Troubleshooting and Architecture Overview for Data Security and Web Security Gateway on the V-Series Appliance

web security | data security | email security

V-series Appliance

- Architecture overview
  - Base platform information with illustrations
  - Which log files are created, and where they are stored
- Understanding Content Gateway (proxy) extended.log
  - What is extended.log
  - Turning on extended.log
  - Viewing extended.log –what do the fields mean?
  - Examples: HTTP request; NTLM messages;
- Understanding error.log
- Common Troubleshooting Scenarios
  - Top 5 issues

    Subscription issues

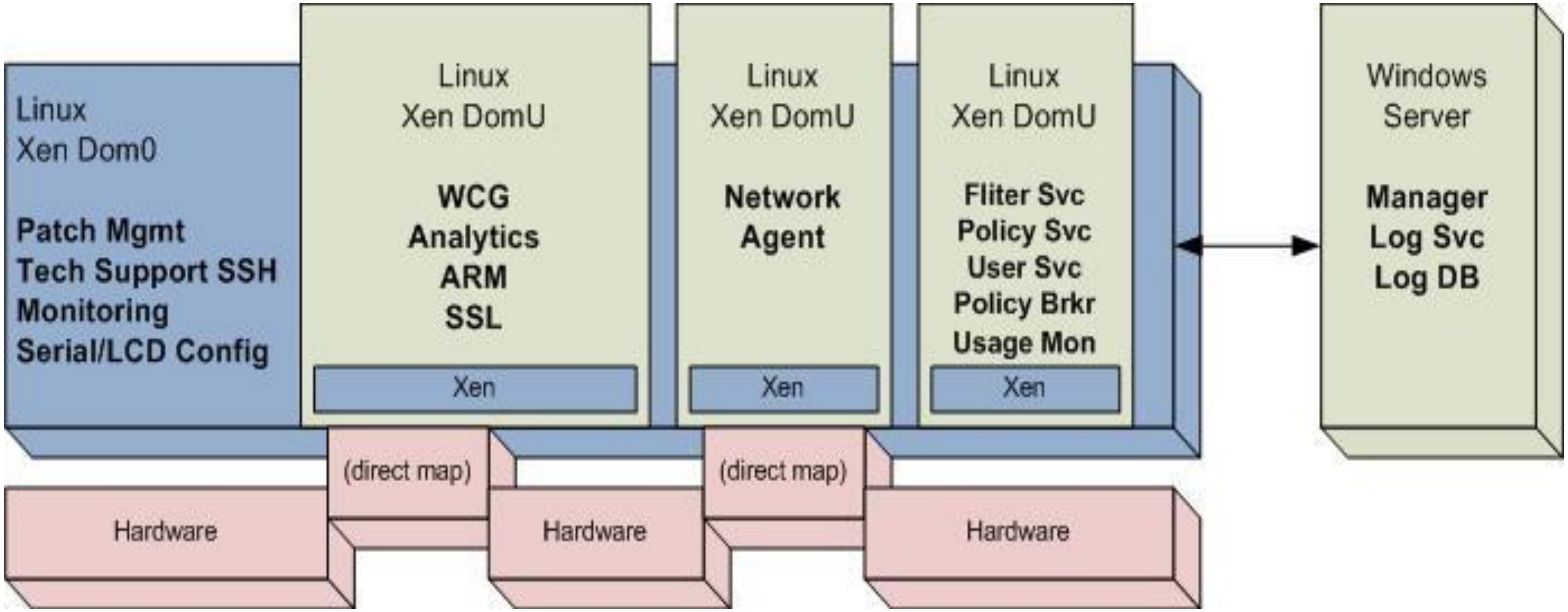
