions
jcontractor	56.2KB	00:03		9		3	12
jeppich	1.9MB	00:04		131		3	134
Totals (all available data):	2.0MB	00:07		140		6	146
[Find User ID or C	lient IP				Columns Export

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

SECURE ACCESS HOW-TO GUIDES

cisco.

				Iten	ns Displayed 10 🗘
URL Category	Bandwidth Used	Time Spent	Blocked URL Category	Transactions Completed	Total Transactions 🔻
SaaS and B2B	921.1KB	00:00	0	47	4
Business and Industry	123.7KB	00:00	0	26	2
Streaming Video	734.6KB	00:02	0	19	1
Computer Security	13.8KB	00:00	0	10	1
Computers and Internet	49.7KB	00:00	0	9	
Advertisements	7,559B	00:00	0	5	!
Infrastructure and Content Delivery Netw	4,218B	00:00	0	4	!
Box	26.0KB	00:00	0	3	
Online Storage and Backup	4,297B	00:00	0	2	:
Search Engines and Portals	55.2KB	00:00	0	2	:
Totals (all available data)	: 1.9MB	00:04	2	131	134
Find URL Category		•			Columns Export
pplications 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	OB	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 Protecti	on Threats Detected	4			÷
No data was found in the sele	ected time range				
Malware Threats Detected					
No data was found in the sele	ected time range				
Policies Matched					÷

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 P	olicy Name				Columns Export

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

Destination	
URL:	www.netflix.com
Transaction	
Client or User:	To represent a client by IP address, choose "No authentication or Identification" and enter the IP address below. To represent a user identified through ISE, choose "Identity Services Engine (ISE)" and enter an IP address.
	Authentication / Identification: Identity Services Engine (ISE) +
	Client IP Address: 10.0.0.15
	User Name:
Advanced	
	Find Policy Match
Results	
User Information	
User Name: None Authentication Realm Group Membership: None Secure Group Tag Membership: Employee User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS	X 10.8; rv:39.0) Gecko/20100101 Firefox/39.0
URL Check	
WBRS Score: 6.9 URL Category: Streaming Video Scanner "AVC' Verdict (Request): Netflix (Media) Scanner "Webroat" Verdict (Request): Unknown MINE-Type: text/html;charset=UTF-8 Object Size: 0 bytes	
Policy Match	
Cisco Data Security policy: None Decryption policy: None Routing policy: Global Routing Policy Identification Profile: ISE Access policy: Employee	

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

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: Client IP Address: User Name:
▶ 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 WBRS Score: 5.3 URL Category: Online Storage and Backup Scanner TWVC Verdict (Request): Box.net (File Sharing) Custom URL Category: Box Scanner TWVC 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: 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:	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: 10.0.0.15 User Name:
▶ Advanced	
	Cancel
User Information User Name: None Authentication Realm Group Membership: None Secure Group Tag Membership: Employee User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS) URL Check WBRS Score: 5.5 URL Category: Social Networking Groups MURT Medit (Menueth, Second Com	
Scanner "AVC" Verdict (Request): Facebook Genera Policy Match	a (racebook)
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

cisco Identity Services E	ngine	<u> А</u> н	ome Operations 🔻	Policy V Gues	st Access 🔻 Administr	ation	
Authentications	oorts 🛛 🔯 Ada	aptive Network Control	💊 Troubleshoot				
Misconfigured Supplicants	5 (I)	Misconfigured Netwo	rk Devices (i)	RADIL	JS Drops (i)	Client Stopped Respondin	ng (i)
0		0		c)	0	
I Changling Consists - Standard	Denner Celeman -	🙆 Defection 👩 Decet De	and Causta			Bofeech France 1 minute	- Chau Latart 20 arreste
Show Live Sessions 🙀 Add or I	Remove Columns 🔻		_	_	_	Refresh Every 1 minute	Show Latest 20 records
Status	Details Repeat	Televille (i)		Endpoint Profile	Authentication Policy	Refresh Every 1 minute Authorization Policy	
ne V Status	Details Repeat	Count Identity	Endpoint ID	Endpoint Profile () VMWare-Device	Authentication Policy		
ne Status	Details Repeat	Count Identity () 0 LAB6\jeppich	Endpoint ID () 00:0C:29:79:02:A8	VMWare-Device			

