

Websense Content Gateway HTTPS Configuration

Support Webinars



Scott Peckenpaugh

- **Title: Sr. Tech Support Specialist**
 - Cisco Certified Security Professional
 - Microsoft Certified Systems Engineer

- **SSL Overview**
 - General SSL information
- **HTTPS Module Overview**
 - WCG's HTTPS
- **HTTPS Configuration**
 - Configuration Steps
- **SSL Bypass**
 - Incident management
- **Certificate Management**
 - Managing Digital Certificates



SSL Overview

- **Secure Sockets Layer (SSL)**
 - Provides security between server and client
 - Authenticates with a digital certificate
 - Encrypts using Public/Private key
 - Host side integrated into your web browser

■ Authentication

- A digital certificate is tied to a specific domain
- Issued by Certification Authority (CA)
- The CA is a trusted third party
- Confirms identity of the owner of the domain
- VeriSign or Thawte

■ Encryption

- The process of transforming information to make it unintelligible to all but the intended recipient.
- This forms the basis of data integrity and privacy necessary for e-commerce.
- Uses the public-and-private key encryption system developed by RSA.

■ Public Key

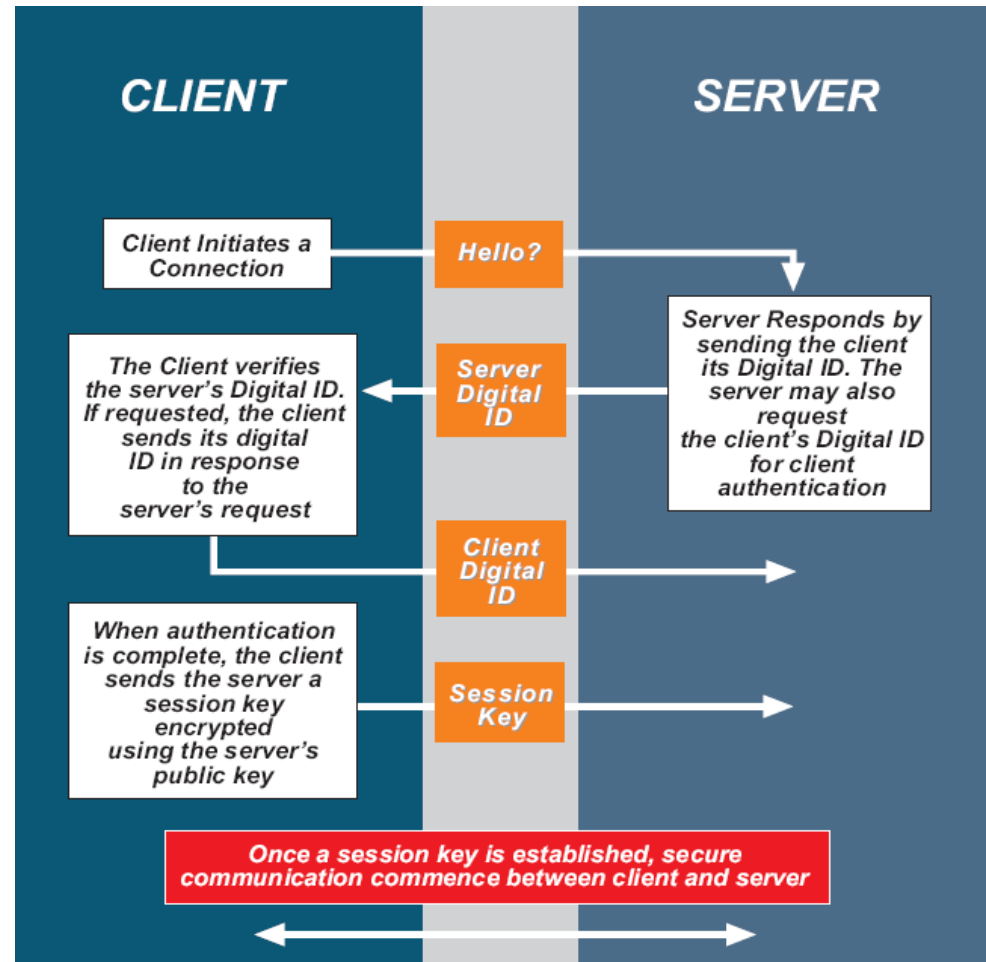
- Numeric code used to encrypt messages sent to the holder of the corresponding private key.
- Public key may be freely circulated without compromising encryption.

■ Private Key

- Numeric code used to decrypt messages encrypted with a unique corresponding public key.
- Integrity of encryption depends on the private key being kept secret.

