

Installing and Configuring Websense Content Gateway

Websense Support Webinar - September 2009

Support Webinars

- **Title: Installing and Configuring Websense Content Gateway**

- Audio information:
 - **This presentation incorporates STREAMING AUDIO.**
 - Use of speakers or headsets is required. *If unable to hear streaming audio or it is choppy, a limited number of dial-in numbers are available.*

- Dial-in numbers:
 - **U.S. dial-in numbers:**
 - Toll free: **1-888-373-5705**, pass-code: **977210**
 - Toll: **1-719-457-3840**, pass-code: **977210**
 - **Find international dial-in numbers at:**
 - <http://www.websense.com/SeptemberIntlNumbers>
 - Pass-code: **977210**



Greg Didier

- **Title:** Tech Support Specialist
- **Accomplishments:**
 - Over 5 years supporting Websense products
- **Certifications:**
 - Security & Network design
 - MCP
 - WCWSA – Websense Certified Web Security Associate
- **Qualifications:**
 - Trainer
- **For additional information:**
www.websense.com/support/

Goals and Objectives

- Preinstall considerations
- Check Linux server
- Install Websense Content Gateway (WCG)
- Enable HTTPS
- Create and deploy certificates
- Test filtering

Pre-install Requirement

- Websense Web Security Gateway must be installed before you install Websense Content Gateway.
- The integration mode must be Websense Content Gateway.

Hardware Requirements

- CPU – quad-core, 2.8 GHz or faster
- Memory – 4 GB RAM
- Disk Space – two disks
 - 100 GB disk for Red Hat Linux, Websense Content Gateway, temporary data
 - 147 GB disk (max size) for caching
 - Must be a raw disk
 - Must be dedicated
 - Must not be part of a RAID
- Network Interfaces
 - One NIC for non-clustered setup
 - Two NICs for a clustered configuration

■ Linux only

- Red Hat Enterprise, Advanced Server, release 4, update 5, kernel 2.6.9-55
- May use the “Minimal” Linux install option
 - RPM “compat-libstdc++-33-3.2.3-47.3.i386.rpm” is required
- 32-bit