    Database download failures

    Unable to access a Web site

V-series Architecture

V-series Appliance

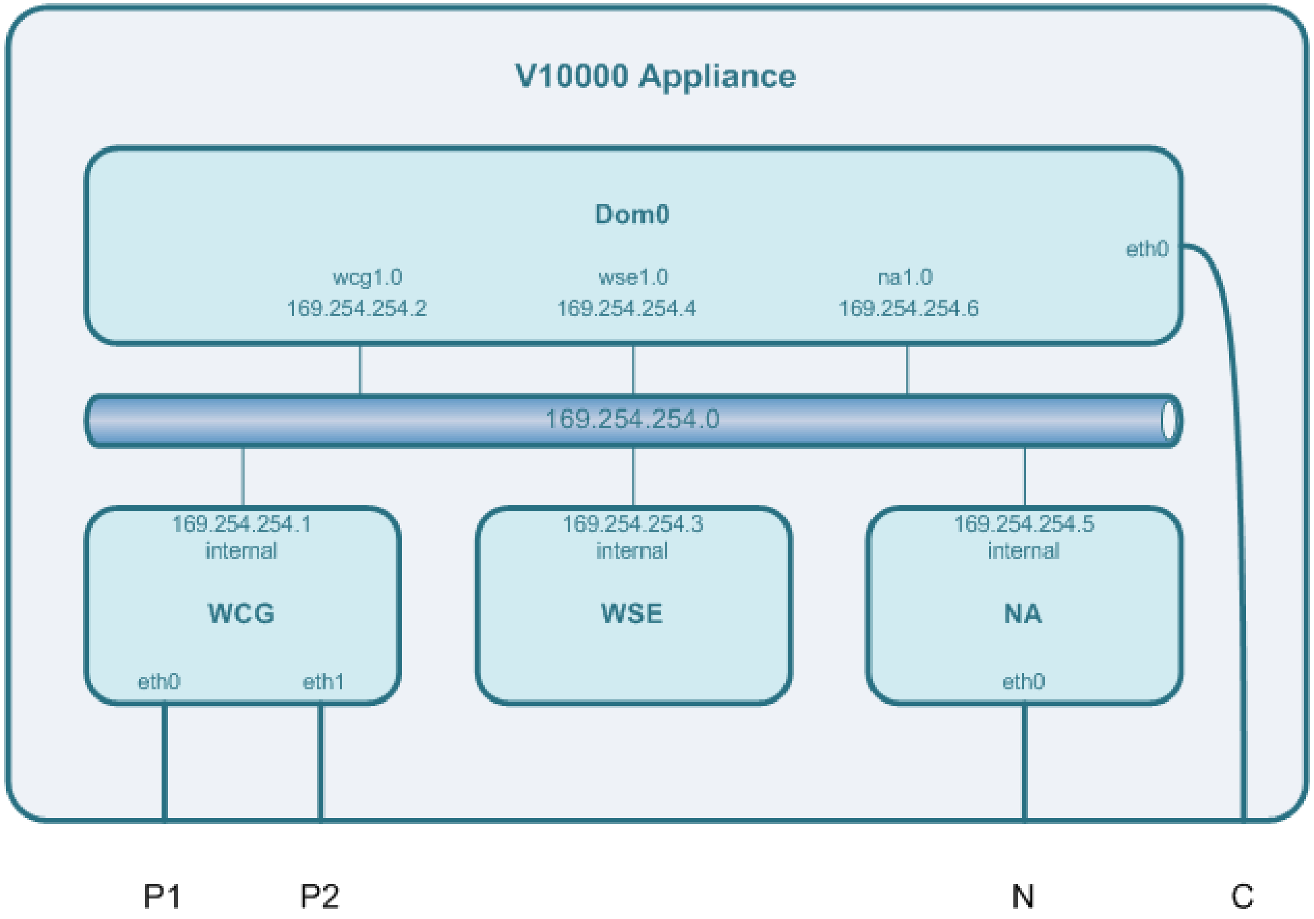
- Architecture



V-series Appliance

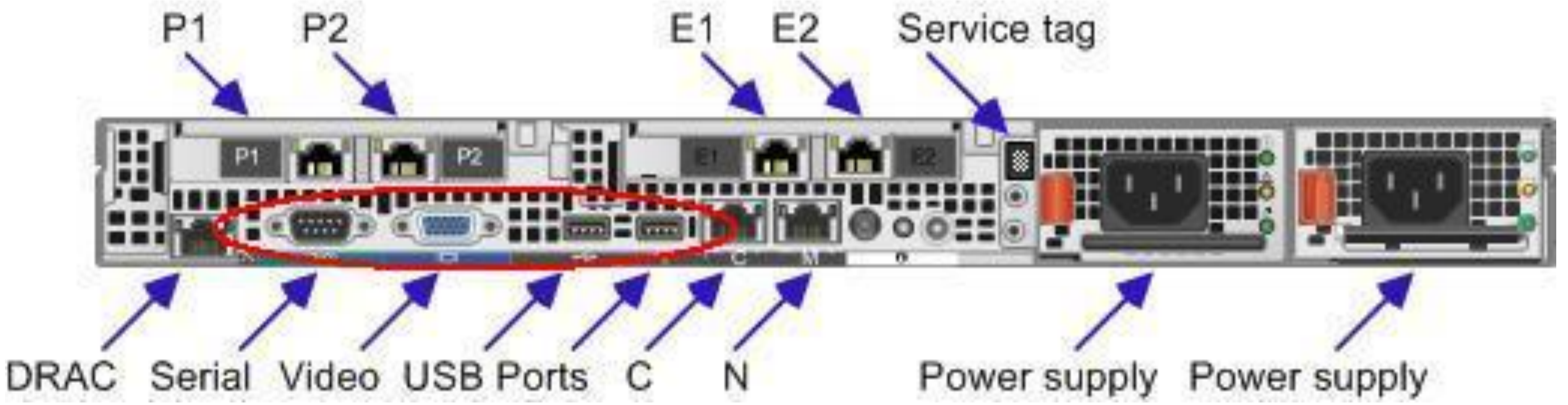
- Architecture

Understanding the IP addressing structure of the V-Series



V-series Appliance

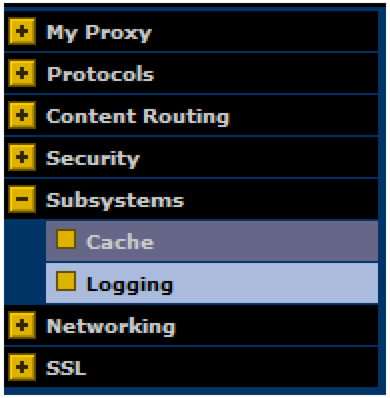
- Base platform information with illustrations

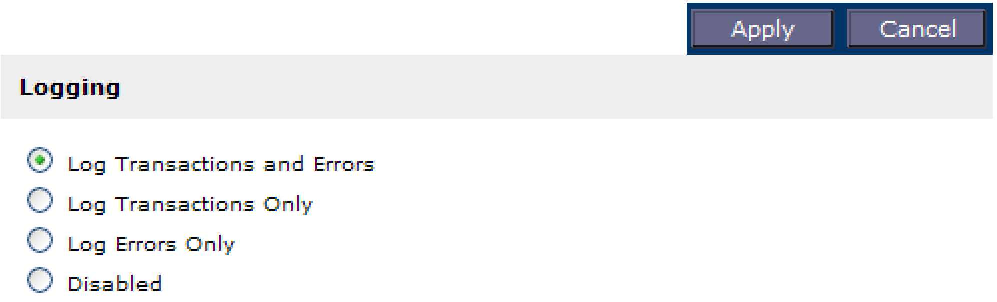


Understanding logs

Logging Essentials

- What is extended.log?
  - Accumulates record of traffic going through the proxy
  - Is turned off by default
  - When is an entry added to extended.log?
  - Turning on extended.log