How is a SSL Session Setup?

- Client requests connection (lists supported Ciphers).
- Server chooses strongest mutual Cipher and sends Digital Certificate (DC).
- Client validates DC, encrypts a random number with Public Key.
- Server decrypts with Private key to get the random number.
- This shared secret random number is then used to encrypt all traffic.

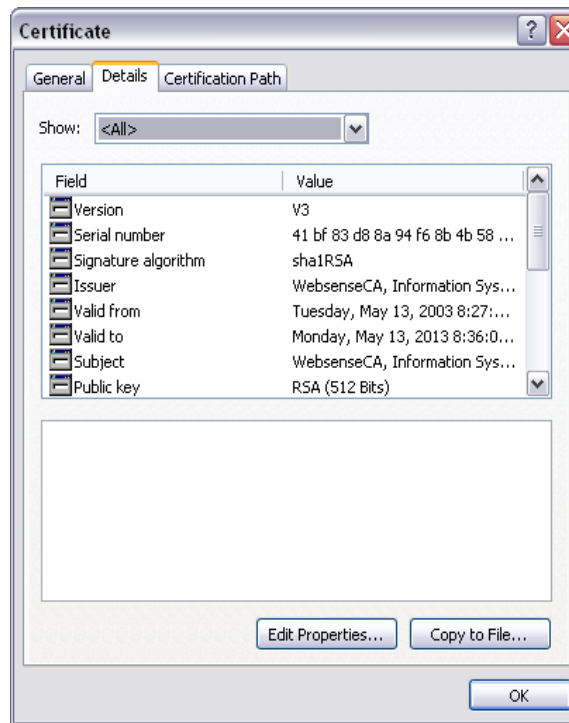
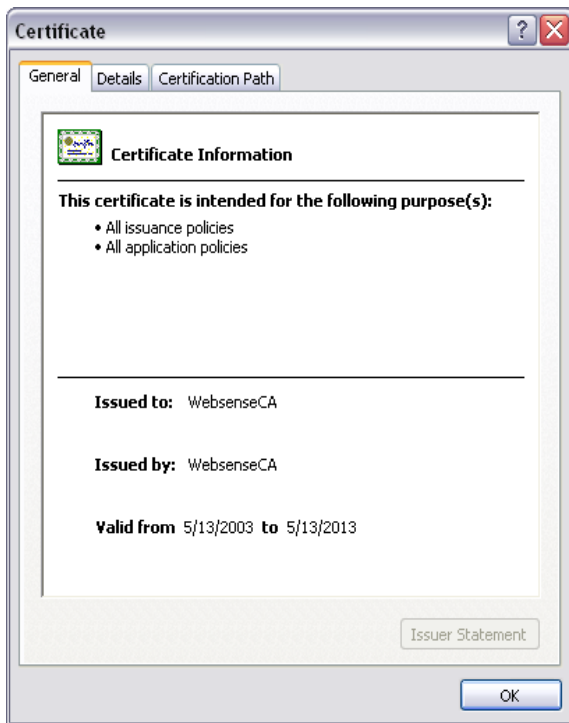


■ Padlock

- Look for a padlock on the browser status bar.
- When a SSL session is established the padlock icon will appear.
- The strength of the encryption can be shown by mousing over the padlock on IE.



Internet Explorer



- The domain for which the certificate was issued.
- The CA which issued the certificate.
- Time period the certificate is valid.
- The owner of the certificate.
- The physical location of the owner.
- Certification path or Certificate chain

- Certificates can be stolen, bogus, expired or revoked.
- The user, not the security officer, makes the final decision about the “trustworthiness” of a website or entity.
- In the best case, digital certificates can only guarantee the identity of a person or entity. They cannot provide any assurance about the person’s intentions.

- Secures communication between server and client.
- Authenticates with Digital Certificate
- Encrypts with Public/Private keys
- CA's are trusted 3rd party



HTTPS Module Overview

- Websense has contracted with Microdasys to provide the HTTPS termination process used by WCG.
- SCIP - Secure Content Inspection Proxy
- SCIP provides 2 primary areas of functionality:
 - Certificate Validation
 - Proxy

■ Certificate Validation

- Digital certificates are checked for validity.
- SCIP catches bogus, self-signed and revoked certificates
- Certificates are inspected and allowed or denied at the gateway level, based on security policies, not the discretion of the client user.
- Automatic revocation checking with Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) support.
- Extensive exception handling and incident management capabilities.