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 1Select->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 ad	d Secure Group Tags. To remove Secur	e Group Tags from this policy, use the Delete option.	
1 Secure Group Tag(s) currently inclu	uded in this policy.		
Secure Group Tag Name	SGT Number	SGT Description	Delete All
Guest	5	NONE	
			Delete
Add button to add to this policy.		tion. Select one or more Secure Group Tags from the list and use	e the
Enter any text to search for a Secur	e Group Tag name, number, or descrip x	tion. Select one or more Secure Group Tags from the list and use	e the
Enter any text to search for a Secur Add button to add to this policy.	x	tion. Select one or more Secure Group Tags from the list and use	e the Add
Enter any text to search for a Secur Add button to add to this policy. Search	x	tion. Select one or more Secure Group Tags from the list and use SGT Description	
Enter any text to search for a Secur Add button to add to this policy. Search O Secure Group Tag(s) selected	x for Add		Add
Enter any text to search for a Secure Add button to add to this policy. Search O Secure Group Tag(s) selected Secure Group Tag Name	x for Add SGT Number	SGT Description	Add Select All
Enter any text to search for a Secure Add button to add to this policy. Search O Secure Group Tag(s) selected Secure Group Tag Name Unknown	x for Add SGT Number 0	SGT Description Unknown Security Group	Add Select All
Enter any text to search for a Secure Add button to add to this policy. Search O Secure Group Tag(s) selected Secure Group Tag Name Unknown Engineering	x for Add SGT Number 0 3	SGT Description Unknown Security GroupNONENONENONENONE	Add Select All
Enter any text to search for a Secure Add button to add to this policy. Search O Secure Group Tag(s) selected Secure Group Tag Name Unknown Engineering ASA	x for Add SGT Number 0 3 2	SGT Description Unknown Security GroupNONENONE	Add Select All
Enter any text to search for a Secure Add button to add to this policy. Search O Secure Group Tag(s) selected Secure Group Tag Name Unknown Engineering ASA Guest	x for Add SGT Number 0 3 2 5	SGT Description Unknown Security GroupNONENONENONENONE	Add Select All

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 Identification Profiles and Users:	options. All criteria must be met for the po	-			
	Identification Profile	Authorized Users and Groups	Add Identification Profile		
	ISE ÷	All Authenticated Users Selected Groups and Users ISE Secure Group Tags: Guest Users: No users entered Guests (users failing authentication)	ŝ		

- 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.

	Use					
	Global Settings	Block 3	Monitor	Warn ?	Quota-Based	Time-Based
Category	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
😔 Education	1				_	_
😌 Entertainment	1				_	_
😔 Extreme	1				_	_
😝 Fashion	1				_	_
3 File Transfer Services		1			_	_
😔 Filter Avoidance	1				-	-

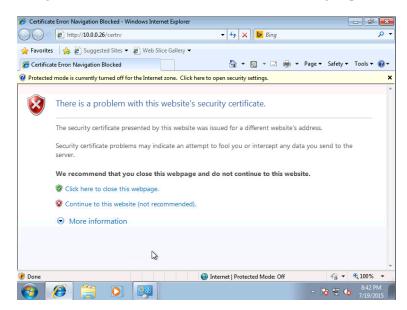
- **Step 7** Set the BOX URL policy as monitoring or allow
- **Step 8** Submit and Commit Changes twice

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 is 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 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