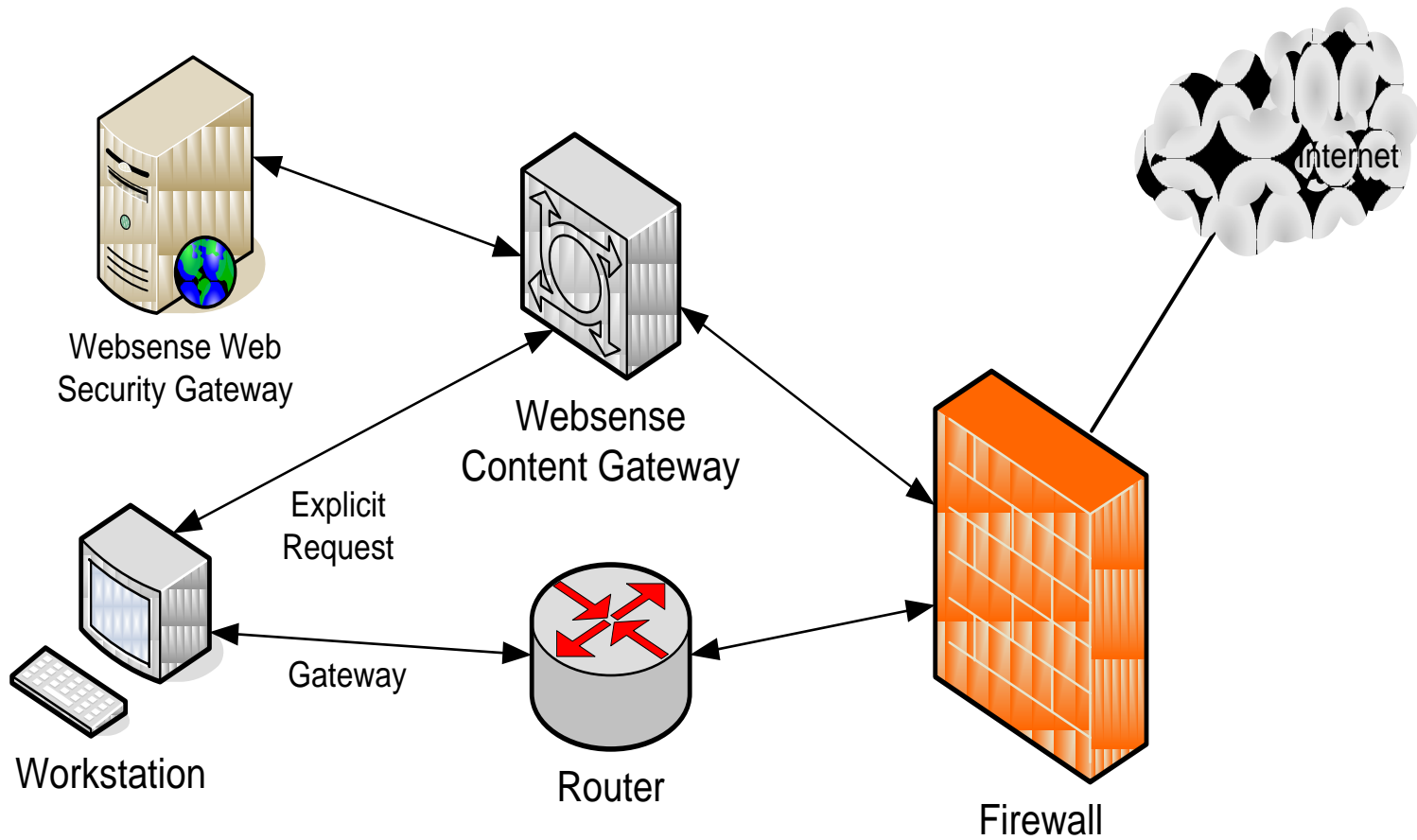
■ Websense Filtering integration

- Websense Web Security Gateway v7.1
- Websense Web Security v7.1
- Websense Web Filter v7.1