■ Proxy

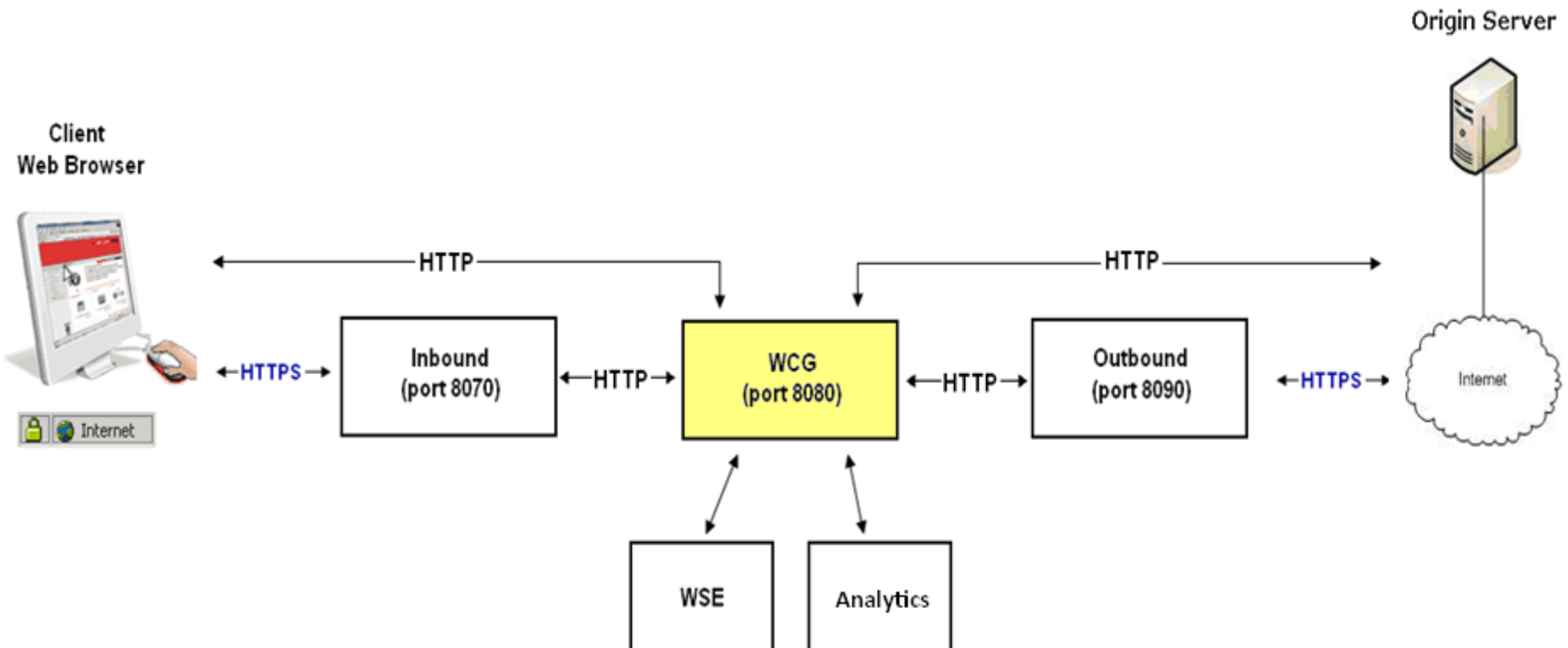
- The data is decrypted, forwarded to WCG.
- WCG applies inspection rules (ie. WSE, Analytics)
- Re-encrypted and sent to its destination.
- Applies security policies to all encrypted inbound and outbound Internet traffic.
- Data can be decrypted and hence inspected for malware.

- Certificate validation ensures the following
 - Certificate is not revoked
 - Certificate is not expired
 - Certificate owner and URL have the same identity
 - Certificate is issued by a trustworthy CA
- Network Security Administrator has the power to decide which site to be allowed not the client.
 - Any decision about the trustworthiness of a certificate must be made solely by the security administrator.
 - Any exception to the rule can only be made and allowed by the security administrator.
 - The user of a client workstation can only request exceptions, but not make them.
- Control over data transmitted
 - Data can be decrypted and hence inspected for malware.

Traffic Flow

The client will accept the certificate without prompting the user if the following three requirements are fulfilled:

- 1 The certificate is signed by a trusted CA
- 2 The certificate is valid
- 3 The URL matches the Common Name Field of the Certificate.



