

Quick Start 3: Installing and configuring Websense Web Security Gateway v7.7

Websense Support Webinar February 2013

TRITON™

Web security

Email security

Data security

Mobile security



Greg Didier

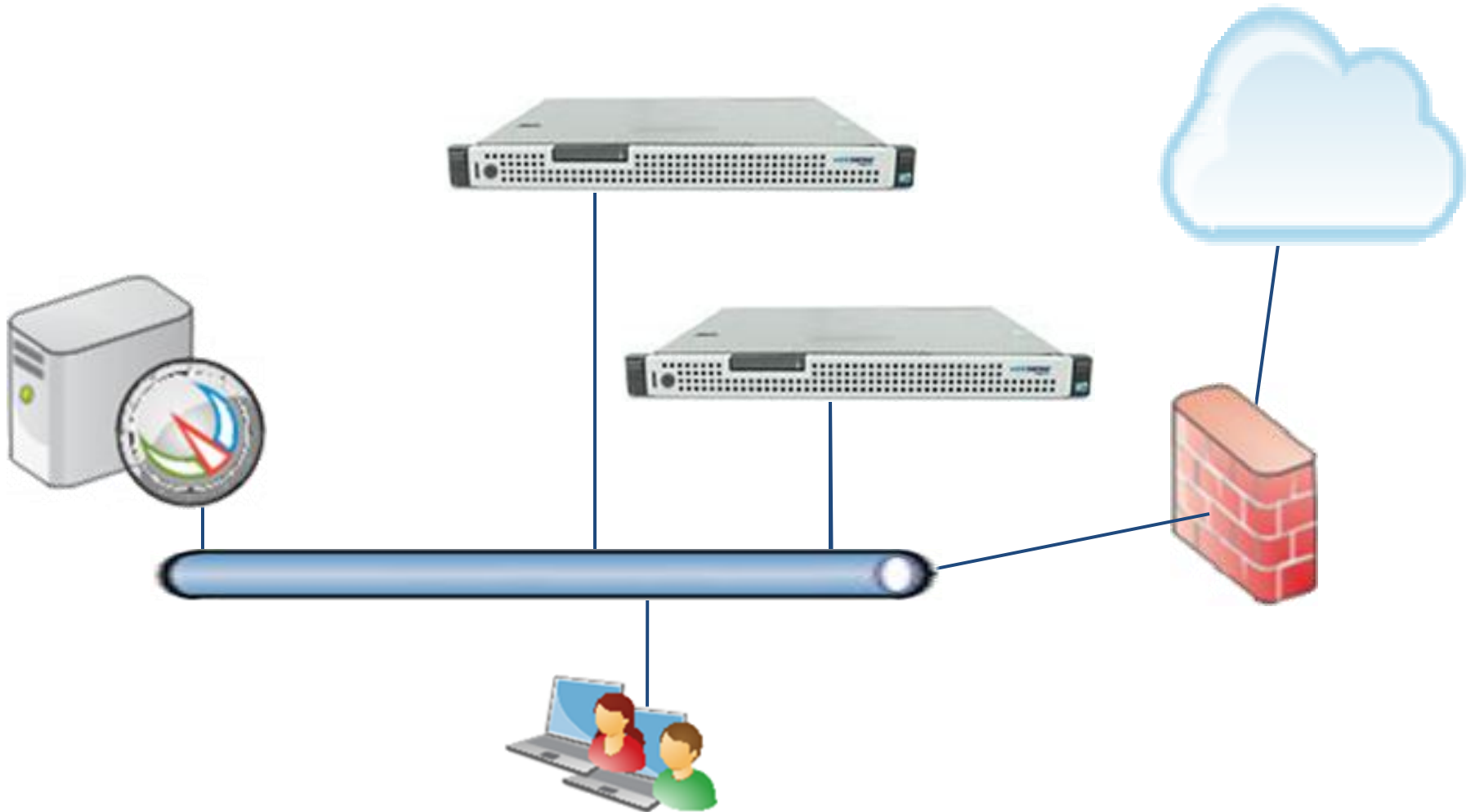
- **Title:**
 - Support Specialist
- **Accomplishments:**
 - 9 years supporting Websense products
- **Qualifications:**
 - Technical Support Mentor
 - Product Trainer

- Pre-installation considerations
- Installation steps
 - V-Series appliance
 - Red Hat Enterprise Linux
- Content Gateway initial configuration
 - Clustering
 - Virtual IP
 - WCCP redirection
 - DNS Proxy caching
 - SSL content inspection
 - Authentication

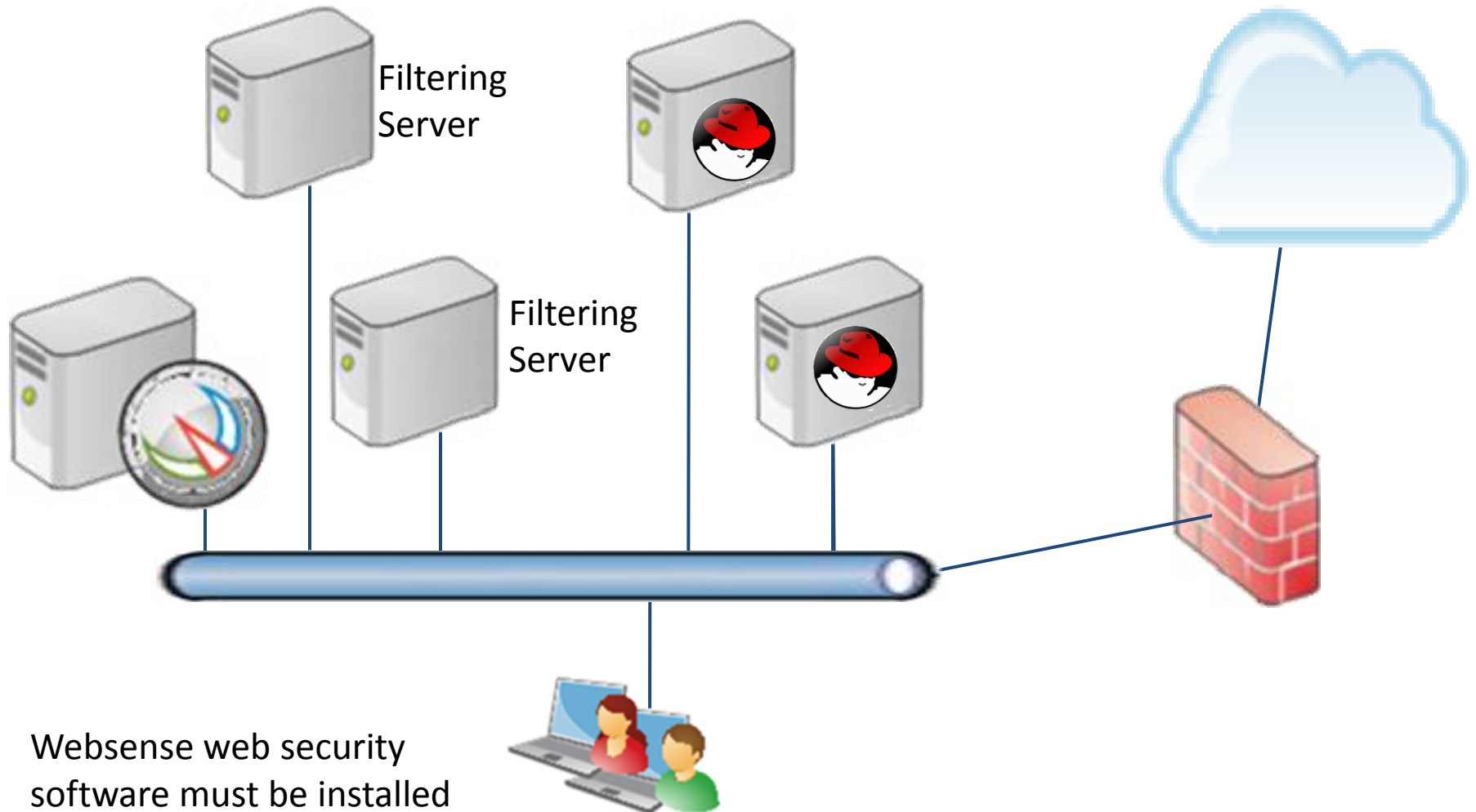
- Websense Content Gateway deployment options
 - As a Web proxy cache
 - Content Gateway serves the content directly
 - In a cache hierarchy
 - Internet requests can be routed to other regional caches
 - In a managed cluster
 - Cluster nodes automatically share configuration information
 - As an SSL server
 - HTTPS data is decrypted, inspected, and then re-encrypted
 - As a DNS proxy cache
 - Reduces response times for DNS lookups

- Proxy platforms
 - V-Series appliance
 - Software
- Sending traffic to the Content Gateway web proxy
 - Explicit proxy
 - Transparent proxy

Deployment Considerations



Deployment Considerations



Websense web security software must be installed prior to Content Gateway.

- Websense Content Gateway is the web proxy for Web Security Gateway

The screenshot displays the Websense V5000 G2 management console. The top navigation bar includes the 'Status' tab, a 'General' section, and a 'Configuration' section. The 'General' section is expanded, showing 'CPU and Memory', 'Disk Usage', and 'Network Bandwidth'. The 'Configuration' section is also expanded, showing 'Configuration' and 'Administration'. The 'Status' tab is selected, and the 'General' section is expanded. The 'Websense Content Gateway' section is highlighted with a red box. This section displays 'Resources Used' (CPU(s): 4, RAM: 3.94 GB, Interface(s): P1 (dedicated), P2 (dedicated), C (shared)) and 'Services' (Content Cop, Content Gateway, Content Gateway Manager). The 'Websense Web Security' section is also visible below, showing 'Resources Used' (CPU(s): 2, RAM: 1.97 GB, Interface(s): C (shared)) and 'Services' (Filtering Service, Policy Database, Policy Broker, Policy Server, User Service, Policy Server, User Service).