■ Supported browsers

- Internet Explorer 7 or 8
- Mozilla Firefox 2 or 3

Websense Content Gateway In Your Network



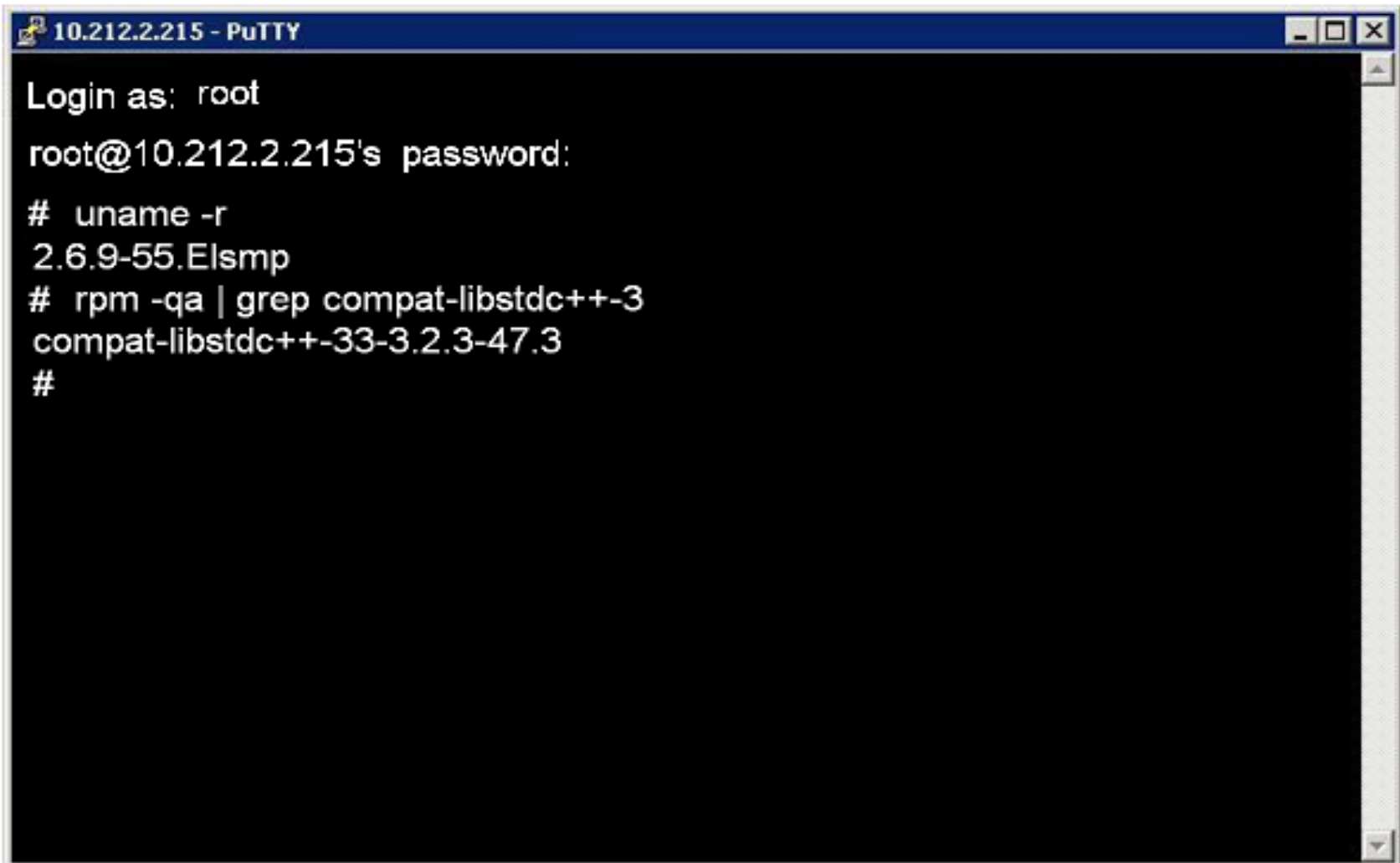
■ Ports used for Websense Content Gateway

- **21** TCP (Transparent FTP proxy)
- **22** TCP (SSH)
- **53** and **5353** UDP (DNS requests)
- **80** TCP (Transparent HTTP proxy)
- **443** TCP (Transparent HTTPS proxy)
- **2048** UDP (WCCP)
- **2121** TCP (Explicit FTP proxy)
- **8070** TCP (Explicit HTTPS proxy)
- **8071** and **8081** TCP (Proxy management interface)
- **8080** TCP (Explicit HTTP proxy)
- **8082 – 8090, 3031** TCP (Required only if clustering proxies)
- **40000, 55806, 55880, 55905** TCP (Local Websense Policy Server)
- **55807, 15868** TCP (Local Websense Filtering Service)
- **65535** TCP (Remote Websense Policy Server or Filtering Service)

- Pre-install check list for Websense Content Gateway
 - Linux version
 - IP configuration
 - Hostname
 - IP / hostname resolution
 - Routing table
 - DNS
 - IPv6 is disabled
 - Date and time
 - SELinux is disabled
 - Iptables
- Demonstration

- Linux IPTables (the firewall)
 - See KB 4106: *Configuring IPTables for Websense Content Gateway*
- Install files
 - www.mywebsense.com
 - Knowledge Base article # 4191
 - Title: *v7: Accessing Websense Content Gateway downloads*
- Move files to Linux server
 - WinSCP – secure file transfer utility
- Install Websense Content Gateway
 - Using putty
- Demonstration

Review Linux Configuration



```
10.212.2.215 - PuTTY
Login as: root
root@10.212.2.215's password:
# uname -r
2.6.9-55.Elsmpt
# rpm -qa | grep compat-libstdc++-3
compat-libstdc++-33-3.2.3-47.3
#
```