- **SCIP**
 - Secure Content Inspection Proxy
- **Certificate Validation**
 - Common Name, Date, CA
- **Proxy**
 - Allows inspection of packet



HTTPS Configuration

SSL Decryption

- To enable the SSL configuration options, you first need to enable the SSL Decryption Feature.
- Configure > My Proxy > Basic > General > HTTPS
 - Select “On” Radio Button
 - Click Apply
- Configure > My Proxy > Basic > General > Reset
 - Click Restart

The screenshot shows the Websense Content Gateway configuration interface. The left sidebar contains a navigation menu with 'My Proxy' expanded, and 'Basic' selected. The main content area shows the 'General' tab under 'Basic Configuration'. The 'Restart' button is highlighted with a red box. The 'Proxy Name' field contains 'wcg2.wsg-train.com'. The 'Alarm email' field contains 'elothrop@websense.'. The 'Features' table has 'HTTPS' selected with a radio button.

WEBSense® Content Gateway

Monitor | Configure | User: admin | Get Help!

My Proxy

- Basic
- Subscription
- UI Setup
- Snapshots
- Logs

Protocols

- Content Routing
- Security
- Subsystems
- Networking
- SSL

General | Clustering

Basic Configuration [Apply] [Cancel]

Restart [Restart] • Restarts Websense Content Gateway proxy and manager services on all nodes in the cluster.

Proxy Name [wcg2.wsg-train.com] • Specifies the name of the Websense Content Gateway node/cluster. • In a Websense Content Gateway cluster, all nodes must share the same name.

Alarm email [elothrop@websense.] • Specifies the email address to which Websense Content Gateway will send alarm notifications.

Features

Feature	On	Off
General		
SNMP	<input type="radio"/>	<input checked="" type="radio"/>
Protocols		
FTP	<input type="radio"/>	<input checked="" type="radio"/>
HTTPS	<input checked="" type="radio"/>	<input type="radio"/>

■ Enable the Certificate Verification Engine

- To enable or disable verifying certificates and checking for certificate revocation.
- If this option is not selected, checking does not occur.

The screenshot shows the Websense Content Gateway configuration interface. The left sidebar contains a navigation menu with categories like My Proxy, Protocols, Content Routing, Security, Subsystems, Networking, and SSL. Under SSL, the 'Validation' option is selected and highlighted with a red box. The main window displays the 'Configure Certificate Validation' dialog box, with the 'General' tab selected and highlighted with a red box. The 'General' tab contains several options, with the first one, 'Enable the certificate verification engine', checked and highlighted with a red box. Other options include 'Deny certificates where the common name does not match the URL', 'Allow wildcard certificates', 'No expired or not yet valid certificates', 'Verify entire certificate chain', 'Check certificate revocation by CRL', 'Check certificate revocation by OCSP', 'Preferred method for revocation check: CRL', 'Block certificates with no CRL or with unknown OCSP state', and 'Run external program on incidents:'. The 'Apply' and 'Cancel' buttons are visible at the bottom right of the dialog box.



Certificate Management

- SCIP comes installed with the same list of CAs as the standard web browser installation.
- Other CAs are automatically added when sites signed by them are visited.
- Sites can also be added manually.
- Users can delete, allow, and block individual CAs and Sub-CAs.

Certificate Authority Tree

- Used to manage all known root CAs, trusted CAs are listed
- New CAs are added automatically with denied state
- Selecting and clicking on the certificate allows changing the state

The screenshot displays the Websense Content Gateway configuration interface. The top navigation bar includes 'Monitor' and 'Configure' tabs, with 'Configure' selected. The user is identified as 'admin'. The left sidebar shows a tree of configuration categories, with 'SSL' expanded and 'Certificates' selected. The main content area is titled 'Certificate Authorities' and features a toolbar with 'Add Root CA', 'Backup Certificates', and 'Restore Certificates' buttons. Below the toolbar is a tree view of the 'Certificate Authority Tree' containing various CA entries, each with a folder icon and a status indicator (green circle for trusted, red circle with 'i' for denied).

Monitor **Configure** **Content Gateway** websense
User: admin [Get Help!](#)

My Proxy
Protocols
Content Routing
Security
Subsystems
Networking
SSL
 Certificates
 Decryption / Encryption
 Validation
 Incidents
 Client Certificates
 Logging
 Customization
 Internal Root CA

Certificate Authorities **Add Root CA** **Backup Certificates** **Restore Certificates**