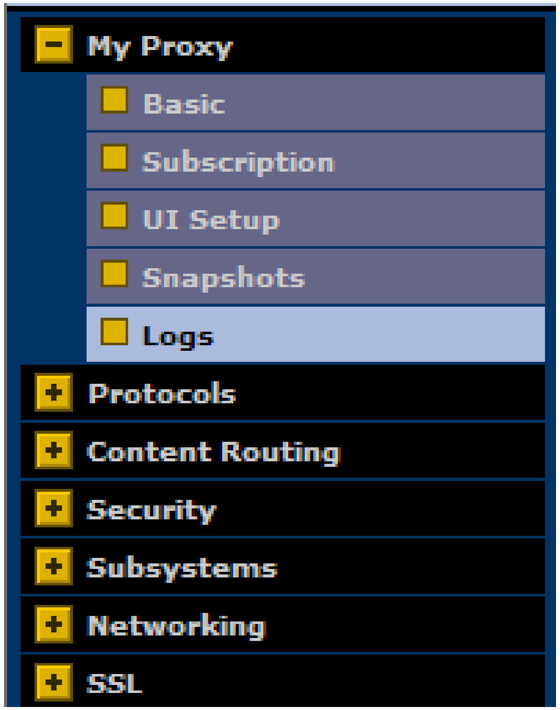
Logging

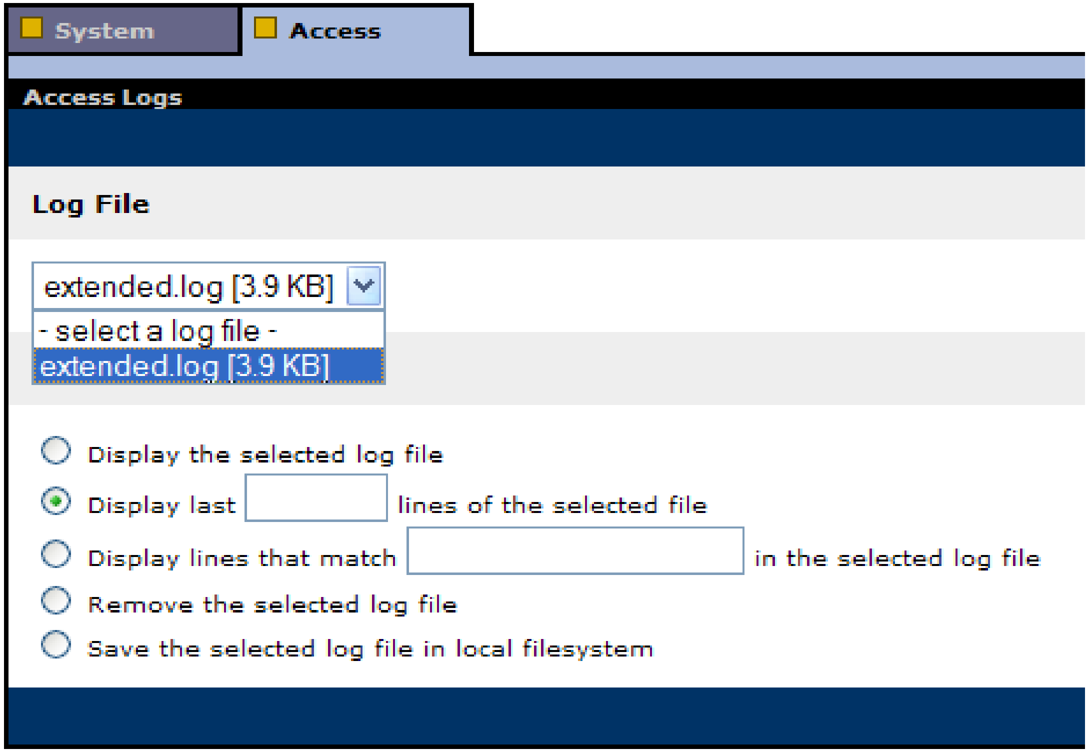
● Log Transactions and Errors
○ Log Transactions Only
○ Log Errors Only
○ Disabled

V-series Appliance

How to view extended.log:

- Viewing in the Content Gateway Manager GUI
- Go to: Configure > My Proxy > Logs and then the Access tab





Access Logs

Log File

extended.log [3.9 KB]

- select a log file -
extended.log [3.9 KB]

○ Display the selected log file

● Display last ☐ lines of the selected file

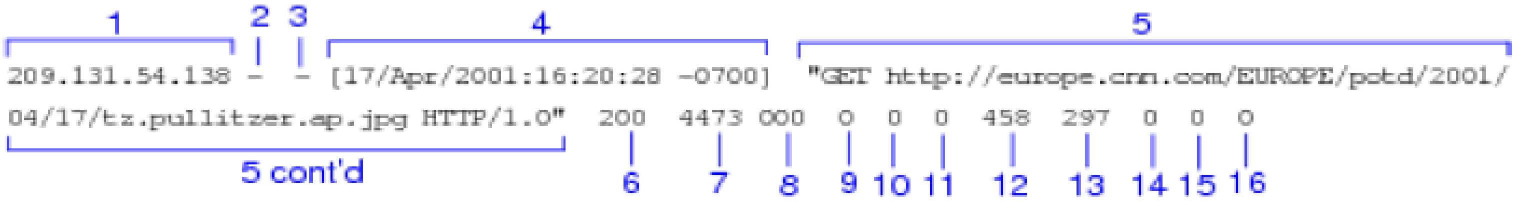
○ Display lines that match ☐ in the selected log file