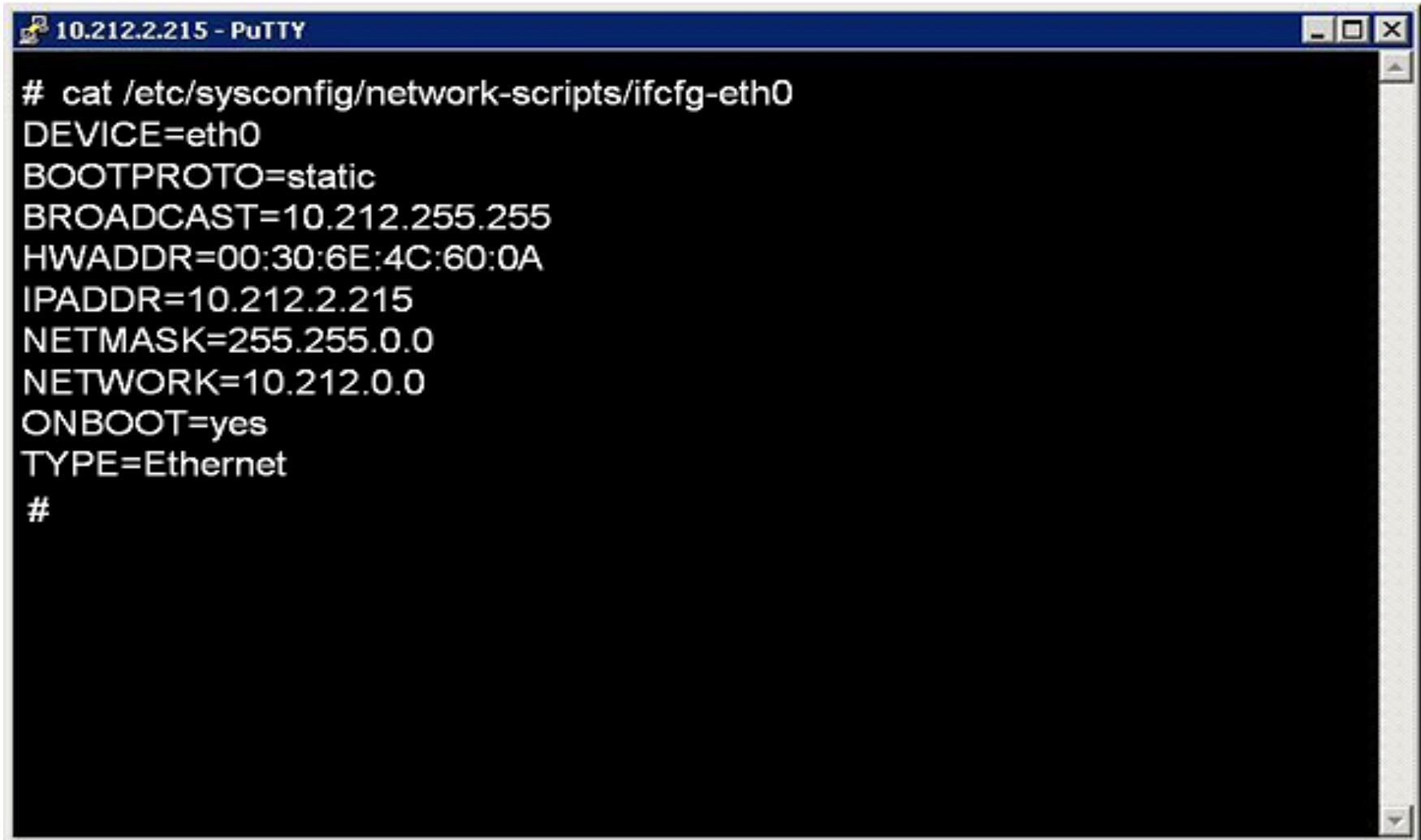
IP Configuration

```
10.212.2.215 - PuTTY
# ifconfig
eth0  Link encap:Ethernet  HWaddr 00:30:6E:4C:60:0A
      inet addr:10.212.2.215  Bcast:10.212.255.255  Mask:255.255.0.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:2042885 errors:0 dropped:0 overruns:0 frame:0
      TX packets:238896 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:757726686 (722.6 MiB)  TX bytes:24951794 (23.7 MiB)
      Base address:0x2080  Memory:da100000-da120000

lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:574108 errors:0 dropped:0 overruns:0 frame:0
      TX packets:574108 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:889856434 (848.6 MiB)  TX bytes:889856434 (848.6 MiB)

#
```