General

Alerts

✓ No alerts to report.

Appliance Controller

Resources Used:

CPU(s): 2
RAM: 1.96 GB
Interface(s): ✓ C (shared)

[Restart Appliance](#)
[Shutdown Appliance](#)

☐ Monitor status without timing out

Websense Content Gateway

Resources Used:

CPU(s): 4
RAM: 3.94 GB
Interface(s): ✓ P1 (dedicated)
✓ P2 (dedicated)
✓ C (shared)

[Restart Module](#)

Services:

✓ Content Cop
✓ Content Gateway
✓ Content Gateway Manager [Launch](#)

[Stop Services](#)

Websense Web Security

Resources Used:

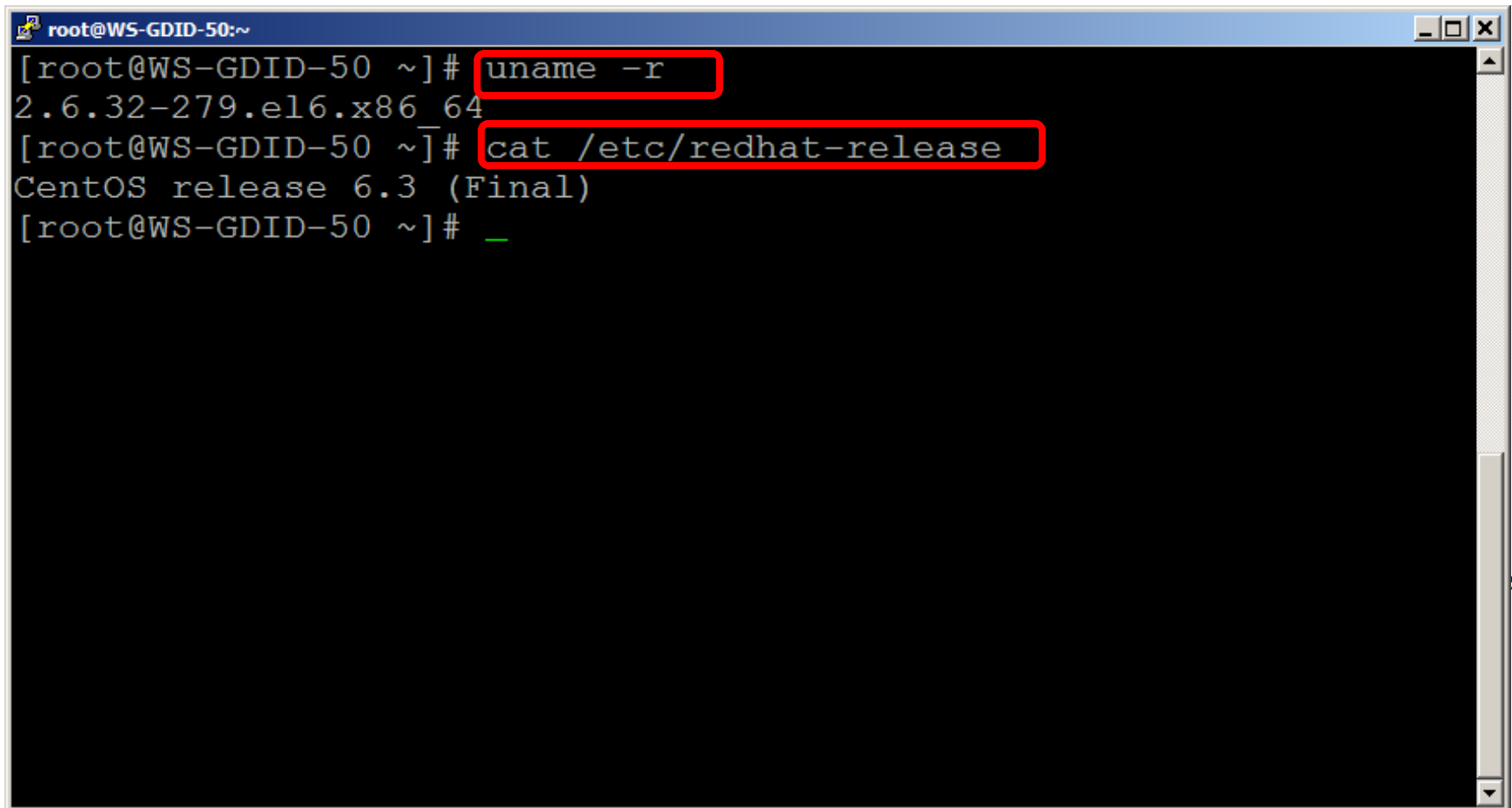
CPU(s): 2
RAM: 1.97 GB
Interface(s): ✓ C (shared)

Services:

✓ Filtering Service
✓ Policy Database
✓ Policy Broker
✓ Policy Server
✓ User Service
✓ Policy Server
✓ User Service

- Verify system hardware requirements
- Verify kernel version support
 - Websense Content Gateway v7.7.3 is certified on:
 - Red Hat Enterprise Linux, 6 series, updates 0, 1, 2, and 3, Basic Server, 64-bit
 - » Kernel version for 6.0: 2.6.32-71
 - » Kernel version for 6.1: 2.6.32-131
 - » Kernel version for 6.2: 2.6.32-220
 - » Kernel version for 6.3: 2.6.32-279
 - Red Hat Enterprise Linux, 5 series, updates 3, 4, 5, 6, and 7, Basic or Advanced Platform, 32-bit only

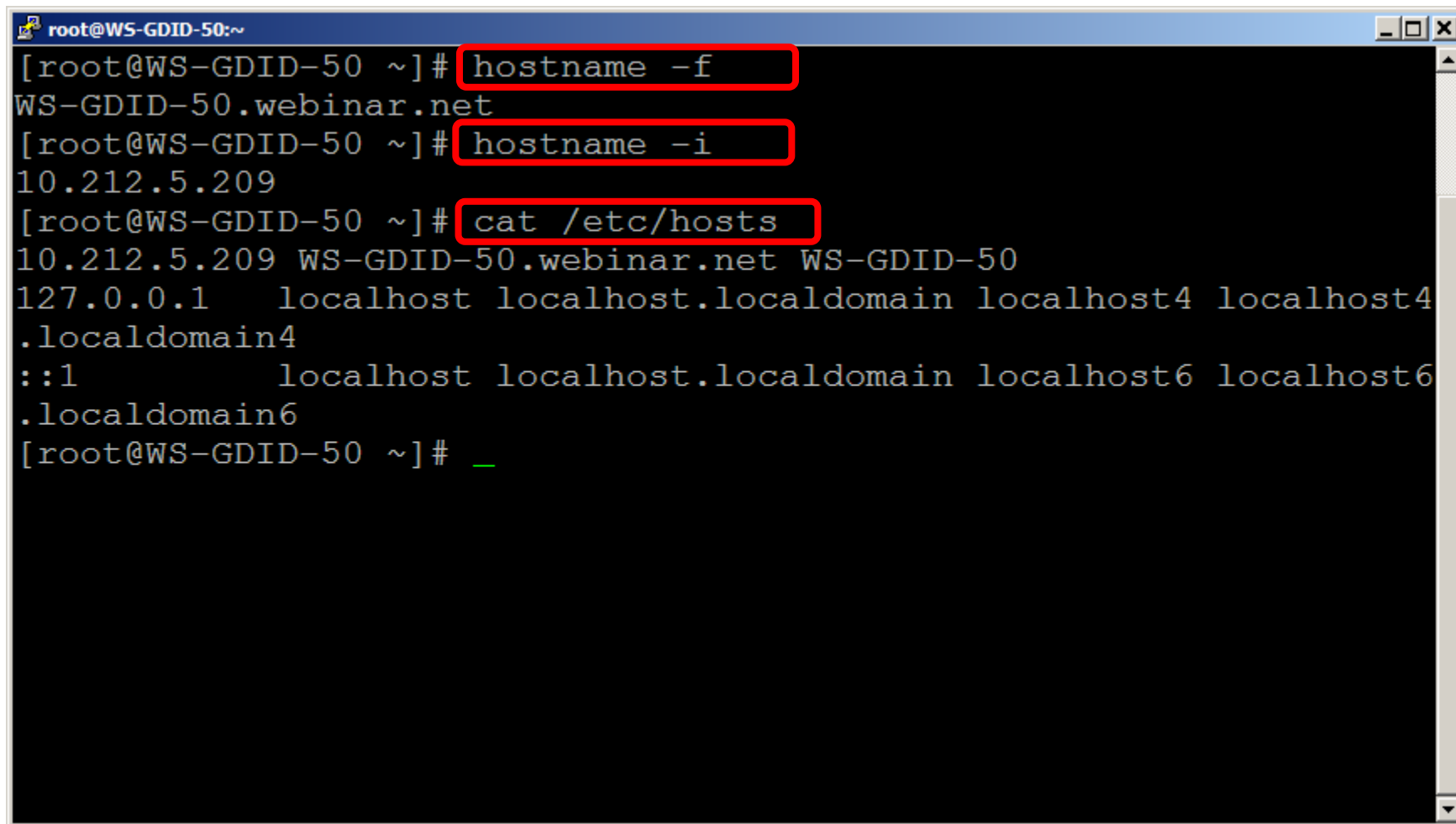
- Verify system hardware requirements
- Verify kernel version support



A terminal window titled 'root@WS-GDID-50:~' showing the execution of two commands. The first command, 'uname -r', is highlighted with a red box and returns the output '2.6.32-279.el6.x86_64'. The second command, 'cat /etc/redhat-release', is also highlighted with a red box and returns the output 'CentOS release 6.3 (Final)'. The prompt returns to the root user after each command.