○ Remove the selected log file

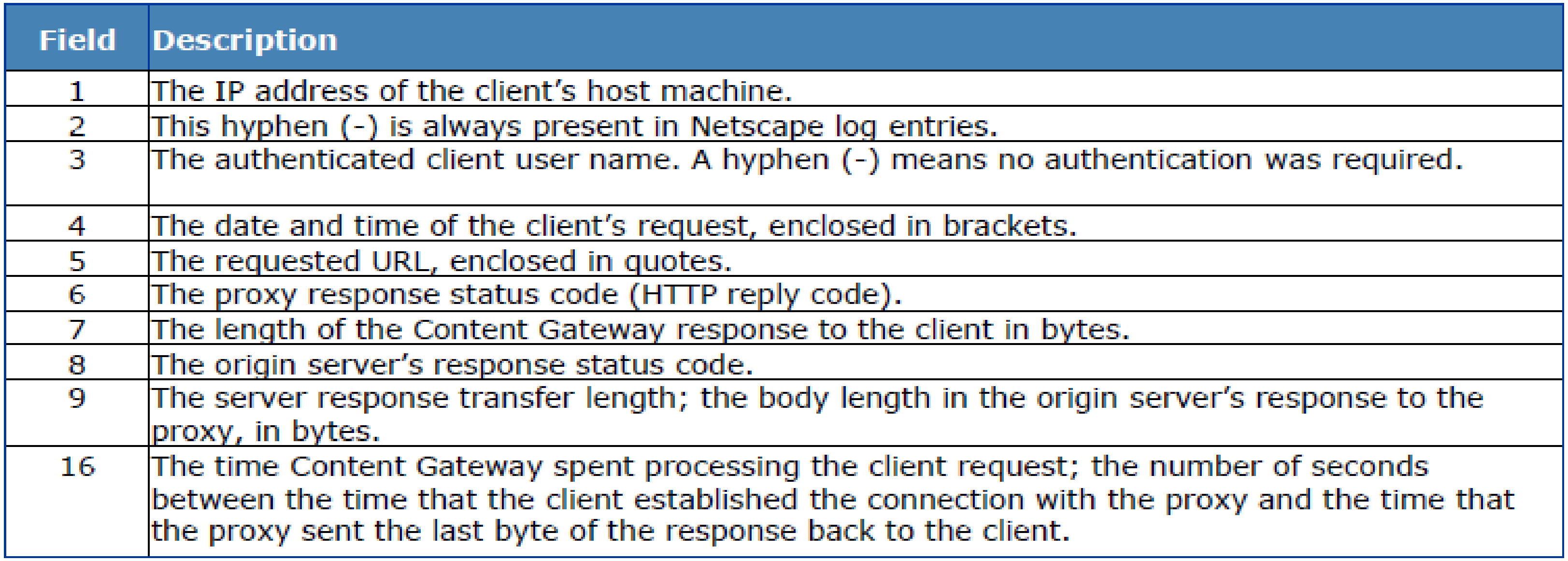
○ Save the selected log file in local filesystem

V-series Appliance

- Understanding extended.log
  - extended.log field descriptions:



```
209.131.54.138 - - [17/Apr/2001:16:20:28 -0700] "GET http://europe.cnn.com/EUROPE/potd/2001/
04/17/tz.pullitzer.ap.jpg HTTP/1.0" 200 4473 000 0 0 0 458 297 0 0 0
```



Field	Description
1	The IP address of the client’s host machine.
2	This hyphen (-) is always present in Netscape log entries.
3	The authenticated client user name. A hyphen (-) means no authentication was required.
4	The date and time of the client’s request, enclosed in brackets.
5	The requested URL, enclosed in quotes.
6	The proxy response status code (HTTP reply code).
7	The length of the Content Gateway response to the client in bytes.
8	The origin server’s response status code.
9	The server response transfer length; the body length in the origin server’s response to the proxy, in bytes.
16	The time Content Gateway spent processing the client request; the number of seconds between the time that the client established the connection with the proxy and the time that the proxy sent the last byte of the response back to the client.

Details can be found in Content Gateway Online Help by searching for “extended.log”.

V-Series Appliance

- Extended.log examples:

•Successful HTTP GET request:

```
10.0.0.1 --[06/Jul/2010:11:51:07 -0000] "GET http://www.websense.com/content/home.aspx HTTP/1.0" 200 64384 200 64384 0 0 204 250 233 222 0
```

•NTLM authentication interaction:

```
10.0.0.2 --[06/Jul/2010:11:54:20 -0000] "GET http://www.google.co.uk/ HTTP/1.1" 407 322 000 0 0 0 581 309 0 0 0
10.0.0.2 --[06/Jul/2010:11:54:20 -0000] "GET http://www.google.co.uk/ HTTP/1.1" 407 322 000 0 0 0 665 306 0 0 0

10.0.0.2 –USER1 [06/Jul/2010:11:54:20 -0000] "GET http://www.google.co.uk/ HTTP/1.1" 200 6076 200 6076 0 0 906 264 677 236 0
```

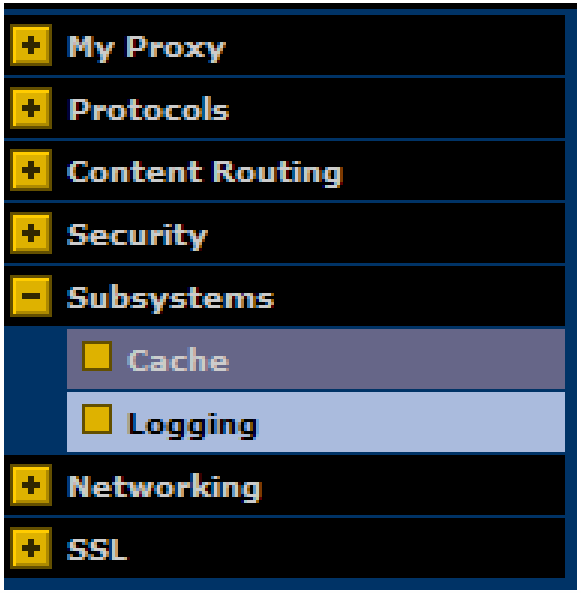
•Websense Block message:

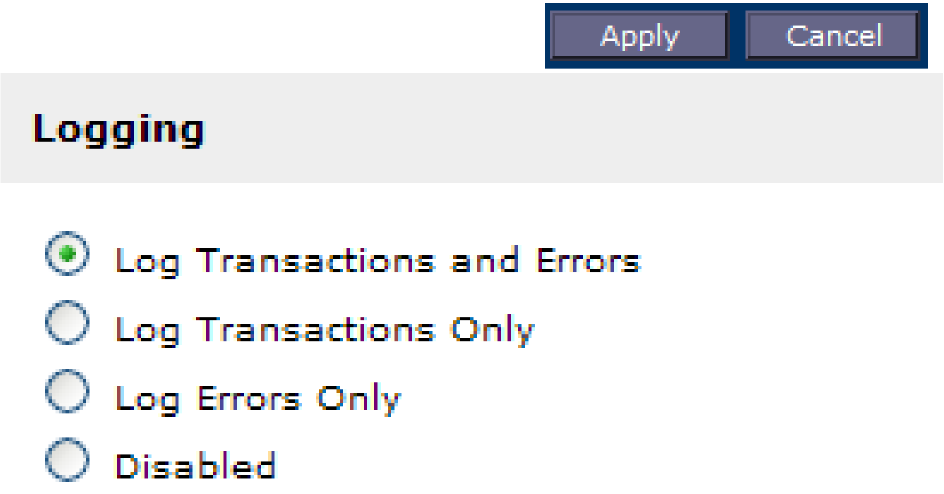
```
10.0.0.3 --[06/Jul/2010:11:57:55 -0000] "GET http://www.playboy.com/ HTTP/1.0" 302 0 000 0 0 0 133 187 0 0 0

10.0.0.3 --[06/Jul/2010:11:57:55 -0000] "GET http://10.0.0.20 1:15871/cgi-bin/blockpage.cgi?ws-session=687865857 HTTP/1.0" 200 1505 200 1505 0 0 141 144 170 118 0
```

V-Series Appliance

Understanding error.log

- What is error.log?
  - Accumulates record of traffic going through the proxy which was not processed correctly.
  - Is turned off by default
  - Turning on error.log





Logging

● Log Transactions and Errors
○ Log Transactions Only
○ Log Errors Only
○ Disabled

V-Series Appliance

- Error.log examples:

```
20100128.11h12m49s RESPONSE: sent 0.0.0.0 status 403 (Tunnel or SSL Forbidden) for 'talk.google.com:5222/'
```

This indicate the HTTPS request through port 5222 is not allowed. Add the port 5222 under Configure-> HTTP-> HTTPS Redirect

```
20100128.11h28m38s RESPONSE: sent <IP Address> status 504 (Maximum Transaction Time Exceeded) for
'http://0.channel35.facebook.com/x/3737112985/false/p_1576646402=0'
```

This indicates the request timed out, the server did not receive a timely response from the upstream/origin server specified by the URL.

Should be Protocols->HTTP->Timeouts->Active Timeouts.

```
20100128.11h28m39s RESPONSE: sent 0.0.0.0 status 400 (Invalid HTTP Request) for '/'
```

WCG has received a invalid response from the Origin Server.

Common issue and Troubleshooting

V-Series Appliance

Common Troubleshooting Scenarios

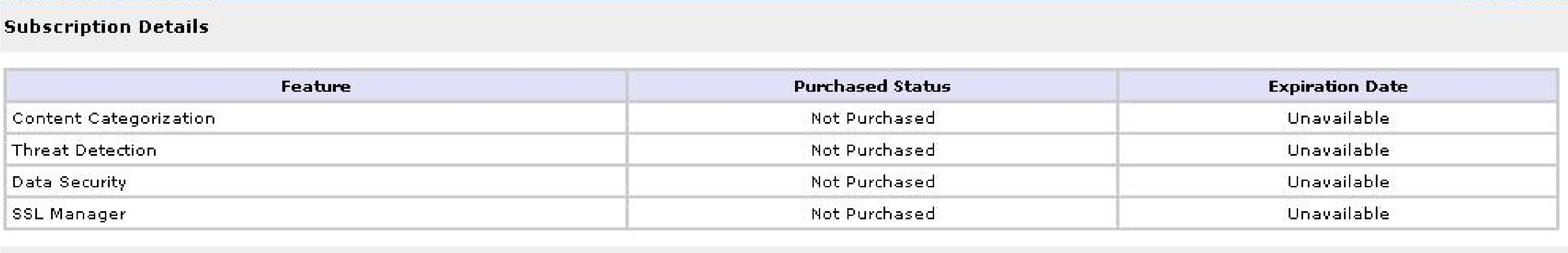
- Top 5 issues
  - Subscription issues
  - Database download failures
  - Unable to access a Web site
  - Patching V-series
  - Enable remote access for technical support

V-Series Appliance

Subscription issues

1. Subscription is not correctly registered in WCG manager.

2. Functionalities show as “Not-Purchased”



Subscription Details

Feature	Purchased Status	Expiration Date
Content Categorization	Not Purchased	Unavailable
Threat Detection	Not Purchased	Unavailable
Data Security	Not Purchased	Unavailable
SSL Manager	Not Purchased	Unavailable

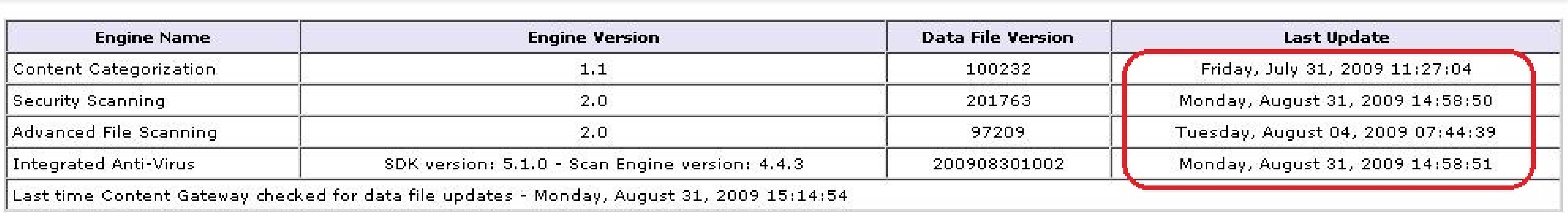
Resolution:

1. Make sure subscription is correctly enter in both WCG and WebsenseManager UI. Same subscription key needs to be used.
2. Verify that you have a working Internet connection.
3. Manually restart the WCG services will initiate a subscription check.
4. Need to enabled download service debug if issue can not be resolved.