Certificate Authority Tree

- ABA.ECOM Root CA
- Autoridad Certificadora de la Asociacion Nacional del Notariado Mexicano, A.C.
- Autoridad Certificadora del Colegio Nacional de Correduria Publica Mexicana, A.C.
- Baltimore EZ by DST
- Belgacom E-Trust Primary CA
- Belgacom E-Trust Root CA for normalised certificates
- Certipost E-Trust Primary CA for Normalised certificates
- C&W HKT SecureNet CA Class A
- C&W HKT SecureNet CA Class B
- C&W HKT SecureNet CA Root
- C&W HKT SecureNet CA SGC Root
- Certiposte Classe A Personne
- Certiposte Serveur
- Certisign - Autoridade Certificadora - AC2
- Certisign - Autoridade Certificadora - AC4
- Certisign Autoridade Certificadora AC1S
- Certisign Autoridade Certificadora AC3S
- Class 1 Primary CA
- Class 1 Public Primary Certification Authority
- VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
- Class 2 Primary CA
- Class 2 Public Primary Certification Authority
- Class 3 Primary CA

Add Root CA

- The certificate has to be in x509 Format and Base64 encoded.

The screenshot displays the Websense Content Gateway configuration interface. The top navigation bar includes 'Monitor' and 'Configure' tabs, with 'Configure' selected. The user is logged in as 'admin'. The left sidebar shows a tree view of configuration categories, with 'SSL' expanded and 'Certificates' selected. The main content area shows the 'Add Root CA' configuration page. At the top of this page, there are four tabs: 'Certificate Authorities', 'Add Root CA' (highlighted with a red box), 'Backup Certificates', and 'Restore Certificates'. Below the tabs, the page title is 'Add Trusted Certificate Authority'. The main section is titled 'Add Root CA' and contains a 'Location:' label followed by a text input field and a 'Browse...' button. To the right of the input field is an 'Add Certificate Authority' button. Below the input field, a note states '(Only base64 encoded x509 certificates are allowed)'. The bottom of the page features a decorative graphic of a globe with binary code.

Backup Certificate

- The database can be saved(*.sdb format) to be used to restore the certificates in the future if needed.
- Click on Get copy of Database and save at the desired location.
- Use Restore Certificates Menu to restore the database

The screenshot displays the Websense Content Gateway interface. The top navigation bar includes 'Monitor' and 'Configure' tabs, with 'Configure' selected. The user is logged in as 'admin'. The left sidebar shows a menu with 'SSL' expanded, and 'Certificates' highlighted. The main content area shows a 'Backup Certificates' tab selected, with a 'Back Up Configuration to Database' button visible.

Restore Certificates

- Here you can restore the certificates backed up earlier.
- Browse and point to the location where database is saved and click Restore.

The screenshot displays the Websense Content Gateway configuration interface. The top navigation bar includes 'Monitor' and 'Configure' tabs, with 'Configure' selected. The user is logged in as 'admin'. The left sidebar shows a tree view of configuration categories, with 'SSL' expanded and 'Certificates' selected. The main content area shows the 'Restore Certificates' tab, which is highlighted with a red box. Below the tab, the 'Restore SSL Configuration' section is visible, featuring a 'Restore configuration' heading and a 'Location' input field with a 'Browse...' button. A 'Restore' button is located below the input field.

- This is the Certificate used by the WCG in response to client HTTPS requests.
- Deployment Options
- Import
 - Import a certificate already purchased from a CA.
 - Advantage of already being in all browsers.
 - The certificate and the private key has to be in x509 Format and Base64 encoded.
- Create
 - Create a new Internal root CA.
 - Will need to be deployed to all browsers (GPO)

Import Internal Root CA

- If you want to use a different Root CA you can do this here.
- The certificate and the private key has to be in x509 Format and Base64 encoded.

The screenshot displays the Websense Content Gateway configuration interface. The top navigation bar includes 'Monitor' and 'Configure' tabs, with 'Configure' being the active tab. The user is logged in as 'admin'. The left sidebar shows a tree view of configuration categories: My Proxy, Protocols, Content Routing, Security, Subsystems, Networking, and SSL. Under the SSL category, 'Internal Root CA' is selected and highlighted with a red box. The main content area shows three tabs: 'Import Root CA' (highlighted with a red box), 'Create Root CA', and 'Backup Root CA'. The 'Import Root CA' form contains the following fields:

- Certificate:** A text input field with a 'Browse...' button. Below it, a red note reads: 'Please use only base64-encoded certificates.'
- Private key:** A text input field with a 'Browse...' button. Below it, a red note reads: 'Please use only base64-encoded certificates.'
- Passphrase:** A text input field.
- Confirm passphrase:** A text input field.

At the bottom of the form is an 'Import Root CA' button.

Note: Restart of the WCG required.

Create Internal Root CA

- Create internal Root CA.
- Creating a new Internal Root CA will invalidate any previously deployed Root CA.