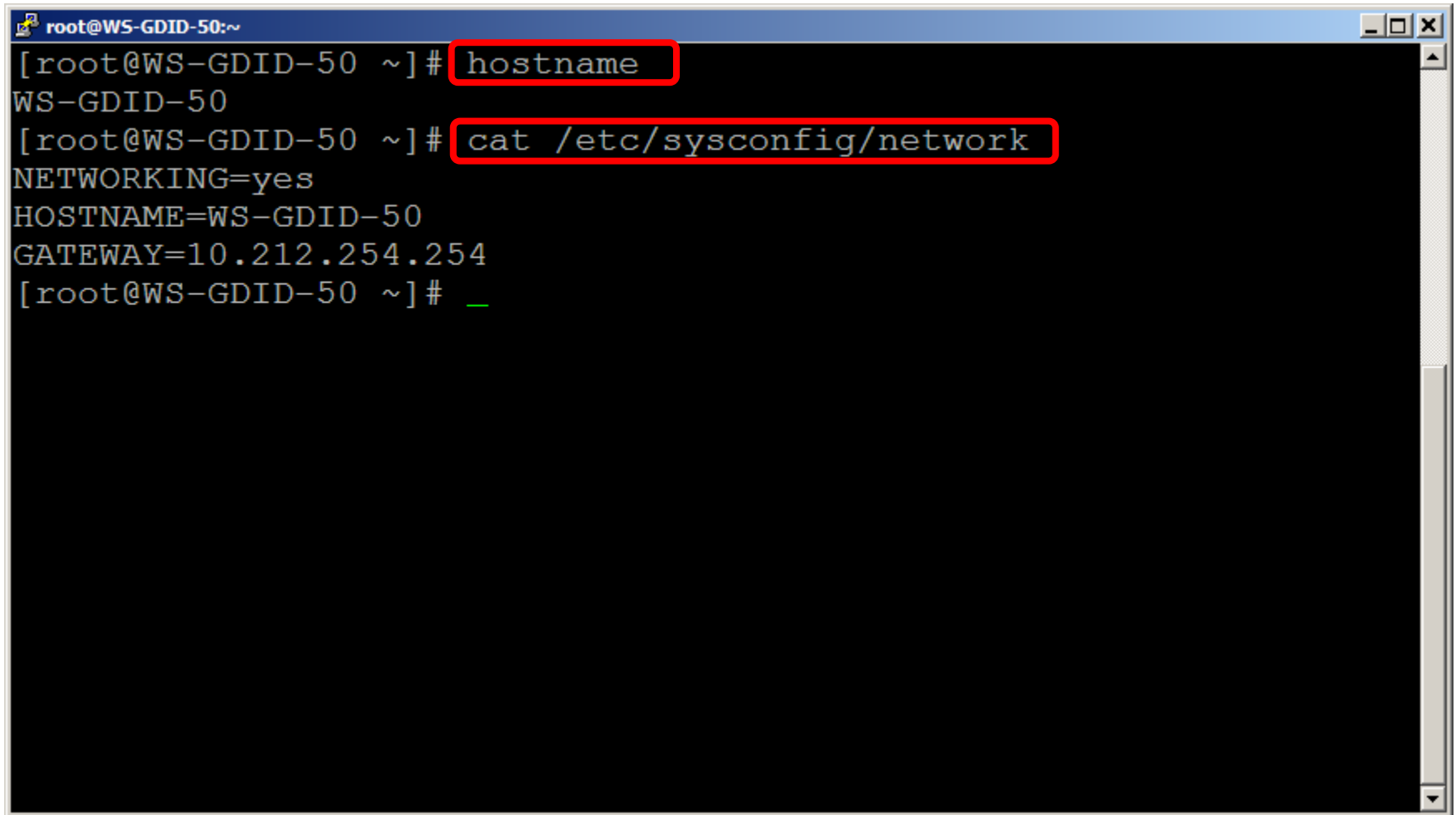
```
root@WS-GDID-50:~  
[root@WS-GDID-50 ~]# uname -r  
2.6.32-279.el6.x86_64  
[root@WS-GDID-50 ~]# cat /etc/redhat-release  
CentOS release 6.3 (Final)  
[root@WS-GDID-50 ~]# _
```

- Verify the IP address associated with the hostname



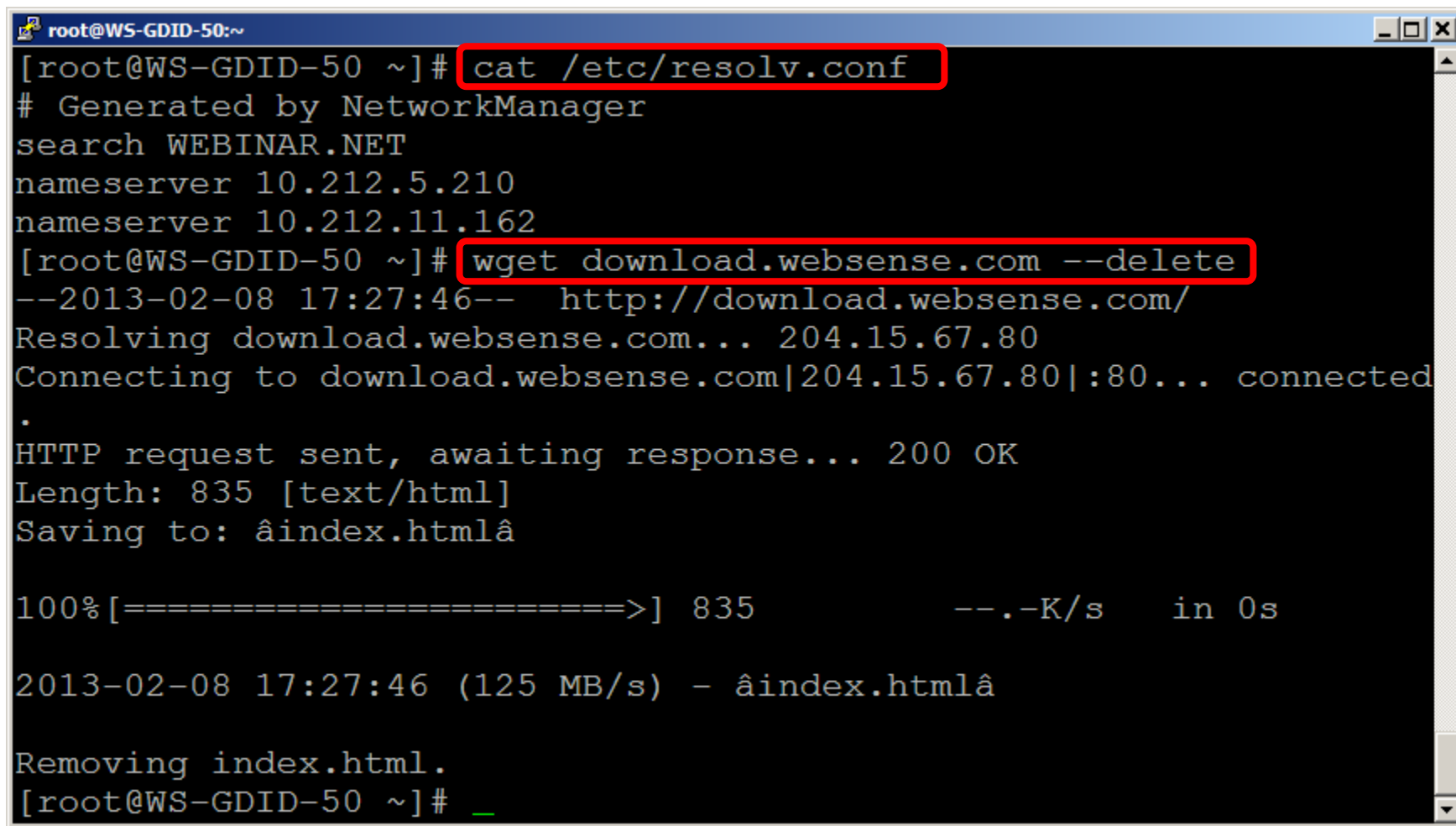
```
root@WS-GDID-50:~  
[root@WS-GDID-50 ~]# hostname -f  
WS-GDID-50.webinar.net  
[root@WS-GDID-50 ~]# hostname -i  
10.212.5.209  
[root@WS-GDID-50 ~]# cat /etc/hosts  
10.212.5.209 WS-GDID-50.webinar.net WS-GDID-50  
127.0.0.1 localhost localhost.localdomain localhost4 localhost4  
.localdomain4  
::1 localhost localhost.localdomain localhost6 localhost6  
.localdomain6  
[root@WS-GDID-50 ~]# _
```