🏉 Sign On - Windows Internet Explorer	
🚱 🕞 🗢 🙋 https://10.0.098/8443/portal/PortalSett 👻 😵 Certificate Error 🐇 🔀 Bing	۹ م
🖕 Favorites 🛛 🚔 🔊 Suggested Sites 🔻 🖉 Web Slice Gallery 💌	
🎉 Sign On 🎒 🔻 🖾 🔻 Page 🔻 Safety 🕯	🕶 Tools 👻 🔞 👻
😢 Protected mode is currently turned off for the Internet zone. Click here to open security settings.	>
cisco. Sponsored Guest Portal	
Sign On Welcome to the Guest Portal. Sign on with the username and password provided to you. Username: jguest	E
Password:	
Sign On	
🖲 Done 🗸 Trusted sites Protected Mode: Off	🔍 100% 🛛 🗸
🚱 🙆 📜 🔍 🐖	8:44 PM 7/19/2015

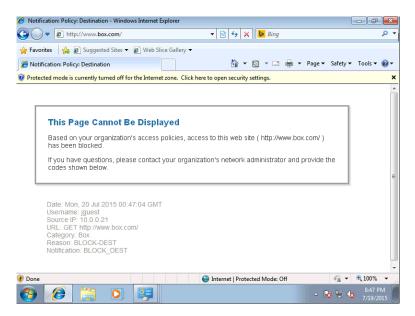
Step 3 Select Continue

🥔 Post-Login Banner - Windows Internet Explorer	
😋 🕞 🗢 😰 https://10.0.0.98:8443/portal/PortalSett 👻 Certificate Error 🍫 🗙 🕨 Bing	+ م
🖕 Favorites 🛛 🚔 🔊 Suggested Sites 🔻 🖉 Web Slice Gallery 👻	
🏉 Post-Login Banner 🎒 🔻 🖾 🖷 🖛 🔻 Page 🔻 Safety 🕶	Tools 🔻 🔞 🕶
Protected mode is currently turned off for the Internet zone. Click here to open security settings.	×
cisco. Sponsored Guest Portal	
Welcome Message Click Continue to connect to the network. You're very close to gaining network access.	
	2
🕐 Done 🗸 Trusted sites Protected Mode: Off 🦿 🍕 🔻	🔍 100% 🔻 🔤
🚱 🧭 📜 🖳 🔍 🚝 🔹 🕫	8:44 PM 7/19/2015

Step 4 Jguest has logged on successfully

🕖 Success - Windows Internet Explorer		
😋 🔵 🗢 😰 https://10.0.0.98:8443/portal/PortalSett 🔻 😵 Certi	ficate Error 😽 🗙 🕨 Bing	+ م
🖕 Favorites 🛛 🖕 🔊 Suggested Sites 👻 🔊 Web Slice Gallery 💌		
Success	🏠 🔻 📓 👻 🖃 🖶 🔻 Page 🕶	Safety 🔻 Tools 🔻 🔞 🕶
Protected mode is currently turned off for the Internet zone. Click h	ere to open security settings.	×
داندان Cisco. Sponsored Guest Portal		
Success You now have Internet access through this network.		
		3
🖲 Done	✓ Trusted sites Protected Mode: Off	🖓 🕶 🔍 100% 💌 🚊
🚱 🥖 🚞 💽 👺	<u>~</u> [8:46 PM 7/19/2015

Step 5 Box.com has been denied



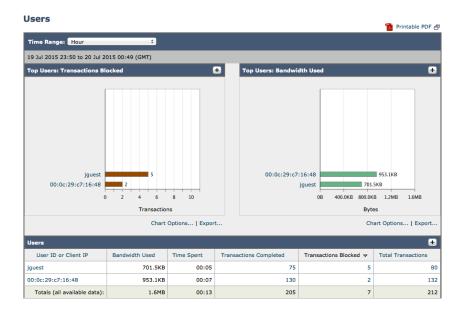
Step 6 Facebook has been allowed



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.
                                                                                                      Ŧ
[]> 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
                                                                                                SGT#
TP
                      Name
                     LAB6\jeppich
00:0C:29:35:48:2A
10.0.0.15
                                                                                                4
10.0.0.98
                                                                                                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
                                                                                                Ø
10.0.0.21
                      jguest
                                                                                                5
                      18:E7:28:2E:29:CC
10.0.0.3
                                                                                                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