The screenshot displays the Websense Content Gateway configuration interface. The top navigation bar includes 'Monitor' and 'Configure' tabs, with 'Configure' selected. The user is identified as 'admin'. The left sidebar shows a tree view of configuration categories, with 'Internal Root CA' highlighted under the 'SSL' section. The main content area is titled 'Internal Root CA' and contains a form for creating a new Root Certificate Authority. The form includes fields for Country (set to US), State, City or locality, Organization, Organizational unit, Common name, Email address, Certificate valid for (set to 10 years), Comment, Passphrase, and Confirm passphrase. A 'Generate and Deploy Certificate' button is located at the bottom of the form, with a note below it stating 'This may take several seconds. Do not click this button again.'

Note: Restart of the WCG required.

Backup Internal Root CA

- Once deployed, changing the root CA will cause HTTPS connection failures.
- Backup Internal Root CA for Failure recovery and Clustering support.

The screenshot displays the Websense Content Gateway administration console. The top navigation bar includes 'Monitor' and 'Configure' tabs, with 'Configure' selected. The user is logged in as 'admin'. The left sidebar contains a menu with categories like 'My Proxy', 'Protocols', 'Content Routing', 'Security', 'Subsystems', 'Networking', and 'SSL'. Under 'SSL', the 'Internal Root CA' option is highlighted with a red box. The main content area shows three tabs: 'Import Root CA', 'Create Root CA', and 'Backup Root CA', with the latter being the active tab and also highlighted with a red box. Below the tabs, the 'Internal Root CA' section is visible, containing a 'Back Up Root CA' area with two buttons: 'Save Public CA Key' and 'Save Private CA Key'.

Verification Bypass

- Configure > SSL > Validation > Verification Bypass
 - Enables users to visit a site even if the certificate is invalid.
- Enable the SSL session cache for bypassed certificates
 - Store information about bypassed certificates in cache and reuse the connections.

The screenshot displays the Websense Content Gateway configuration interface. The top navigation bar includes 'Monitor' and 'Configure' tabs, with 'Configure' selected. The user is identified as 'admin'. The left sidebar shows a tree view of configuration categories, with 'SSL' expanded and 'Validation' selected. The main content area shows the 'Verification Bypass' configuration page, which is highlighted with a red box. The page has three tabs: 'General', 'Verification Bypass', and 'Revocation Settings'. The 'Verification Bypass' tab is active. The configuration includes a section titled 'Bypass certificate verification' with 'Apply' and 'Cancel' buttons. Below this, the 'Verification Bypass' section contains three settings: 1) 'Permit users to visit sites with certificate failures after confirmation' (checked, highlighted with a red box), 2) 'Enable the SSL session cache for bypassed certificates' (checked), and 3) 'Timeout: 6 minutes' (input field). 'Apply' and 'Cancel' buttons are located at the bottom right of the configuration area.

SSL-Certificate Verify failed



A certificate verification error occurred

Overview: The access to the URL wamu.com:443 is restricted because the validation of the certificate failed

Details: *VERIFY DENY: depth=0*, CommonName "www.wamu.com" does not match URL "wamu.com:443"

Options: Pressing the button allows you to visit the website although the certificate is not valid.

Visit Site anyway

Pressing the button allows you to go to the previous page.

Go Back

To find out more about the reason for the block message, please contact your administrator and refer to ID 21.

- **Configure > SSL > Validation > Revocation Settings**
 - Configure how SSL Manager keeps revocation information current. By default, SSL Manager downloads CRLs on a daily basis.

The screenshot displays the Websense Content Gateway configuration interface. The top navigation bar includes 'Monitor' and 'Configure' tabs, with 'Configure' selected. The user is identified as 'admin'. The left sidebar shows a tree view of configuration categories, with 'SSL' expanded and 'Validation' selected. The main content area shows the 'Revocation Settings' page, which is highlighted with a red box. The page title is 'Configure Certificate Revocation'. Under 'CRL Settings', there is a checked checkbox for 'Download the CRL at:' with a dropdown menu set to '1 am'. Below this are buttons for 'Update CRL Now' and 'View CRL Update Progress'. Under 'OCSP Settings', there is a field for 'Cache OCSP data for' set to '14' days (max. 1000). The page has 'Apply' and 'Cancel' buttons at the bottom right.

- Reasons why certificate could become untrustworthy prior to expiration:
 - Compromised or suspected compromise of the certificate subject's private key.
 - Discovery that a certificate was obtained fraudulently.
 - Change in the status of the certificate subject as a trusted entity.