- Verify the hostname and default gateway

A terminal window titled 'root@WS-GDID-50:~' with standard window controls. The terminal shows two commands being executed. The first command, 'hostname', is highlighted with a red box and returns 'WS-GDID-50'. The second command, 'cat /etc/sysconfig/network', is also highlighted with a red box and returns 'NETWORKING=yes', 'HOSTNAME=WS-GDID-50', and 'GATEWAY=10.212.254.254'. A green cursor is visible at the end of the last prompt line.

```
root@WS-GDID-50:~  
[root@WS-GDID-50 ~]# hostname  
WS-GDID-50  
[root@WS-GDID-50 ~]# cat /etc/sysconfig/network  
NETWORKING=yes  
HOSTNAME=WS-GDID-50  
GATEWAY=10.212.254.254  
[root@WS-GDID-50 ~]# _
```

- Verify the DNS specification

A terminal window titled 'root@WS-GDID-50:~' with standard window controls. The terminal shows the execution of two commands. The first command, 'cat /etc/resolv.conf', is highlighted with a red box and shows the contents of the file, including the search domain 'WEBINAR.NET' and two nameservers. The second command, 'wget download.websense.com --delete', is also highlighted with a red box. The output of the second command shows the file being resolved to IP 204.15.67.80, connected to port 80, and successfully downloaded as 'index.html' with a 200 OK status. The terminal ends with a prompt and a cursor.

```
root@WS-GDID-50:~  
[root@WS-GDID-50 ~]# cat /etc/resolv.conf  
# Generated by NetworkManager  
search WEBINAR.NET  
nameserver 10.212.5.210  
nameserver 10.212.11.162  
[root@WS-GDID-50 ~]# wget download.websense.com --delete  
--2013-02-08 17:27:46-- http://download.websense.com/  
Resolving download.websense.com... 204.15.67.80  
Connecting to download.websense.com|204.15.67.80|:80... connected  
.  
HTTP request sent, awaiting response... 200 OK  
Length: 835 [text/html]  
Saving to: âindex.htmlâ  
  
100%[=====>] 835 --.-K/s in 0s  
  
2013-02-08 17:27:46 (125 MB/s) - âindex.htmlâ  
  
Removing index.html.  
[root@WS-GDID-50 ~]# _
```

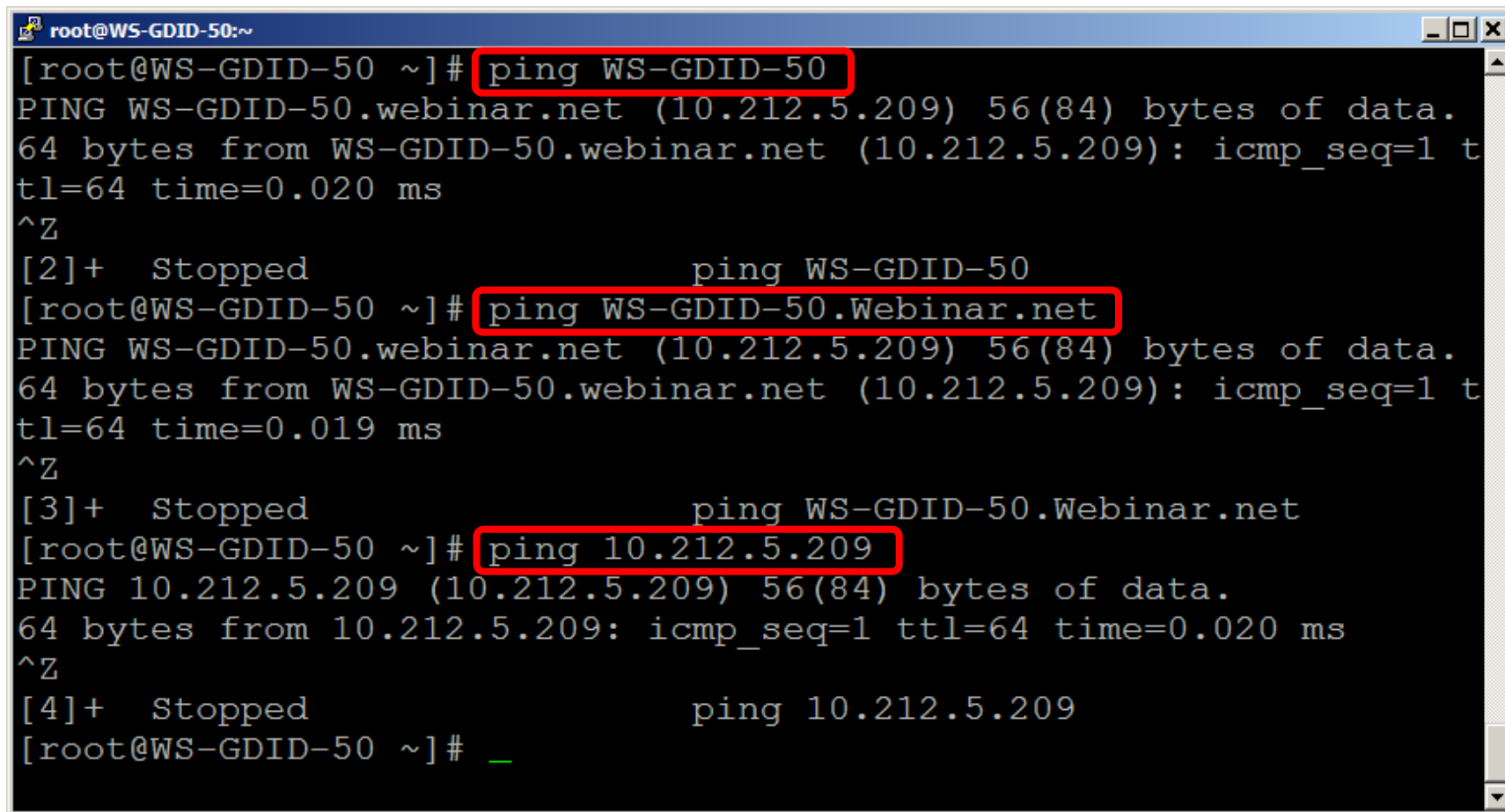
- Verify DNS

```
root@WS-GDID-50:~  
[root@WS-GDID-50 ~]# nslookup  
> www.yahoo.com  
Server:          10.212.5.210  
Address:         10.212.5.210#53  
  
Non-authoritative answer:  
www.yahoo.com    canonical name = fd-fp3.wg1.b.yahoo.com.  
fd-fp3.wg1.b.yahoo.com canonical name = ds-fp3.wg1.b.yahoo.com.  
ds-fp3.wg1.b.yahoo.com canonical name = ds-any-fp3-lfb.wal.b.yahoo.com.  
ds-any-fp3-lfb.wal.b.yahoo.com canonical name = ds-any-fp3-real.wal.b.yahoo.com.  
Name:   ds-any-fp3-real.wal.b.yahoo.com  
Address: 206.190.36.45  
Name:   ds-any-fp3-real.wal.b.yahoo.com  
Address: 98.138.253.109  
> 98.138.253.109  
Server:          10.212.11.162  
Address:         10.212.11.162#53  
  
Non-authoritative answer:  
109.253.138.98.in-addr.arpa    name = ir1.fp.vip.net1.yahoo.com.
```

- Verify the routing table

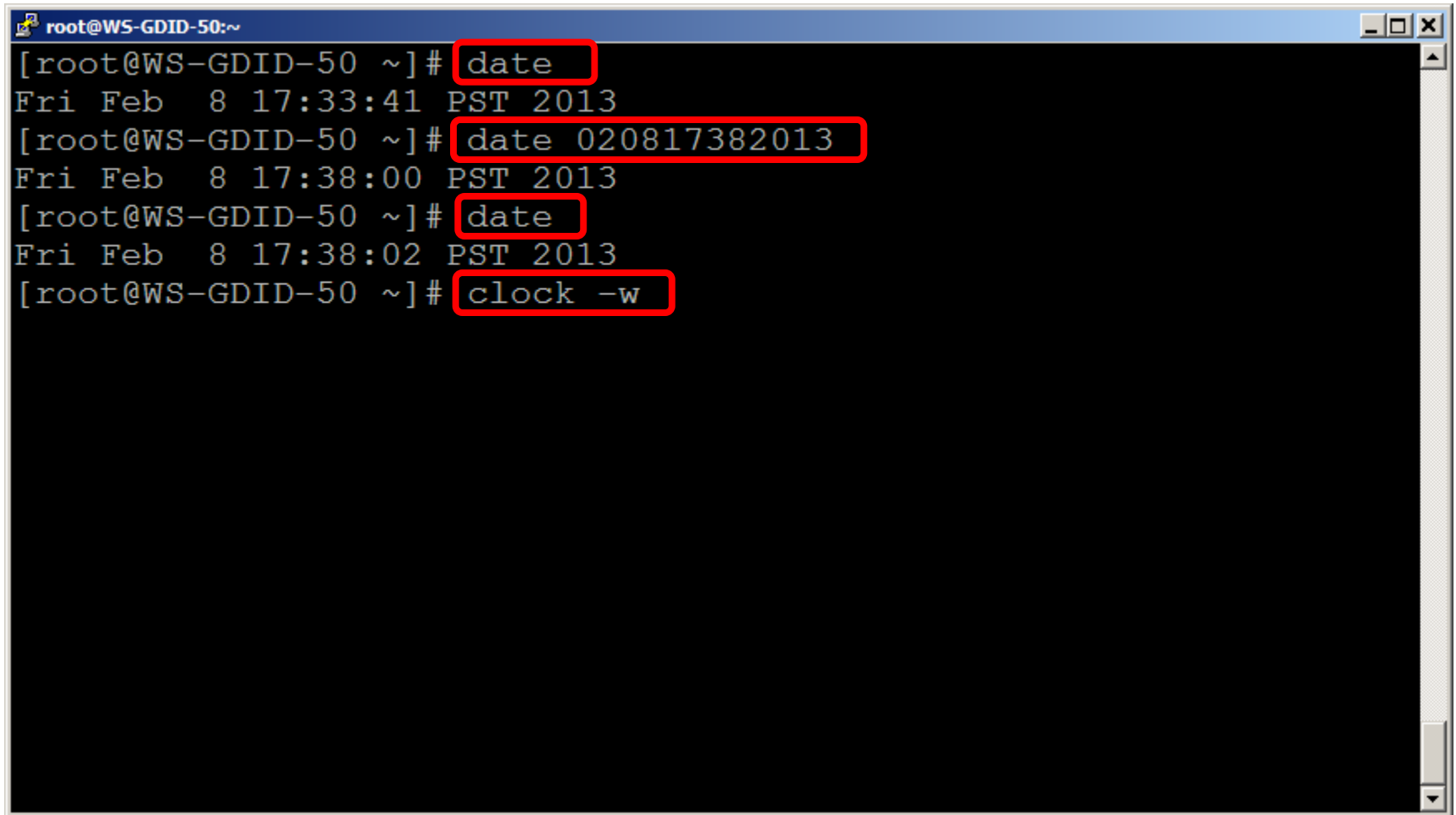
```
root@WS-GDID-50:~  
[root@WS-GDID-50 ~]# route -n  
Kernel IP routing table  
Destination      Gateway          Genmask          Flags Metric Ref  
  Use Iface  
224.0.1.37       0.0.0.0          255.255.255.255 UH      0      0  
    0 eth1  
10.212.0.0        0.0.0.0          255.255.0.0      U        0      0  
    0 eth0  
10.212.0.0        0.0.0.0          255.255.0.0      U        0      0  
    0 eth1  
169.254.0.0       0.0.0.0          255.255.0.0      U       1002    0  
    0 eth0  
169.254.0.0       0.0.0.0          255.255.0.0      U       1003    0  
    0 eth1  
0.0.0.0           10.212.254.254  0.0.0.0          UG       0      0  
    0 eth0  
[root@WS-GDID-50 ~]# _
```