IP Configuration

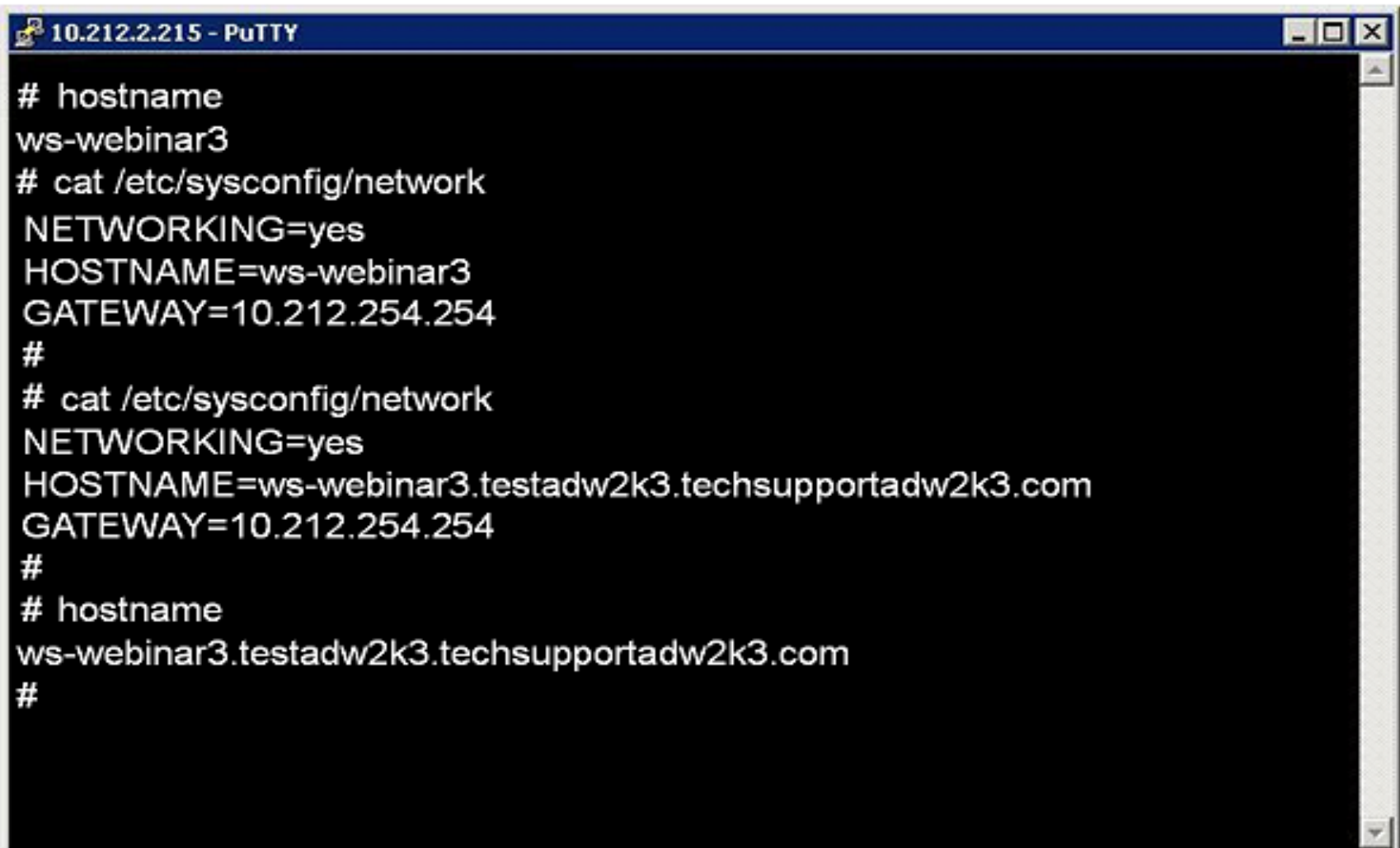


```
10.212.2.215 - PuTTY
# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
BROADCAST=10.212.255.255
HWADDR=00:30:6E:4C:60:0A
IPADDR=10.212.2.215
NETMASK=255.255.0.0
NETWORK=10.212.0.0
ONBOOT=yes
TYPE=Ethernet
#
```