SSL Incident Management

- Configure > SSL > Incidents > Incident List
 - Sort by any field or search for an incident ID

WEBSense®
Content Gateway

Monitor Configure

Get Help!

- My Proxy
- Protocols
- Content Routing
- Security
- Subsystems
- Networking
- SSL
 - Certificates
 - Decryption / Encryption
 - Validation
 - Incidents**
 - Client Certificates
 - Logging
 - Customization
 - Internal Root CA

Incident List Add Website

Website Access Management

Incident List

search ID: Search Show all

ID	Status	Type	URL	Message	Action
1	STOP	Cert	www.gmail.com:443	VERIFY DENY: depth=0, CommonName "mail.google.com" does not match URL "www.gmail.com:443"	Select action... GO
2	STOP	Cert	www.hotmail.com:443	VERIFY DENY: depth=0, (20) unable to get local issuer certificate: "cb1.msn.com" VERIFY DENY: depth=0, (21) unable to verify the first certificate: "cb1.msn.com"	Select action... GO

Delete Tunnel Block Blacklist Allow

- You can add incidents manually and configure the Action you want the SSL Manager to perform

The screenshot displays the Websense Content Gateway interface. On the left is a navigation menu with categories like 'My Proxy', 'Protocols', 'Content Routing', 'Security', 'Subsystems', 'Networking', and 'SSL'. Under 'SSL', 'Incidents' is highlighted. The main area shows the 'Incident List' tab with an 'Add Website' button. An 'Add Incident' dialog box is open, featuring a 'URL' field with 'https://', radio buttons for 'By Certificate' (selected) and 'By URL', and an 'Action' dropdown menu with options 'Blacklist', 'Tunnel', 'Allow', and 'Blacklist'. The 'Blacklist' option is selected in the dropdown. The dialog also includes 'Apply' and 'Cancel' buttons.

- Configure > SSL > Customization > Certificate Failure
- You can customize the message users receive when:
 - They are trying to connect to a site that has an invalid certificate.
 - There is a connection failure.

The screenshot displays the Websense Content Gateway administration console. The top navigation bar includes 'Monitor' and 'Configure' tabs, with 'Configure' selected. The user is identified as 'admin'. The left sidebar shows a tree view of configuration categories, with 'SSL' expanded and 'Customization' selected. The main content area shows the 'Certificate Failure' configuration page. The 'Customization' section is active, displaying a text area for editing the 'Customize Certification Failure Message'. The message content is HTML code that includes a title 'Certificate Verification Error', a link to a stylesheet, and a body with an icon and a heading 'A certificate verification error occurred'. Below the text area is a 'Preview' button. The page also features 'Apply' and 'Cancel' buttons at the top right and bottom right.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<title>Certificate Verification Error</title>
<link rel="stylesheet" href="%P://%H/command/file?block_style.css" type="text/css">
</head>
<body>

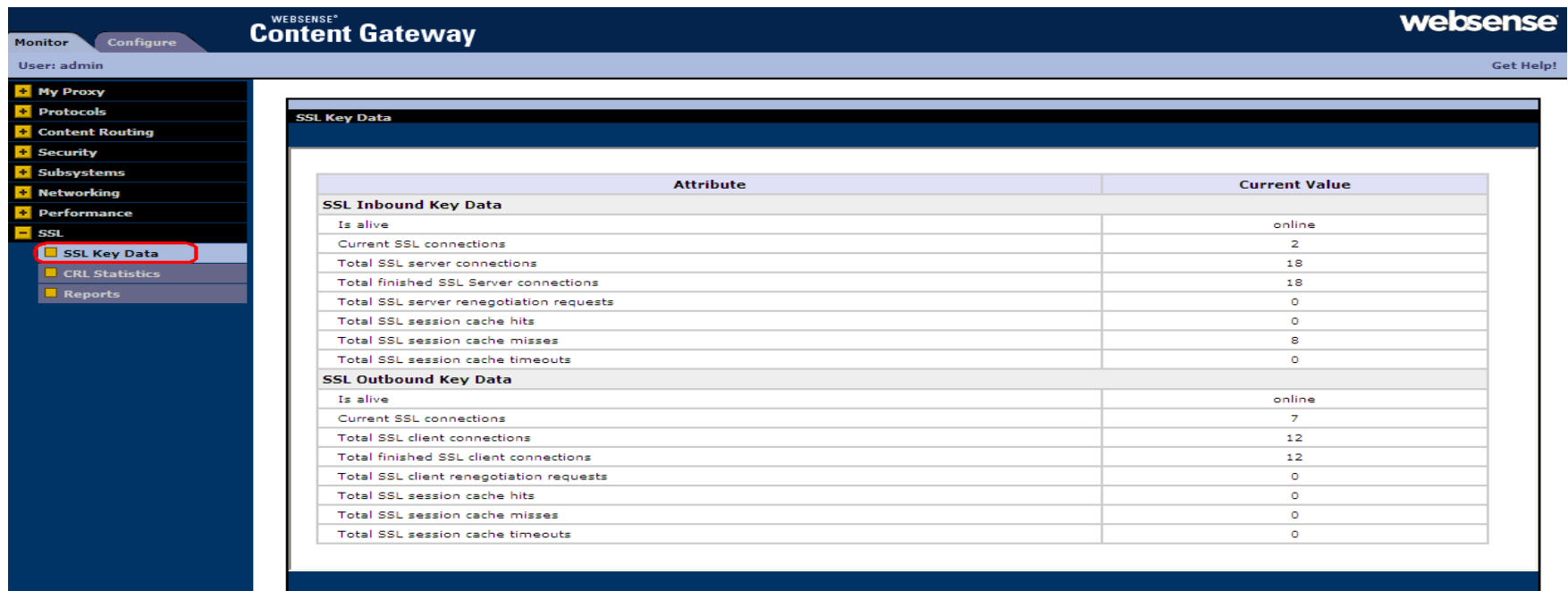
<div id="pagecontainer">
   <!--
Icon for block type-->
  <h1>A certificate verification error occurred</h1>