Time Range: Hour	÷				
19 Jul 2015 23:50 to 20 Jul 20	15 00:51 (GMT)				
URL Categories: Total Trans	actions	(Trend: Total Tra	nsactions	Ð
Social Networkin Bo Online Storage and Backu SaaS and B2 URL Categories Matched	x 5 p 1 1 b 1 0 20 40 Transa	74 60 80 ctions Options Expor	70 - 63 - 56 - 49 - 42 - 33 - 28 - 21 - 14 - 7 - 0	23.55 00.05 00.15 00.2 Transactions Ch	s 0035 0045 art Options Export
URL Category	Bandwidth Used	Time Spent	Blocked URL Category	Transactions Completed	Total Transactions 🔻
Social Networking	702.0KB	00:01	0	74	7
Box	0B	00:04	5	0	
Online Storage and Backup	1,625B	00:00	0	1	
SaaS and B2B	849B	00:00	0	1	

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

Domains Matched					
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
	Find Domain or IP				Columns Export

Step 11 The application matches provide more visibility

Applications Matched										
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					
Fir	nd Application	Find Application Columns Export								

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 "Identify Services Engine (ISE)" and enter an IP address.					
	Authentication / Identification: Identity Services Engine (ISE)					
	Client IP Address: 10.0.0.21					
	User Name:					
▶ Advanced						
	Find Policy Match					
User Information User Name: None Authentication Realm Group Membership: None Secure Group Tag Membership: Guest User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS Custom URL Category: Box	5 X 10.8; rv:39.0) Gecko/20100101 Firefox/39.0					
Policy Match Cisco Data Security policy: None Decryption policy: None Routing policy: None Identification Profile: ISE Access policy: Guest						
Final Result						
Final Result						
Request blocked						
Request blocked Details: Request blocked based on custom URL ca	stegory					

Step 13 Review the Facebook policy trace as well.

Destination	
URL:	www.facebook.com
ransaction	
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: Io.o.21 User Name:
Advanced	Find Policy Match
Results	
User Name: None Authentication Realm Group Membership: 1 Secure Group Tag Membership: Guest User-Agent: Mozilla/5.0 (Macintosh; Intel N URL Check WBRS Score: 5.5 URL Category: Social Networking Scanner "Webroot" Verdict (Request): Unk Scanner "AVC" Verdict (Request): Facebool MIME-Type: text/hmi Object Size: 0 bytes Scanner "AVC" Verdict (Response): Faceboo Policy Match	4ac OS X 10.8; rv:39.0) Gecko/20100101 Firefox/39.0 nown k General (Facebook)
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	
made session complete	

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

رابیان cisco Identity Se					Operations 🛛 🔻	Policy V Gue	est Access 🛛 🔻 Adminis	License Warning 🛕 I	iseca (admin (Logou	it Feedback
Authentications Misconfigured	Eupplicants		Adaptive Network	c Control 🛛 💊 T gured Network Devic O	roubleshoot res (i)		IUS Drops (1)	Client Stop	ped Responding (i)	
Show Live Sessions	Status		-	-	<u> </u>	Endpoint Profile	Authentication Policy	Refresh Every Authorization Policy	1 minute Show Authorization Profiles	Latest 20 records
	▼ Status		Identi	ity T Endpoi	nt ID	Endpoint Profile () Windows7-Worksta	Authentication Policy			
Time	Status All V	Details	Repeat Count	Endpoi	nt ID () 9:C7:16:48				Authorization Profiles (i	IP Address
Time 2015-07-20 00:45:55.580	Status All V	Details	Repeat Count Identi	ity Endpoi t 00:0C:2 t 00:0C:2	nt ID () 9:C7:16:48	Windows7-Worksta		Authorization Policy	Authorization Profiles (i	IP Address (1) 10.0.0.21
Time 2015-07-20 00:45:55.580 2015-07-20 00:45:55.567	Status All V	Details	Repeat Count Identi	ity Endpoi Endpoi O0:0C:2 O0:0C:2	nt ID () 9:C7:16:48 \ 9:C7:16:48 \	Windows7-Worksta		Authorization Policy	Authorization Profiles (i	IP Address (1) 10.0.0.21
Time 2015-07-20 00:45:55.580 2015-07-20 00:45:55.567 2015-07-20 00:45:55.544	Status All All C	Details	Repeat Count Identi 0 jguest jguest	ity Endpoi Endpoi O0:0C:2 O0:0C:2	nt ID () 9:C7:16:48 \ 9:C7:16:48 \ 9:C7:16:48	Windows7-Worksta		Authorization Policy	Authorization Profiles (i	IP Address (* 10.0.0.21 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 1Select->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 ACCESS HOW-TO GUIDES