IP Configuration

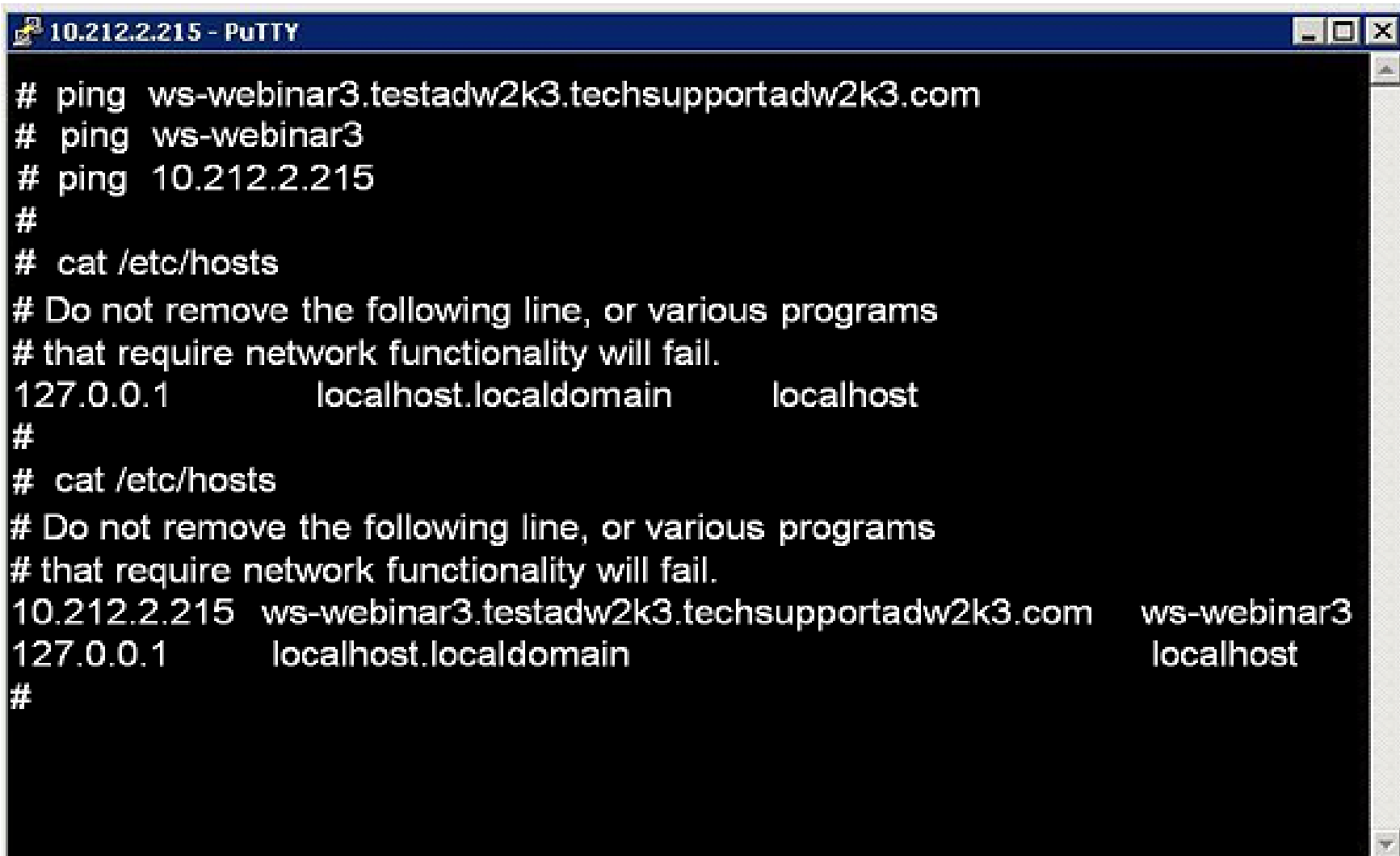
```
10.212.2.215 - PuTTY
# service network restart
Shutting down interface eth0:          [ OK ]
Shutting down loopback interface:      [ OK ]
Disabling IPv4 packet forwarding:      [ OK ]
Setting network parameters:            [ OK ]
Bringing up loopback interface:        [ OK ]
Bringing up interface eth0:            [ OK ]
#
# service network status
Configured devices:
lo eth0 eth1
Currently active devices:
lo eth0
#
```