V-Series Appliance

Database download failures

1. Database is not downloading.
2. Database is not updating.



Engine Name	Engine Version	Data File Version	Last Update
Content Categorization	1.1	100232	Friday, July 31, 2009 11:27:04
Security Scanning	2.0	201763	Monday, August 31, 2009 14:58:50
Advanced File Scanning	2.0	97209	Tuesday, August 04, 2009 07:44:39
Integrated Anti-Virus	SDK version: 5.1.0 - Scan Engine version: 4.4.3	200908301002	Monday, August 31, 2009 14:58:51
Last time Content Gateway checked for data file updates - Monday, August 31, 2009 15:14:54			

Resolution:

1. Verify the Internet connection for P1, check for possible connectivity issue.
2. Turn on DownloadService debug by modifying the \WCG\bin\downloadservice.ini

[DownloadService]

# Enable logging

EnableDebug=0 <Change value to "1">

V-Series Appliance

Database download failures (continued)

3. Restart the download service with command ./init_download in WCG/bin directory.

4. downloadservice.log will be created in WCG/Logs directory.

Sample error in downloadservice.log:

- [08-31-20010 15:31:10.89577] DIAG: Error connecting to proxy server
- [08-31-20010 15:31:10.89613] DIAG: Error connecting to Websense DDS

Not able to connect to download.websense.com through defined proxy, possible connectivity issue.

V-Series Appliance

- Unable to access a Web site through V-series

1. Verify if the URL can be accessed from other segments of the network.
2. Verify the URL can be reached form the V-series with a wget command from WCG domain.
3. Go through the extended.log to see if the cause can be determined from the HTTP response code. A typical HTTP 500 would indicate a Origin Server side issue.
4. Issue with HTTPs site that requires a client side certificate, site to be added into the HTTPs incident and tunneled.
5. Verify the URL is not blocked by Real-time scanning through testlogserver utility.

V-Series Appliance

Patching V-series

How do I get all patches for the Websense V-Series appliance?

Resolution

Websense periodically provides patches to address important V-Series product issues.

Applying a patch

1) First, download the new patch from the Web address provided in your Websense Product Alert message from Technical Support. A user name and password are required. These credentials are included in the Product Alert message.

Use the Administration > Patch Management screen on the V-Series Console to upload and install software patches and review patch history.

2) After a patch is on your network, during a low usage period on your network, use the Administration > Patch Management screen to upload and install the patch on the appliance.

Enable remote access for technical support

How do I enable Remote Access to my Websense V10000 appliance?

Resolution

Enable remote access to the V10000 appliance only at the request of Websense Technical Support.

Log on to the V10000 Console.

Navigate to the page **Administration > Support Tools**.

Check **Enable Remote Access,** and then click **Save**. A passcode is generated and displayed on screen.

Write down the passcode and provide it to your Websense Technical Support technician. This enables SSH, so that the technician can log on to your appliance.

Each time you allow remote access to the V10000 and a Websense technician logs on, a record is added to the **Remote access login history** at the bottom of the **Support Tools** screen.

When the Websense technician is done, be sure to click **Disable remote access** and click **Save** to disable the access.

websense Yes!

ESSENTIAL INFORMATION PROTECTION™

Websense Data Security Suite

Data Security Suite

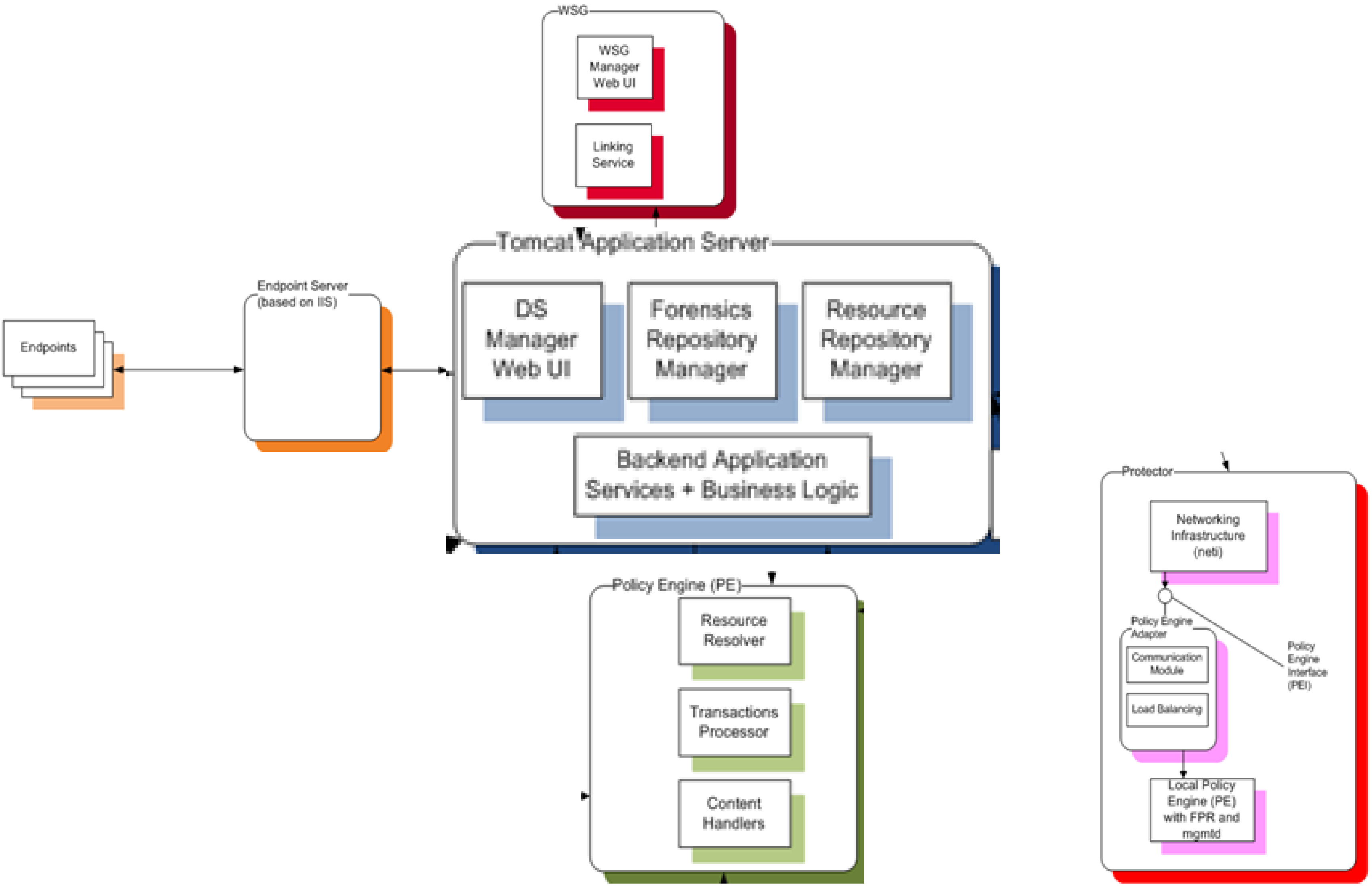
- General introduction of DSS
- Architecture overview
- Which error log files are created, and where they are stored?
  - Names of the logs
  - Structure of the logs
  - How archived data is stored
- Helpful information you can obtain from the log files
- Common Troubleshooting Scenarios
  - Standard troubleshooting procedures for End-point component .