- Test hostname resolution



```
root@WS-GDID-50:~  
[root@WS-GDID-50 ~]# ping WS-GDID-50  
PING WS-GDID-50.webinar.net (10.212.5.209) 56(84) bytes of data.  
64 bytes from WS-GDID-50.webinar.net (10.212.5.209): icmp_seq=1 t  
tl=64 time=0.020 ms  
^Z  
[2]+  Stopped                  ping WS-GDID-50  
[root@WS-GDID-50 ~]# ping WS-GDID-50.Webinar.net  
PING WS-GDID-50.webinar.net (10.212.5.209) 56(84) bytes of data.  
64 bytes from WS-GDID-50.webinar.net (10.212.5.209): icmp_seq=1 t  
tl=64 time=0.019 ms  
^Z  
[3]+  Stopped                  ping WS-GDID-50.Webinar.net  
[root@WS-GDID-50 ~]# ping 10.212.5.209  
PING 10.212.5.209 (10.212.5.209) 56(84) bytes of data.  
64 bytes from 10.212.5.209: icmp_seq=1 ttl=64 time=0.020 ms  
^Z  
[4]+  Stopped                  ping 10.212.5.209  
[root@WS-GDID-50 ~]# _
```

- Verify the date and time

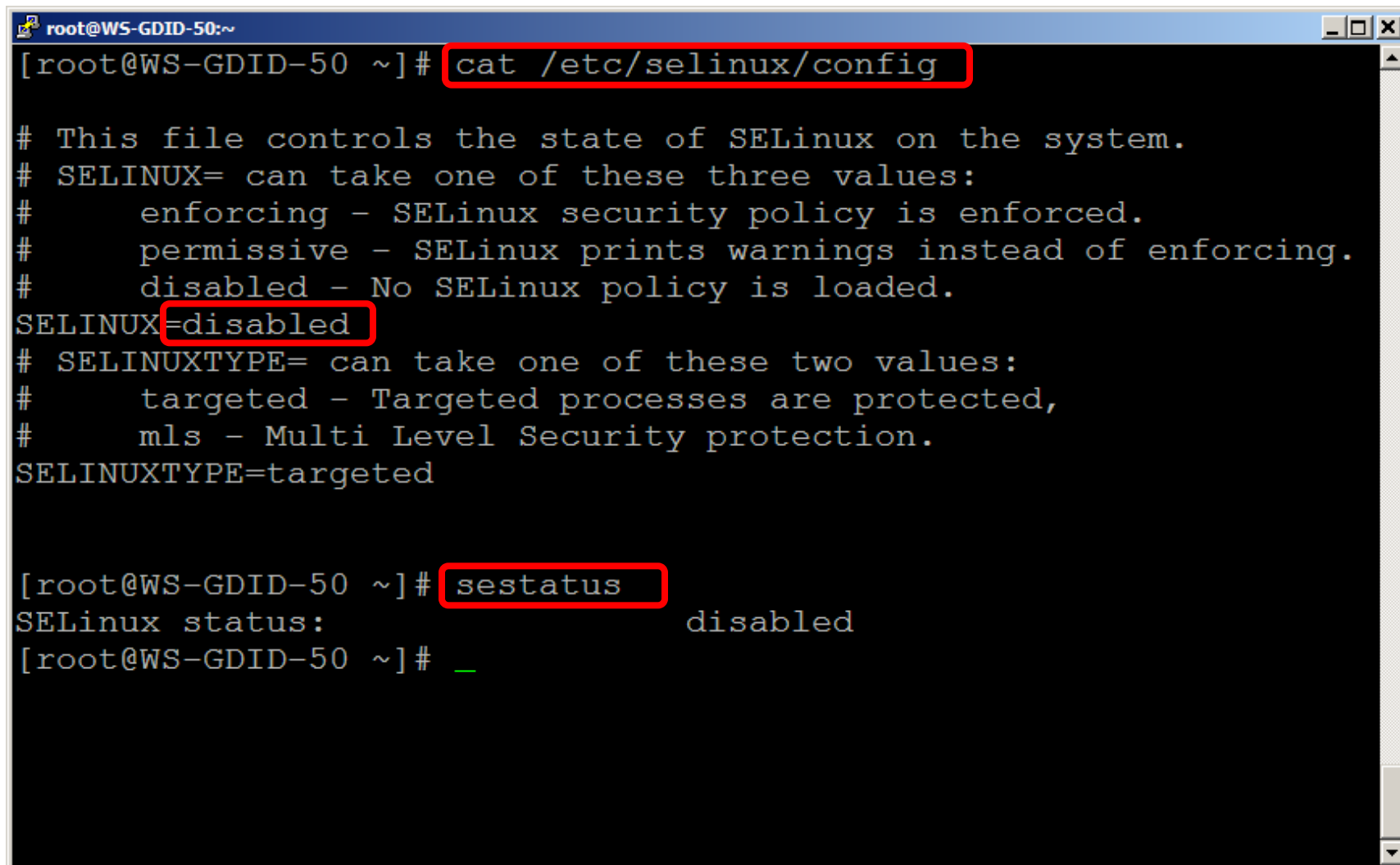
A terminal window titled 'root@WS-GDID-50:~' with a blue header bar. The window contains a series of commands and their outputs. The commands 'date', 'date 020817382013', and 'clock -w' are highlighted with red rectangular boxes. The output of the first 'date' command is 'Fri Feb 8 17:33:41 PST 2013'. The output of the second 'date' command is 'Fri Feb 8 17:38:00 PST 2013'. The output of the third 'date' command is 'Fri Feb 8 17:38:02 PST 2013'.

```
root@WS-GDID-50:~  
[root@WS-GDID-50 ~]# date  
Fri Feb 8 17:33:41 PST 2013  
[root@WS-GDID-50 ~]# date 020817382013  
Fri Feb 8 17:38:00 PST 2013  
[root@WS-GDID-50 ~]# date  
Fri Feb 8 17:38:02 PST 2013  
[root@WS-GDID-50 ~]# clock -w
```