Hostname



```
10.212.2.215 - PuTTY
# hostname
ws-webinar3
# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=ws-webinar3
GATEWAY=10.212.254.254
#
# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=ws-webinar3.testadw2k3.techsupportadw2k3.com
GATEWAY=10.212.254.254
#
# hostname
ws-webinar3.testadw2k3.techsupportadw2k3.com
#
```


IP / Hostname Mapping



```
10.212.2.215 - PuTTY
# ping ws-webinar3.testadw2k3.techsupportadw2k3.com
# ping ws-webinar3
# ping 10.212.2.215
#
# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1      localhost.localdomain    localhost
#
# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
10.212.2.215  ws-webinar3.testadw2k3.techsupportadw2k3.com  ws-webinar3
127.0.0.1     localhost.localdomain    localhost
#
```

```
10.212.2.215 - PuTTY
# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.212.0.0 0.0.0.0 255.255.0.0 U 0 0 0 eth0
169.254.0.0 0.0.0.0 255.255.0.0 U 0 0 0 eth0
0.0.0.0 10.212.254.254 0.0.0.0 UG 0 0 0 eth0
#
```

Checking DNS

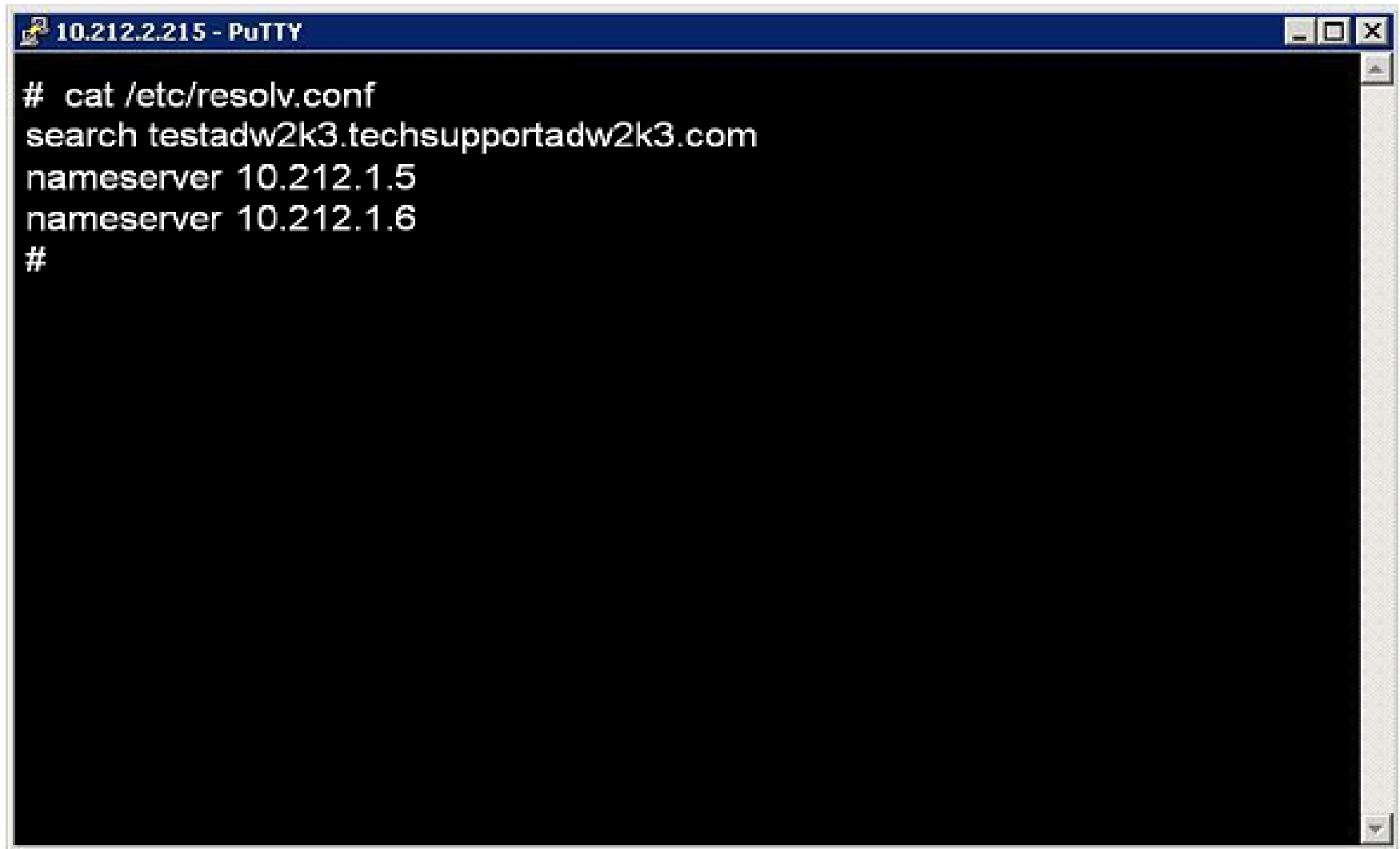
```
10.212.2.215 - PuTTY
# wget download.websense.com --delete
--15:29:57-- http://download.websense.com/
      => `index.html.1'
Resolving download.websense.com... 204.15.66.80
Connecting to download.websense.com|204.15.66.80|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 842 [text/html]

100%[=====>] 842      --.--K/s