DSS – General Goals

- Provide solution for actual and potential Data Loss Prevention
- Classify the information within organization
- Control over information and sensitive data
- Control over information usage by insiders
- Address Potential / Real Data Loss Use Cases:
  - Data in Motion (SMTP / HTTP / FTP / IM etc)
  - Data at Rest (Windows Shares / DMSs)
  - Data in Use (Endpoint)

Architecture and Components

High Level Architecture Diagram


WSG
WSG Manager Web UI
Linking Service
Tomcat Application Server
DS Manager Web UI
Forensics Repository Manager
Resource Repository Manager
Backend Application Services + Business Logic
Endpoints
Endpoint Server (based on IIS)
Policy Engine (PE)
Resource Resolver
Transactions Processor
Content Handlers
Protector
Networking Infrastructure (neti)
Policy Engine Adapter
Communication Module
Load Balancing
Policy Engine Interface (PEI)
Local Policy Engine (PE) with FPR and mgmtd

Main Components

- Management (based on tomcat)
- Policy Engine
- Protector
- Endpoint
- Agents
- WCG / WSG

Logs

Tomcat Logs

- Each web application has its own log4j configuration in addition to one master configuration, the configuration files are in *%dss_home%\tomcat\lib* and they are named:
  - **log4j.properties** – the master configuration
  - **log4j-mng.properties** – the DSS manager logging configuration
  - **log4j-forensics.properties** – the Forensics Repository logging configuration
- These configuration files are reread every 30 seconds. No need for a service restart.

Logs - Data Security Manager

- The DSS Manager log files are in *%dss_home%\Tomcat\logs\mng*
  - **mng-all.log** – this is the most important file containing all of the log records (from all of the components)
  - The rest of the logs are component specific and are included in mng-all.log.
- Changing the Logging Level
  - Edit *%dss_home%\Tomcat\lib\log4j-mng.properties*
  - Change the following from WARN to DEBUG:
    - log4j.logger.com.pa=WARN, PA
    - log4j.logger.com.websense=WARN, PA

PolicyEngine Logs

- Under %dss_home%\Logs
- %dss_home%\conf\PolicyEngine.log.config
- PolicyEngine.log.config topics
  - TransactionMonitor – Basic transaction parameters, transaction analysis time. Save extracted text under temp folder
  - SaveIntermediateFiles – save xml for management under IncidentTemp

Collect all logs

- Under tasks and run DSS statistics
- Collect the latest zip file from %dss_home%\Stats
- It contains all the latest logs from mng server.

Protector Logs

- /opt/websense/neti/log
  - Health_check.log – Health check script log
  - Net.log\netd.log – network messages logs
  - Pama\pamad.log – the main Protector process logs
  - Pamad_PEInterface.log – Pama's policy engine interface log
    - Enabling debug logging - edit */opt/websense/neti/conf/pamad_PEInterface.log.conf*
  - pawd.log – "classic" Protector watchdog log
  - Plat\platd.log – communication log with management daemons (deploy settings)
  - Registration.log – protector registration log
  - Spicer-chat\spicer-xact.log – ICAP logs
  - Icap_PEInterface.log – ICAP PE interface log
    - Enabling debug logging - edit */opt/websense/neti/conf/icap_PEInterface.log.conf*
  - Syslog_client.log – syslog related messages log

Logs – Policy Engine

- /opt/websense/PolicyEngine/Logs
  - FPR.log – fingerprints repository logs
    - To enable debug logging edit FPR.log.config
  - Mgmtd.log – management daemon log. Used for communication between other management daemons and the Protector's platd.
    - To enable debug logging edit mgmtd.log.config
  - PolicyEngine.log – Policy Engine log
    - To enable debug logging edit PolicyEngine.log.config
  - Watchdog.log – FPR\PE\mgmtd watchdog log

Trouble shoot End-point

- DSER log

  Located at INSTALLDIR\DebugDump.txt

  - The default installation directory is C:\Program Files\Websense\Data Security\Websense Data Endpoint

  Logging level can be changed to 'debug' using the registry:

  1. In the regedit registry editor, go to: Computer --> HKEY_LOCAL_MACHINE --> SOFTWARE --> Websense --> Agent --> DSE
  2. Create a new REG_DWORD named *debug_mode*
  3. Change the value of *debug_mode* to 1.