- Verify the network interface configuration

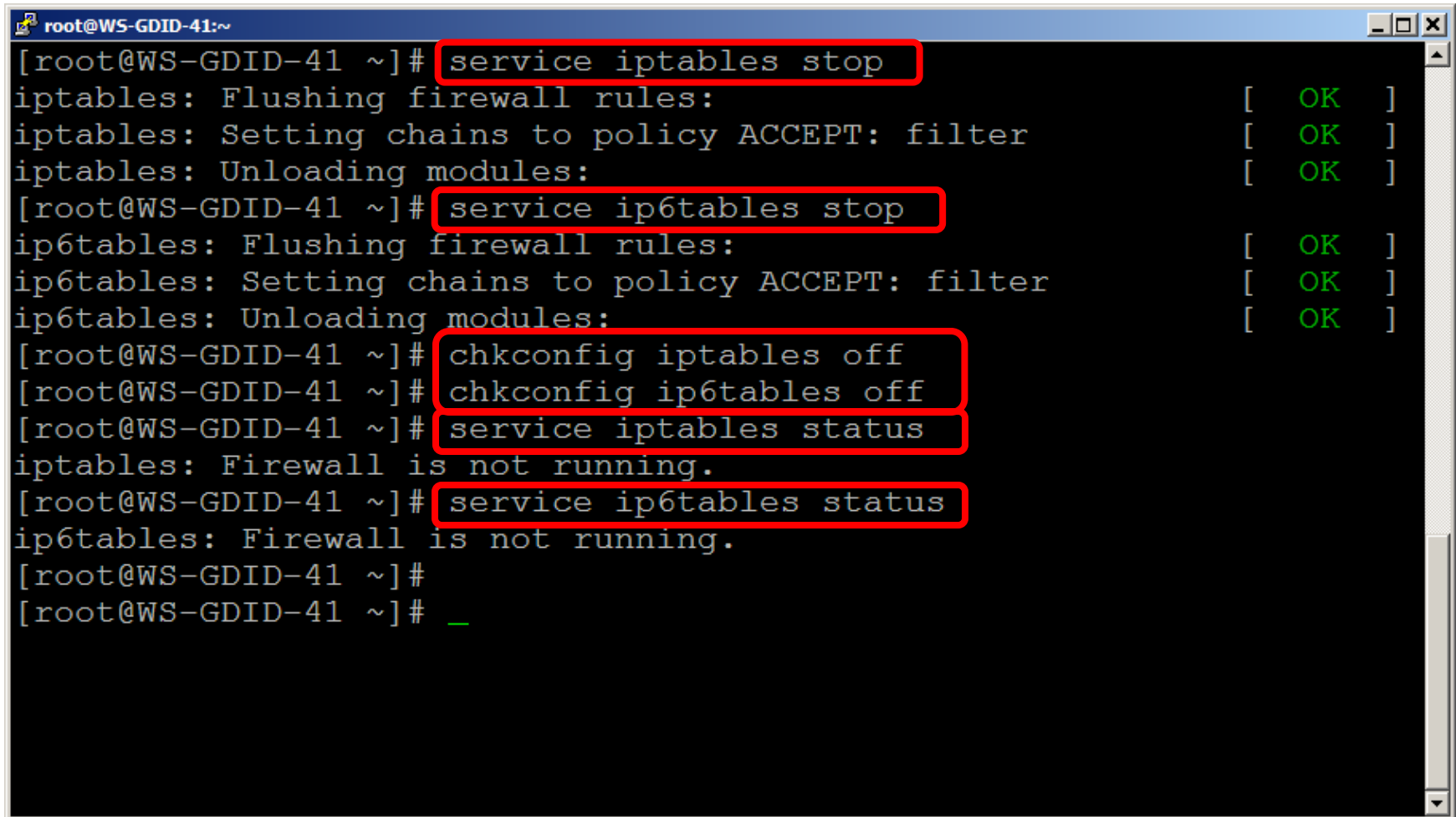
```
root@WS-GDID-50:~  
[root@WS-GDID-50 ~]# ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0C:29:F0:9D:7A  
          inet addr:10.212.5.209  Bcast:10.212.255.255  Mask:255.255.0.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:485293 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:14700 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:59042354 (56.3 MiB)  TX bytes:5089676 (4.8 MiB)  
  
eth0:1    Link encap:Ethernet  HWaddr 00:0C:29:F0:9D:7A  
          inet addr:10.212.11.166  Bcast:10.212.255.255  Mask:255.255.0.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
  
eth1      Link encap:Ethernet  HWaddr 00:0C:29:F0:9D:84  
          inet addr:10.212.5.212  Bcast:10.212.255.255  Mask:255.255.0.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:533915 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:34847 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:85686484 (81.7 MiB)  TX bytes:22659189 (21.6 MiB)  
  
lo        Link encap:Local Loopback
```

- Verify that SELinux is disabled

A terminal window titled 'root@WS-GDID-50:~' with standard window controls. The terminal shows the command 'cat /etc/selinux/config' being executed, followed by the contents of the file. The file contains comments about SELinux states and values. 'SELINUX=disabled' is highlighted with a red box. Then, the command 'sestatus' is executed, and the output 'SELinux status: disabled' is shown, with 'sestatus' also highlighted by a red box. The prompt returns to the root user.

```
root@WS-GDID-50:~  
[root@WS-GDID-50 ~]# cat /etc/selinux/config  
  
# This file controls the state of SELinux on the system.  
# SELINUX= can take one of these three values:  
#     enforcing - SELinux security policy is enforced.  
#     permissive - SELinux prints warnings instead of enforcing.  
#     disabled  - No SELinux policy is loaded.  
SELINUX=disabled  
# SELINUXTYPE= can take one of these two values:  
#     targeted - Targeted processes are protected,  
#     mls      - Multi Level Security protection.  
SELINUXTYPE=targeted  
  
[root@WS-GDID-50 ~]# sestatus  
SELinux status: disabled  
[root@WS-GDID-50 ~]# _
```