se the search function below to			
Secure Group Tag(s) currently i	ncluded in this policy.		
Secure Group Tag Name	SGT Number	SGT Description	Delete
Contractor	6	NONE	
			Delete
nter any text to search for a Se	cure Group Tag name, number, or d	escription. Select one or more Secure Group Tags from the	list and use the
inter any text to search for a Se Idd button to add to this policy.	cure Group Tag name, number, or d	escription. Select one or more Secure Group Tags from the	list and use the
Enter any text to search for a Se Add button to add to this policy.		escription. Select one or more Secure Group Tags from the	list and use the
Enter any text to search for a Se Idd button to add to this policy. iearch	x	escription. Select one or more Secure Group Tags from the	list and use the
inter any text to search for a Se dd button to add to this policy. earch	x	escription. Select one or more Secure Group Tags from the SGT Description	
Inter any text to search for a Se dd button to add to this policy. earch O Secure Group Tag(s) select Secure Group Tag Name	x sed for Add SGT Number 0		Add
nter any text to search for a Se dd button to add to this policy. earch 9 Secure Group Tag(s) select Secure Group Tag Name Inknown ngineering	x sed for Add SGT Number	SGT Description Unknown Security GroupNONE	Add Select All
inter any text to search for a Se dd button to add to this policy. earch 9 Secure Group Tag(s) select Secure Group Tag Name Inknown ingineering	x eed for Add SGT Number 0 3 2	SGT Description	Add Select All
Enter any text to search for a Se did button to add to this policy. Iearch 9 Secure Group Tag(s) select Secure Group Tag Name Joknown Engineering ISA	x sed for Add SGT Number 0 3 2 5	SGT Description Unknown Security GroupNONE	Add Select All
Enter any text to search for a Se lad button to add to this policy. Search 0 Secure Group Tag(s) select Secure Group Tag Name Jnknown Engineering ASA Suest Employee	x sed for Add SGT Number 0 3 2 5 4	SGT Description Unknown Security GroupNONENONENONENONENONENONENONE	Add Select All
Add button to add to this policy. Search O Secure Group Tag(s) select	x sed for Add SGT Number 0 3 2 5	SGT Description Unknown Security GroupNONENONENONENONE	Add Select All

Step 2 Click->Done

Step 3 You will see the following

Policy Settings			
✓ Enable Policy			
Policy Name: 🕐	Contractor (e.g. my IT policy)		
Description:			
Insert Above Policy:	1 (Employee) ‡		
Membership is defined by the combination of the following Identification Profiles and Users:	options. All criteria must be met for the pol Select One or More Identification Profiles		
	Identification Profile	Authorized Users and Groups	Add Identification Profile
	ISE :	All Authenticated Users Selected Groups and Users ⑦ ISE Secure Group Tags: Contractor Users: No users entered Guests (users failing authentication)	<u></u>

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

Predefined URL Category Filtering						
These URL Categories are defined as group membership criteria. All other categories and	re not applica	ble for this	policy.			
	Use		Override Global Settings			
	Global Settings	Block 3	Monitor	Warn 🕐	Quota-Based	Time-Based
Category	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
😝 Education	1				-	-
😝 Entertainment	1				-	-
😔 Extreme	1				-	-
\varTheta Fashion	1				-	_
S File Transfer Services		1			-	-
😔 Filter Avoidance	1				-	-

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.