  <div class="row">
    <p class="label">Overview:</p>
    <p class="item">The access to the URL %H is restricted because
the validation of the certificate failed</p>

Preview
```

Monitor > SSL > SSL Key Data

- Provides information about the status of the SSL connection. and activity
- Between the client and SSL Manager and SSL Manager and the destination server.



WEBSENSE® Content Gateway

Monitor Configure

User: admin [Get Help!](#)

SSL Key Data

Attribute	Current Value
SSL Inbound Key Data	
Is alive	online
Current SSL connections	2
Total SSL server connections	18
Total finished SSL Server connections	18
Total SSL server renegotiation requests	0
Total SSL session cache hits	0
Total SSL session cache misses	8
Total SSL session cache timeouts	0
SSL Outbound Key Data	
Is alive	online
Current SSL connections	7
Total SSL client connections	12
Total finished SSL client connections	12
Total SSL client renegotiation requests	0
Total SSL session cache hits	0
Total SSL session cache misses	0
Total SSL session cache timeouts	0

- CRL is the Certificate Revocation List
 - Provides statistics on certificate status
 - CRL - generally downloaded nightly
 - OCSP – Online Certificate Status Protocol
 - Checks certificate status online. Returns Current, Expired or Unknown

The screenshot displays the Websense Content Gateway administration interface. The top navigation bar includes 'Monitor' and 'Configure' tabs, with 'Configure' selected. The user is logged in as 'admin'. The left sidebar contains a menu with categories like My Proxy, Protocols, Content Routing, Security, Subsystems, Networking, Performance, and SSL. Under the SSL category, 'CRL Statistics' is highlighted with a red box. The main content area shows a table titled 'CRL Statistics' with two columns: 'Attribute' and 'Current Value'. The table lists 'CRL list count' with a value of 45518, and 'OCSP Statistics' with sub-rows for 'OCSP good count' (0) and 'OCSP unknown count' (0).

Attribute	Current Value
CRL Statistics	
CRL list count	45518
OCSP Statistics	
OCSP good count	0
OCSP unknown count	0

- **SSL Overview**
 - Digital certificates, Public/Private keys, CA's
- **HTTPS Module Overview**
 - SCIP, Proxy, Certificate Validation
- **HTTPS Configuration**
 - Enable HTTPS, Certificate Validation
- **SSL Bypass**
 - Incident management, manual
- **Certificate Management**
 - Create, Import, Backup Certs. and Internal Root CA

Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.

Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.

Tech Alerts

- Subscribe to receive product specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

ask.websense.com

- Create and manage support service requests using our online portal.

Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit:
<http://www.websense.com/findaclass>
- Websense Training Partners also offer classes online and onsite at your location.
- For more information, please send email to:
readiness@websense.com

WEBSense®
**Authorized Training
Partner**

WEBSense®
Certified Instructor



Upcoming Webinar

**Title: Troubleshooting, Logging and Reporting
Issues for Websense Web Filter 7.x**

Date: March 10, 2010

Time: 8:00 AM PST

How to register:

[http://www.websense.com/content/
SupportWebinars.aspx](http://www.websense.com/content/SupportWebinars.aspx)

Questions?