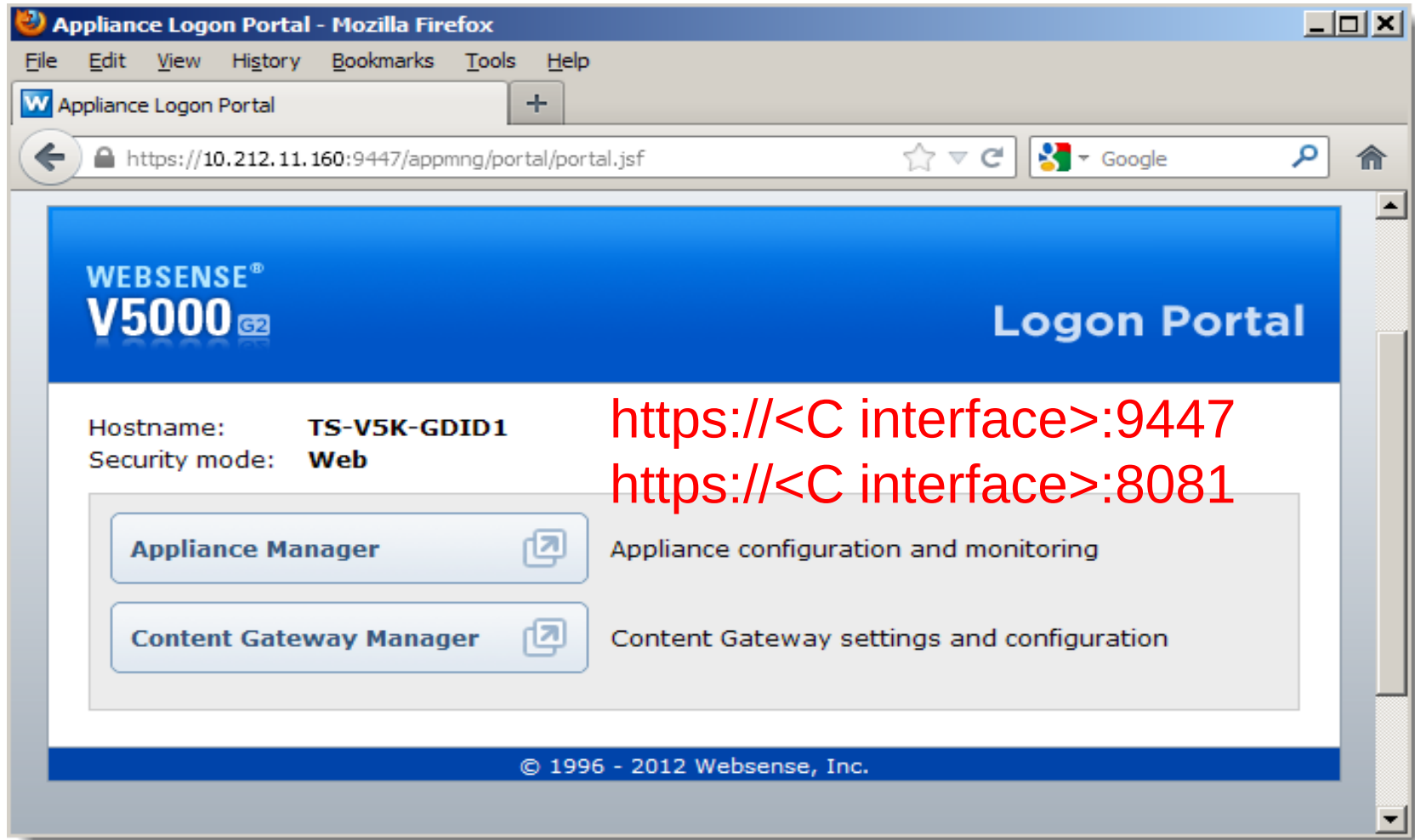
- Verify the IPTables are stopped



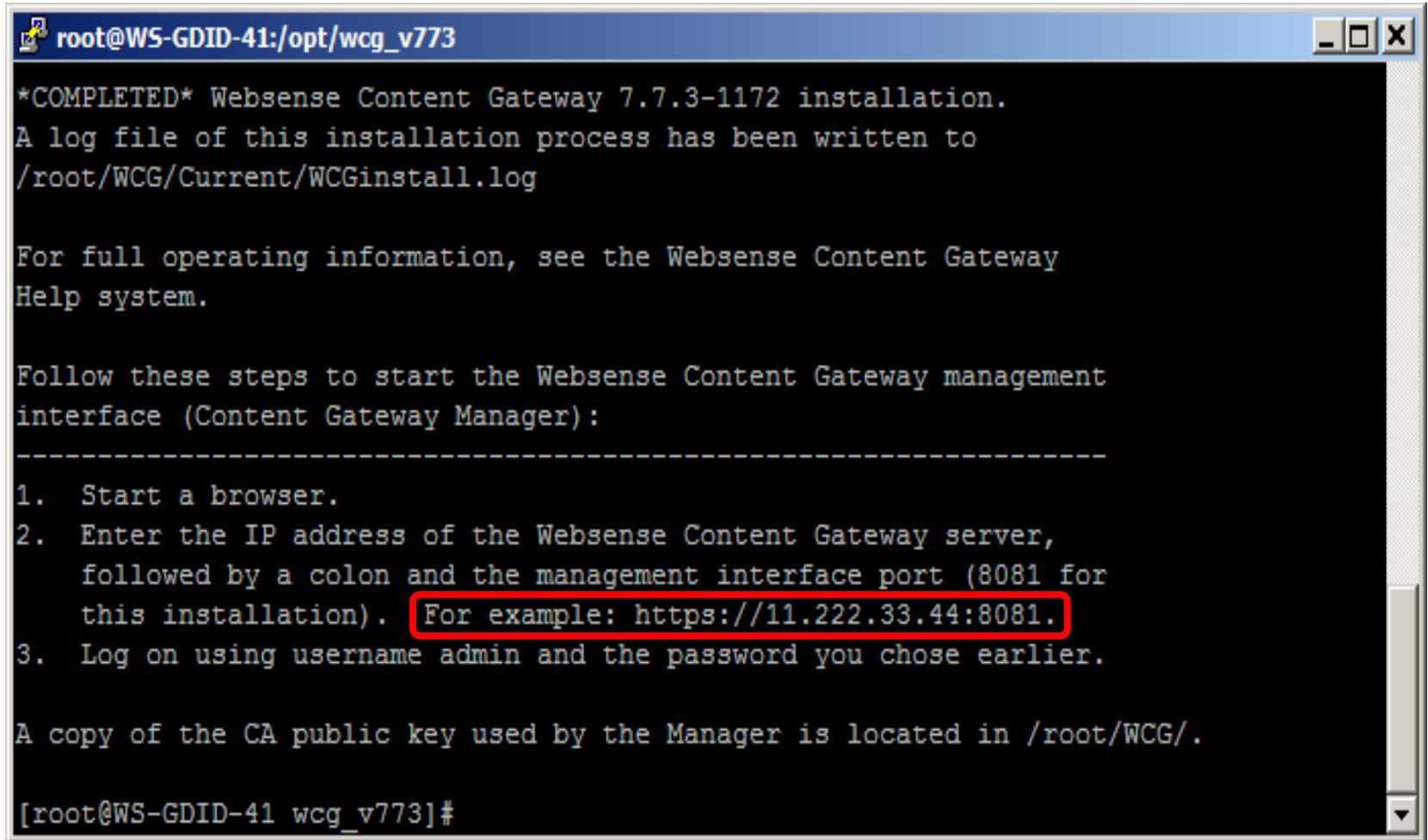
```
root@WS-GDID-41:~  
[root@WS-GDID-41 ~]# service iptables stop  
iptables: Flushing firewall rules: [ OK ]  
iptables: Setting chains to policy ACCEPT: filter [ OK ]  
iptables: Unloading modules: [ OK ]  
[root@WS-GDID-41 ~]# service ip6tables stop  
ip6tables: Flushing firewall rules: [ OK ]  
ip6tables: Setting chains to policy ACCEPT: filter [ OK ]  
ip6tables: Unloading modules: [ OK ]  
[root@WS-GDID-41 ~]# chkconfig iptables off  
[root@WS-GDID-41 ~]# chkconfig ip6tables off  
[root@WS-GDID-41 ~]# service iptables status  
iptables: Firewall is not running.  
[root@WS-GDID-41 ~]# service ip6tables status  
ip6tables: Firewall is not running.  
[root@WS-GDID-41 ~]#  
[root@WS-GDID-41 ~]# _
```

- For more suggestions for preparing your Red Hat server for installing Websense Content Gateway, see article:
 - [Prepare Red Hat server for Websense Content Gateway installation](#)
 - [Deployment and Installation Center](#)
 - [v7.7.3 Release Notes for Websense Content Gateway](#)

- Content Gateway Manager on the V-Series appliance



- Content Gateway Manager on Red Hat software



```
root@WS-GDID-41:/opt/wcg_v773

*COMPLETED* Websense Content Gateway 7.7.3-1172 installation.
A log file of this installation process has been written to
/root/WCG/Current/WCGinstall.log

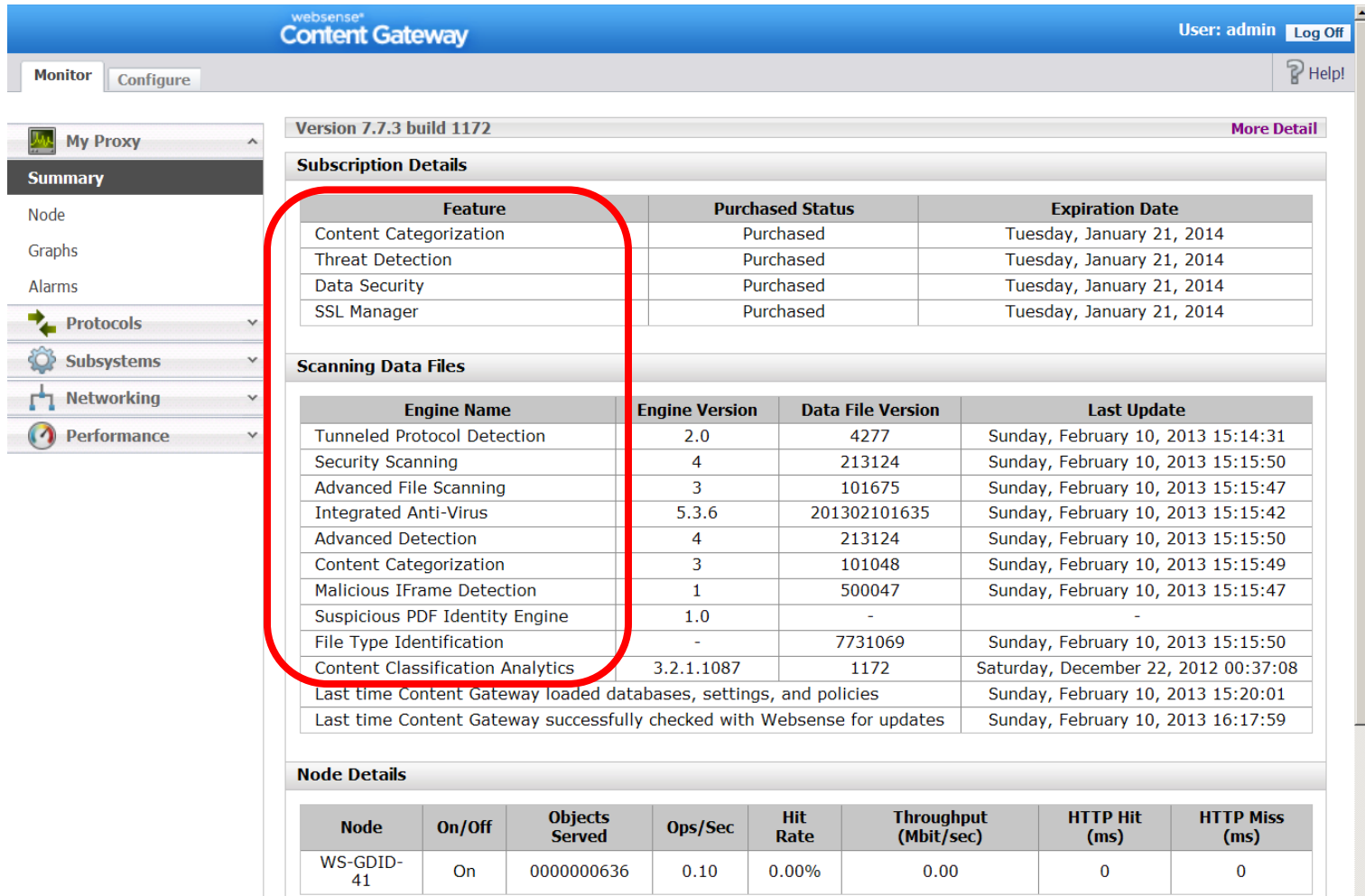
For full operating information, see the Websense Content Gateway
Help system.

Follow these steps to start the Websense Content Gateway management
interface (Content Gateway Manager):
-----
1. Start a browser.
2. Enter the IP address of the Websense Content Gateway server,
   followed by a colon and the management interface port (8081 for
   this installation). For example: https://11.222.33.44:8081.
3. Log on using username admin and the password you chose earlier.

A copy of the CA public key used by the Manager is located in /root/WCG/.

[root@WS-GDID-41 wcg_v773]#
```

- Ensure features are enabled and data files downloaded



The screenshot displays the Websense Content Gateway interface. The top navigation bar includes the 'Monitor' and 'Configure' tabs, the user 'admin', and a 'Log Off' button. The left sidebar contains a 'My Proxy' icon and a 'Summary' section with links to 'Node', 'Graphs', 'Alarms', 'Protocols', 'Subsystems', 'Networking', and 'Performance'. The main content area shows 'Version 7.7.3 build 1172' and a 'More Detail' link. The 'Subscription Details' section contains a table with the following data:

Feature	Purchased Status	Expiration Date
Content Categorization	Purchased	Tuesday, January 21, 2014
Threat Detection	Purchased	Tuesday, January 21, 2014
Data Security	Purchased	Tuesday, January 21, 2014
SSL Manager	Purchased	Tuesday, January 21, 2014