00	ste Error: Navigation Blocked - Windows Internet Explorer	X
$\Theta \Theta$	2	• م
🚖 Favorite		
Certific	ate Error: Navigation Blocked 🐴 🔻 🖾 🖷 🖝 Page 🔻 Safety 🔻 Tools 👻	0-
Protecte	d mode is currently turned off for the Internet zone. Click here to open security settings.	×
8	There is a problem with this website's security certificate.	^
	The security certificate presented by this website was issued for a different website's address.	
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.	
	We recommend that you close this webpage and do not continue to this website.	
	Click here to close this webpage.	
	Continue to this website (not recommended).	
	More information	
	2	
🖲 Done	😝 Internet Protected Mode: Off 🛛 🍕 🔻 🔍 100%	•
1	 (a) 107 Pi (b) 107 Pi (c) 107 Pi	

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

Sign On - Windows Internet E	xplorer			1	
🗨 🗢 🔽 https://10.0.0.	98:8443/portal/PortalSett 👻 😵 Certi	ficate Error 🍫 🗙	🕨 Bing		• م
🍾 Favorites 🛛 👍 💋 Sugges	ted Sites 👻 🙋 Web Slice Gallery 👻				
Sign On		🟠 👻	🔊 * 🖃 🖶 * P	age 👻 Safety 🕶	Tools 👻 🔞 🕶
Protected mode is currently t	urned off for the Internet zone. Click h	ere to open security s	settings.		3
cisco. Spon	sored Guest Portal				
Sign On Welcome to the Guest Username:	Portal. Sign on with the usern	ame and passw	ord provided to yo	u.	
Jcontractor					
Password:					
•••••	I				
	Sig	gn On			
Done		✓ Trusted sites P	rotected Mode: Off		a 100% -
				- 😼 🛱 👈	9:09 PM

Step 3 Contractor selects continue

🔗 Post-Login Banner - Windows Internet Explorer		
🚱 🔵 🗢 🙋 https://10.0.0.98:8443/portal/PortalSett 👻 😵 Certifica	ate Error 🤣 🔀 📴 Bing	+ م
🚖 Favorites 🛛 👍 🔊 Suggested Sites 🔻 🔊 Web Slice Gallery 🕶		
🖉 Post-Login Banner	🏠 🕶 🔝 👻 🚍 🖶 🕶 Page	▼ Safety ▼ Tools ▼ 🕢 ▼
Protected mode is currently turned off for the Internet zone. Click here	to open security settings.	×
cisco. Sponsored Guest Portal		
Welcome Message Click Continue to connect to the network. You're very close to gaining network access. Con	tinue	
		6 - 6 1002 -
	Trusted sites Protected Mode: Off	√a ▼ € 100% ▼ 9:10 PM 9:10 PM
		7/19/2015

Step 4 Contractor has successfully logged into the Sponsored Guest Portal

SECURE ACCESS HOW-TO GUIDES

🏉 Success - Windows Inte	ernet Explorer			[
🕞 🔵 🗢 🙋 https://	10.0.0.98:8443/portal/PortalSetu	▼	🍫 🔀 🕨 Bing		+ ۹
🚖 Favorites 🛛 🚔 🙋 S	uggested Sites 👻 🧕 Web Slice	e Gallery 🔻			
C Success			🏠 • 🔊 • 🖃 🖶 •	Page 🔻 Safety 🔻	Tools 🔻 🔞 🕶
Protected mode is current	ently turned off for the Internet z	one. Click here to open	ecurity settings.		×
ultulu cisco S	ponsored Guest P	ortal			4.2
Success You now have Inte	rnet access through this	network.			
🕖 Done		🗸 Trustee	sites Protected Mode: Off	• •	€ 100% ▼
🚱 🥖 🔋	3 🔉 😝			- 🖪 🛱 🕼	9:11 PM 7/19/2015