- Collect all logs:
  – Run clientinfo.exe under INSTALLDIR
  – The zip file is sent to the desktop in the format ClientInfo_WORKSTATION_Date.zip

Technical Support Process

Creating Support Ticket

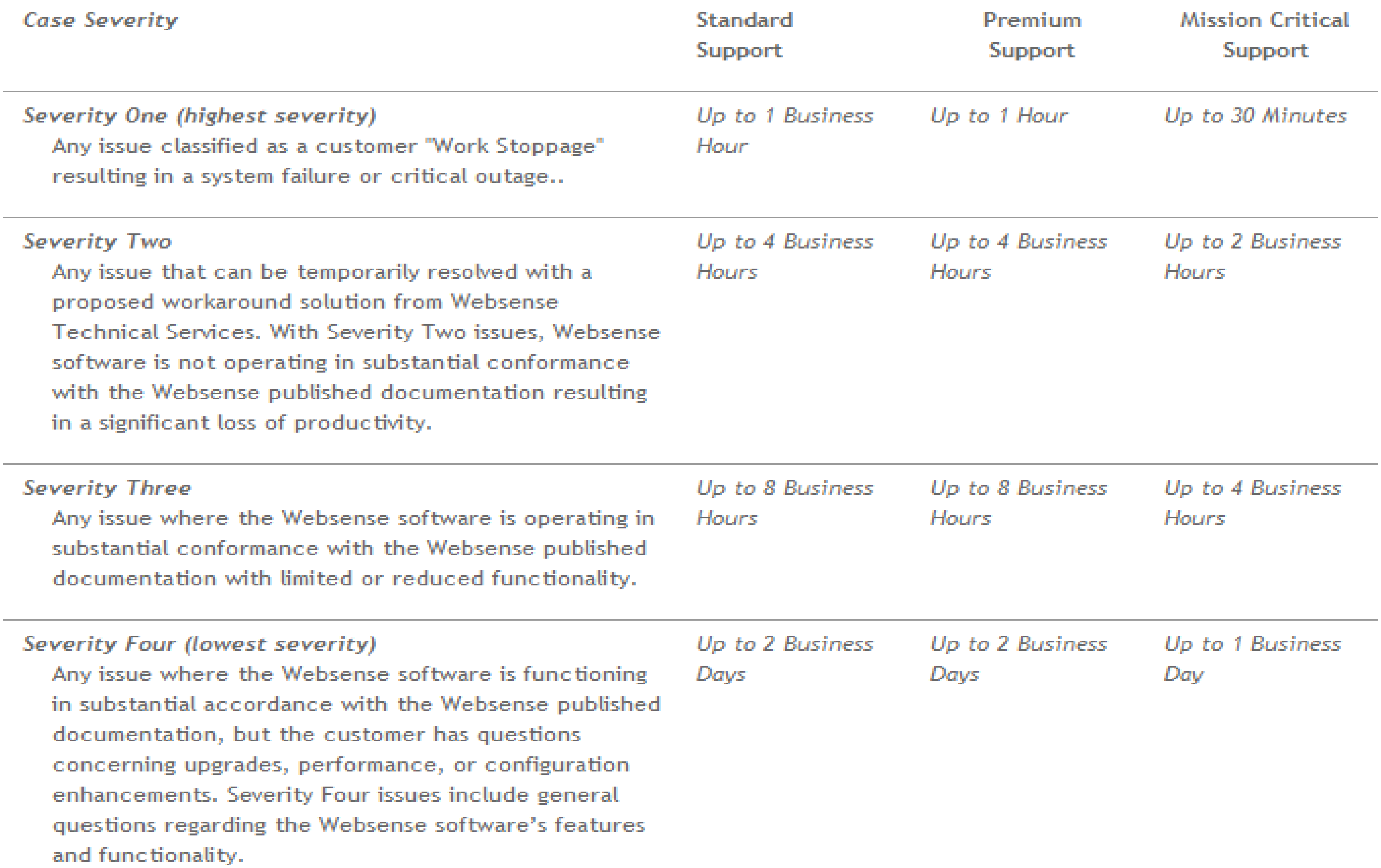
- Call support line
  - •Asia: +86-1058844200
  - •Australia/New Zealand: +61 2 9414 0033
  - •India: +1.858.332.0061

- Preferred information:
  - Product name and version
  - Subscription key

Creating Support Ticket

- Open ticket on line, here are two ways to access your support cases:
  - Via MyWebsense
  - Via ask.websense.com
    - Log into ask.websense.com from any access point on the website with your MyWebsense log-in credentials.
    - If you are a Partner, you will be directed to the Partner Portal.
- Click on ‘Create a New Case’ link or ‘Case’ tab to create a new case
  - Provide details on required fields
  - Provide a brief case subject
  - For faster resolution:
    - Provide a detailed problem description
    - http://www.websense.com/content/CaseInformationList.aspx
  - Partner is required to correctly enter the end-use account name.
- Click on ‘View Existing Cases’ link to view existing cases
  - Select options from dropdown menu to view open/closed/all cases.

Targeted response time



Case Severity	Standard Support	Premium Support	Mission Critical Support
Severity One (highest severity) Any issue classified as a customer "Work Stoppage" resulting in a system failure or critical outage..	*Up to 1 Business Hour*	*Up to 1 Hour*	*Up to 30 Minutes*
Severity Two Any issue that can be temporarily resolved with a proposed workaround solution from Websense Technical Services. With Severity Two issues, Websense software is not operating in substantial conformance with the Websense published documentation resulting in a significant loss of productivity.	*Up to 4 Business Hours*	*Up to 4 Business Hours*	*Up to 2 Business Hours*
Severity Three Any issue where the Websense software is operating in substantial conformance with the Websense published documentation with limited or reduced functionality.	*Up to 8 Business Hours*	*Up to 8 Business Hours*	*Up to 4 Business Hours*
Severity Four (lowest severity) Any issue where the Websense software is functioning in substantial accordance with the Websense published documentation, but the customer has questions concerning upgrades, performance, or configuration enhancements. Severity Four issues include general questions regarding the Websense software's features and functionality.	*Up to 2 Business Days*	*Up to 2 Business Days*	*Up to 1 Business Day*

Support online resources

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

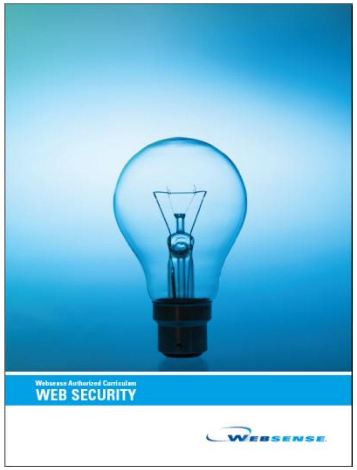
- Create and manage support service requests using our online portal.

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



Questions?