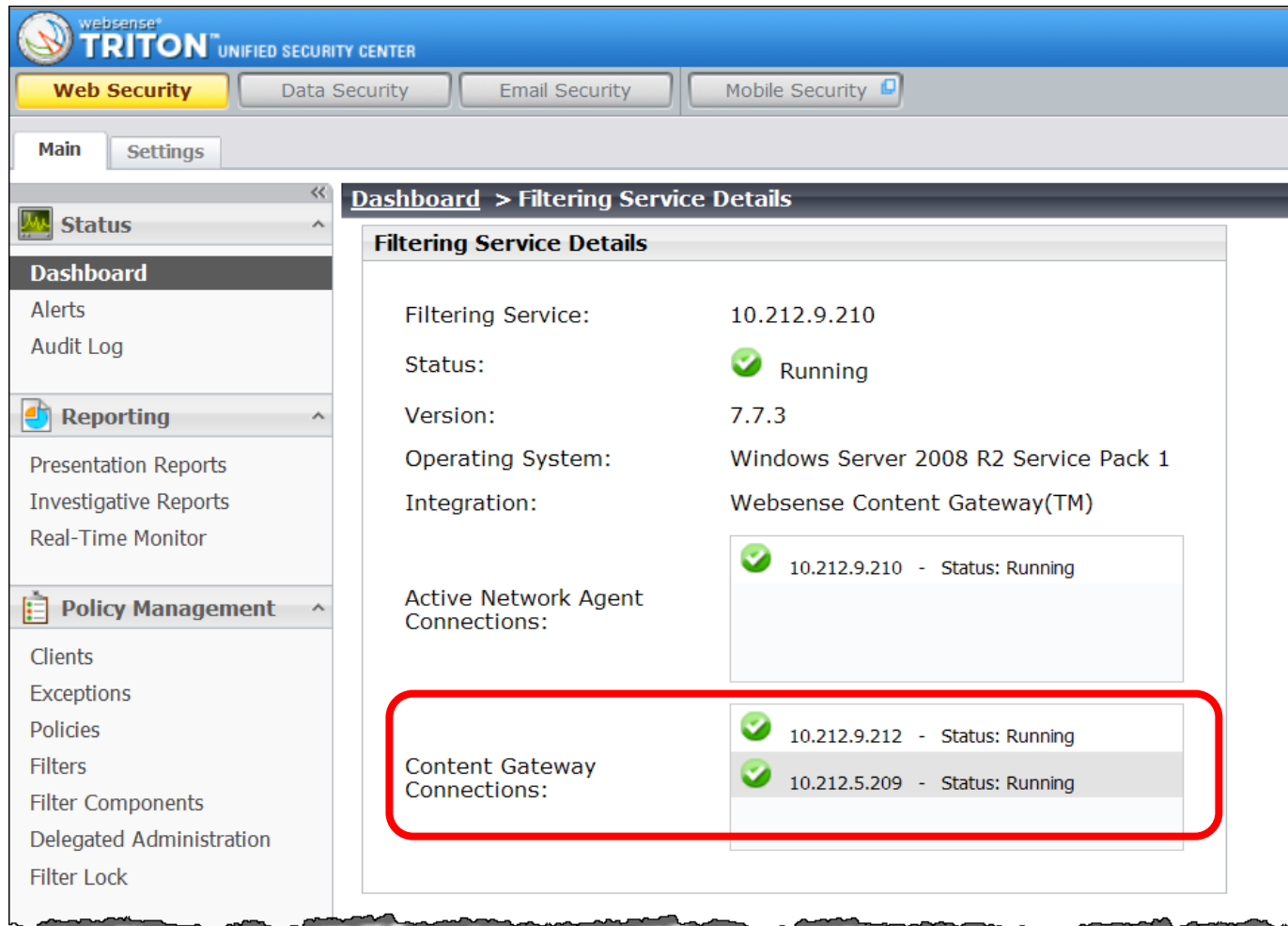
The 'Scanning Data Files' section contains a table with the following data:

Engine Name	Engine Version	Data File Version	Last Update
Tunneled Protocol Detection	2.0	4277	Sunday, February 10, 2013 15:14:31
Security Scanning	4	213124	Sunday, February 10, 2013 15:15:50
Advanced File Scanning	3	101675	Sunday, February 10, 2013 15:15:47
Integrated Anti-Virus	5.3.6	201302101635	Sunday, February 10, 2013 15:15:42
Advanced Detection	4	213124	Sunday, February 10, 2013 15:15:50
Content Categorization	3	101048	Sunday, February 10, 2013 15:15:49
Malicious IFrame Detection	1	500047	Sunday, February 10, 2013 15:15:47
Suspicious PDF Identity Engine	1.0	-	-
File Type Identification	-	7731069	Sunday, February 10, 2013 15:15:50
Content Classification Analytics	3.2.1.1087	1172	Saturday, December 22, 2012 00:37:08
Last time Content Gateway loaded databases, settings, and policies			Sunday, February 10, 2013 15:20:01
Last time Content Gateway successfully checked with Websense for updates			Sunday, February 10, 2013 16:17:59

The 'Node Details' section contains a table with the following data:

Node	On/Off	Objects Served	Ops/Sec	Hit Rate	Throughput (Mbit/sec)	HTTP Hit (ms)	HTTP Miss (ms)
WS-GDID-41	On	0000000636	0.10	0.00%	0.00	0	0

- Confirm the Content Gateway successfully registered



The screenshot shows the Websense TRITON Unified Security Center interface. The left sidebar contains navigation links for Main, Settings, Status, Dashboard, Alerts, Audit Log, Reporting, Policy Management, Clients, Exceptions, Policies, Filters, Filter Components, Delegated Administration, and Filter Lock. The main content area displays the 'Filtering Service Details' page, which includes the following information:

- Filtering Service: 10.212.9.210
- Status: Running
- Version: 7.7.3
- Operating System: Windows Server 2008 R2 Service Pack 1
- Integration: Websense Content Gateway(TM)

Below this information, there are two sections for active network agent connections:

- Active Network Agent Connections: 10.212.9.210 - Status: Running
- Content Gateway Connections: 10.212.9.212 - Status: Running and 10.212.5.209 - Status: Running

A red box highlights the 'Content Gateway Connections' section, indicating that the Content Gateway is successfully registered and running.

- After installation and analytic database downloads, Content Gateway is ready to protect your network. For simple testing, no further configuration is required.
- To test, redirect traffic to the web proxy.
 - Explicit proxy (manually point browser)
 - Check Content Gateway graphs for client activity
 - Confirm Filtering Service machine sends a block page
- Demonstration
- The web security block page is a good indicator of a successful installation and of network connectivity.
- Proceed with addition proxy configurations

- Clustering
- Virtual IP
- WCCP
- DNS Proxy
- SSL content inspection
- Authentication

The screenshot shows the Websense Content Gateway configuration interface. The top bar indicates the user is 'admin' and provides a 'Log Off' link. The main navigation pane on the left lists various configuration categories: My Proxy, Basic, Subscription, UI Setup, Snapshots, Logs, Protocols, Content Routing, Security, Subsystems, Networking, and SSL. The 'Configure' tab is active, and the 'Clustering' sub-tab is selected. The 'Features' section contains a table with columns for 'Feature', 'On', and 'Off'. The table lists various features and their status, with radio buttons for selection.

Feature	On	Off
Protocols		
FTP	☐	☒
HTTPS	☐	☒
Networking		
WCCP	☐	☒
DNS Proxy	☐	☒
Virtual IP	☐	☒
IPv6 (Explicit proxy only; requires IPv6 enabled in Appliance Manager or operating system)	☐	☒
Data Security	☐	☒
☐ Integrated on-box		
☐ ICAP		
Security		
SOCKS	☐	☒
Authentication		
None	☒	
Integrated Windows Authentication	☐	
LDAP	☐	
Radius	☐	
Legacy NTLM	☐	
Multiple Realm Authentication	☐	
	On	Off
Read authentication from child proxy	☐	☒
Send authentication to parent proxy	☐	☒

- The Content Gateway is a powerful web proxy. It is best practice to become familiar with Content Gateway features and configurations before placing in a production network.
- When testing new features, it is best practice to deploy Content Gateway in a test environment.
- TIP: For easy testing, you can integrate Content Gateway, residing on a Red Hat server, into your existing Websense Web Security environment.
 - Ensure all Websense components are the same version
 - For testing traffic, redirect a small subset of users
- When confirmed, redirect production traffic

- [System requirements](#)
- [Requirements for Red Hat Enterprise Linux](#)
- [Preparing to install Websense Content Gateway](#)
- [Prepare Red Hat server for Websense Content Gateway installation](#)
- [Deployment options](#)
- [Content Gateway Ports](#)
- [How do I configure IPTables to harden the Content Gateway host system?](#)
- [Installing Websense Content Gateway](#)
- Prior WCCP Webinars: [Oct 2011](#) and [Dec 2011](#)

- [Content Verification Engine Best Practices](#)
- [SSL Manager Certificate Verification Engine v7.7](#)
- [Configuring DNS proxy caching](#)
- [Content Gateway explicit and transparent proxy deployments](#)
- [Content Gateway initial configuration](#)

Webinar Update

Title:

Quick Start 4: Identifying and Troubleshooting proxy issues for Websense Web Security Gateway

Date:

March 20th, 2013

Time:

8:30 A.M. PDT (GMT -8)

How to register:

<http://www.websense.com/content/SupportWebinars.aspx>

- To find Websense classes offered by Authorized Training Partners in your area, visit:

<http://www.websense.com/findaclass>

- Websense Training Partners offer classes online and onsite at your location.

- For more information, please send email to:

readiness@websense.com

WebSense Customer Training

Designed for:

- ▶ System administrators
- ▶ Network engineers
- ▶ Other members of your organization as appropriate

Training locations:

All training is conducted at Authorized Training Centers (ATCs). Each ATC has information on costs, course schedules, and types of classes (in-person, virtual, or computer-based).