Step 5 Contractor accesses Box.com and is denied

🖉 Notification: Policy: Destination - Windows Internet Explorer	
🚱 🔾 🗢 🙋 http://www.box.com/ 💿 💀 😽 🗙 🕨 Bing	• م
🐈 Favorites 🛛 🙀 🔊 Suggested Sites 🔻 🔊 Web Slice Gallery 👻	
🍘 Notification: Policy: Destination	afety 🕶 Tools 🕶 🔞 🕶
Protected mode is currently turned off for the Internet zone. Click here to open security settings.	3 >
	4
	_
This Page Connet Re Displayed	
This Page Cannot Be Displayed	
Based on your organization's access policies, access to this web site (http://www.box.com/) has been blocked	
If you have questions, please contact your organization's network administrator and provide the	
codes shown below.	
Date: Mon, 20 Jul 2015 01:12:05 GMT	
Username: jcontractor Source IP: 10.0.0.21	
URL: GET http://www.box.com/ Category: Box	
Reason: BLOCK-DEST	
Notification: BLOCK_DEST	
	-
🖲 Done 😜 Internet Protected Mode: Off	@ ▼ 🔍 100% 👻
🚱 🤔 📜 💽 📰 🔹 😿	9:12 PM 7/19/2015

Step 6 Contractor accesses Facebook

🔾 🔾 🔻 🚹 https://www.facebook.com/ 🛛 👻 🔒 🐓 🗙 🕨 Bin	ng 🔎
🚖 Favorites 🛛 🚔 🙋 Suggested Sites 👻 😰 Web Slice Gallery 👻 🛛 🔪	
f Welcome to Facebook - Log In, Sign Up or Learn 🛛 👘 🔻 🖾 👻	📑 🖶 🝷 Page 🖛 Safety 🖛 Tools 🖛 🔞
Protected mode is currently turned off for the Internet zone. Click here to open security settings.	
facebook	Email or Phone F
Connect with friends and the	Sign Up It's free and always will
Johneet with menus and the	
vorld around you on Facebook.	First name
See photos and updates from friends in News Feed.	First name
	First name Email or mobile number Re-enter email or mobil
See photos and updates from friends in News Feed.	First name Email or mobile numbe
See photos and updates from friends in News Feed.	First name Email or mobile number Re-enter email or mobil New password

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

ျပျပ cisco Identity Ser	vices En	gine		ا (1)	Home Operations	Policy Gue	est Access 🔻 Adminis	License Warning 👔	I iseca I admin I Logou	t Feedback 🔎
Authentications	👖 Rep	orts	Realize N	etwork Control	💊 Troubleshoot					
Misconfigured S	upplicants	(i)	М	lisconfigured Netwo	ork Devices (i)		US Drops (1)	Client Stop	pped Responding (1)	k
🗓 Show Live Sessions 🐇	Add or R	emove Co	lumns 🔻 🛞 Rel	fresh 💿 Reset Re	peat Counts			Refresh Every	1 minute T Show	Latest 20 records
Time 🔻	Status All 🔻	Details	Repeat Count	Identity (i)	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
2015-07-20 01:11:05.682	0	ò	0	jcontractor	00:0C:29:C7:16:48	Windows7-Worksta				10.0.0.21
2015-07-20 01:11:05.671		0		jcontractor	00:0C:29:C7:16:48	Windows7-Worksta	Default >> MAB	Default >> Contractor	Contractor, PermitAccess	10.0.0.21
2015-07-20 01:11:05.648		0			00:0C:29:C7:16:48					
2015-07-20 01:09:47.806		0		jcontractor	00:0C:29:C7:16:48					10.0.0.21
2015-07-20 01:06:18.811	Image: A start a st	0		#ACSACL#-IP-rec						
2015-07-20 01:06:18.799		0		00:0C:29:C7:16:4	00:0C:29:C7:16:48		Default >> MAB >> Def.	Default >> Redirect	Redirect	10.0.0.21

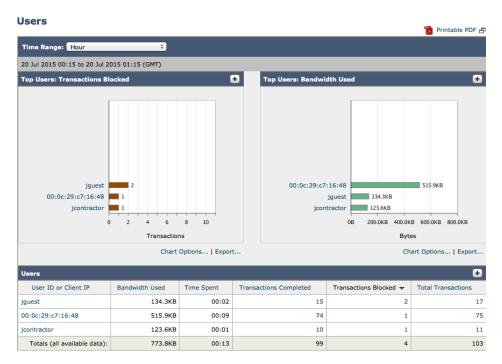
Step 8 On the WSA console, type in "isedata" to view the IP-SGT mappings for jcontractor

```
00

☆ jeppich — ssh — 80×24

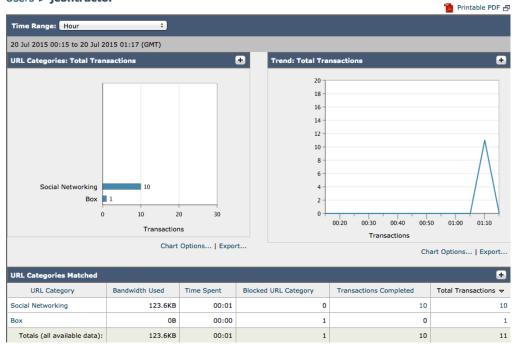
                                                                                       R.M
- CACHE - Show the ISE cache or check an IP address.
- SGTS - Show the ISE Secure Group Tag (SGT) table.
[]> CACHE
Choose the operation you want to perform: - SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[]> SHOW
IΡ
                  Name
                                                                                   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
                   18:E7:28:2E:29:CC
10.0.0.3
                                                                                   Ø
Choose the operation you want to perform: - SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[]>
```

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



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	ı				
Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions 🔻
akamaihd.net	105.3KB	00:00	8	0	8
facebook.com	18.3KB	00:01	2	0	2
box.com	OB	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):		123.6KB	10	1	11
Find	Policy Name				Columns Export

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

Destination	
URL:	www.box.com
Transaction	
Client or User:	To represent a client by IP address, chose 'Vo 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) 1 Client IP Address: User Name:
Advanced	
	Find Policy Match
Results	
User Information User Name: None Authentication Realm Group Membership: None Secure Group Tag Membership: Contractor User-Agent: Nozila/S.0 (Medionshi): Intel Mac OS Custom URL Category: Box	5 X 10.8; rv:39.0) Gecko/20100101 Firefox/39.0
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 c	ategory
Trace session complete	

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

Destination	
URL:	www.facebook.com
Transaction	
Client or User:	To represent a client by IP address, choose "No authentication or Identification" and enter the IP address below. To represent a user identified through ISE, choose "Identity Services Engine (ISE)" and enter an IP address. Authentication / Identification: Identity Services Engine (ISE) ‡ Client IP Address: 10.0.0.21 User Name:
Advanced	
	Find Policy Match

SECURE ACCESS HOW-TO GUIDES

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 WRS 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. Rune "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

ernet Options					8
cal Area Netw	vork (LAN) Settin	gs			-2
Automatic con	figuration				
	figuration may ove settings, disable a				re the
Automatica	ally detect settings	É			
Use autom	atic configuration :	script			
Address]	
Proxy server					
	y server for your l /PN connections).	L <mark>AN (Th</mark> ese	e settings v	vill not app	ly to
Address:	10.0.0.22	Port:	3128	Advan	ced
V Bypass	proxy server for	local addre	sses		
			OK	Ca	ncel
Local Area Ne	twork (LAN) settin	as			
LAN Settings	do not apply to di	al-up conn		LAL	ettings
	ings above for dial	-up setting	s.		
Choose Setti					
Choose Setti					
Choose Setti					

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.

				_
ers				
L T	Гуре	Proxy address to use		Port
	TTP:	10.0.0.22	:	3128
s	Secure:	10.0.0.22	:	3128
F	TP:	10.0.022	:	3128
s	Socks:		:	
eptions	s Do not use 1.1.1.1;i	e same proxy server for all protoc e proxy server for addresses beg seca.lab6.com olons (;) to separate entries.		:

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: <u>http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_sw_cnfg.html</u>

```
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: <u>http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-</u> <u>Self signed pxGridClient selfsigned pxGrid.pdf</u>

Deploying certificates with pxGrid: using CA-signed ISE pxGrid node and CA- signed pxGrid client: <u>http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-</u> <u>Self signed pxGridClient selfsigned pxGrid.pdf</u>