15:29:57 (38.24 MB/s) - `index.html.1' saved [842/842]

Removing index.html.1.
#
```

Checking DNS



```
10.212.2.215 - PuTTY
# cat /etc/resolv.conf
search testadw2k3.techsupportadw2k3.com
nameserver 10.212.1.5
nameserver 10.212.1.6
#
```

- Install Manager certificate
- Enter subscription key
 - Websense Content Gateway and Websense Web Security Gateway use the same key
- Websense Content Gateway services
 - Status check
- Verify Websense Web Security Gateway is integrated with Websense Content Gateway
 - Filtering service install type

- Demonstration

- Failed install, review:
 - OS and kernel version
 - Proper libraries (RPMs) installed
 - Hostname and host file
 - Ethernet settings
 - DNS configuration
 - IPv6 disabled
 - Iptables correctly configured
 - SELinux disabled
 - Date and time match on Websense Content Gateway and Websense Web Security Gateway
 - Internet connectivity
- Once the problem is identified and corrected
 - Reinstall Websense Content Gateway

Initial Configuration of Websense Web Security Gateway

- Downloading the Master Database via the proxy
- Scanning options
- Identify the Log Server location
- Configure Network Agent

- Demonstration

- Enable HTTPS
- Create a *self-signed* certificate
- Backup the *self-signed* certificate
- Restart Websense Content Gateway
- Test SSL
- Import the certificate into the *Trusted Root CA Store*

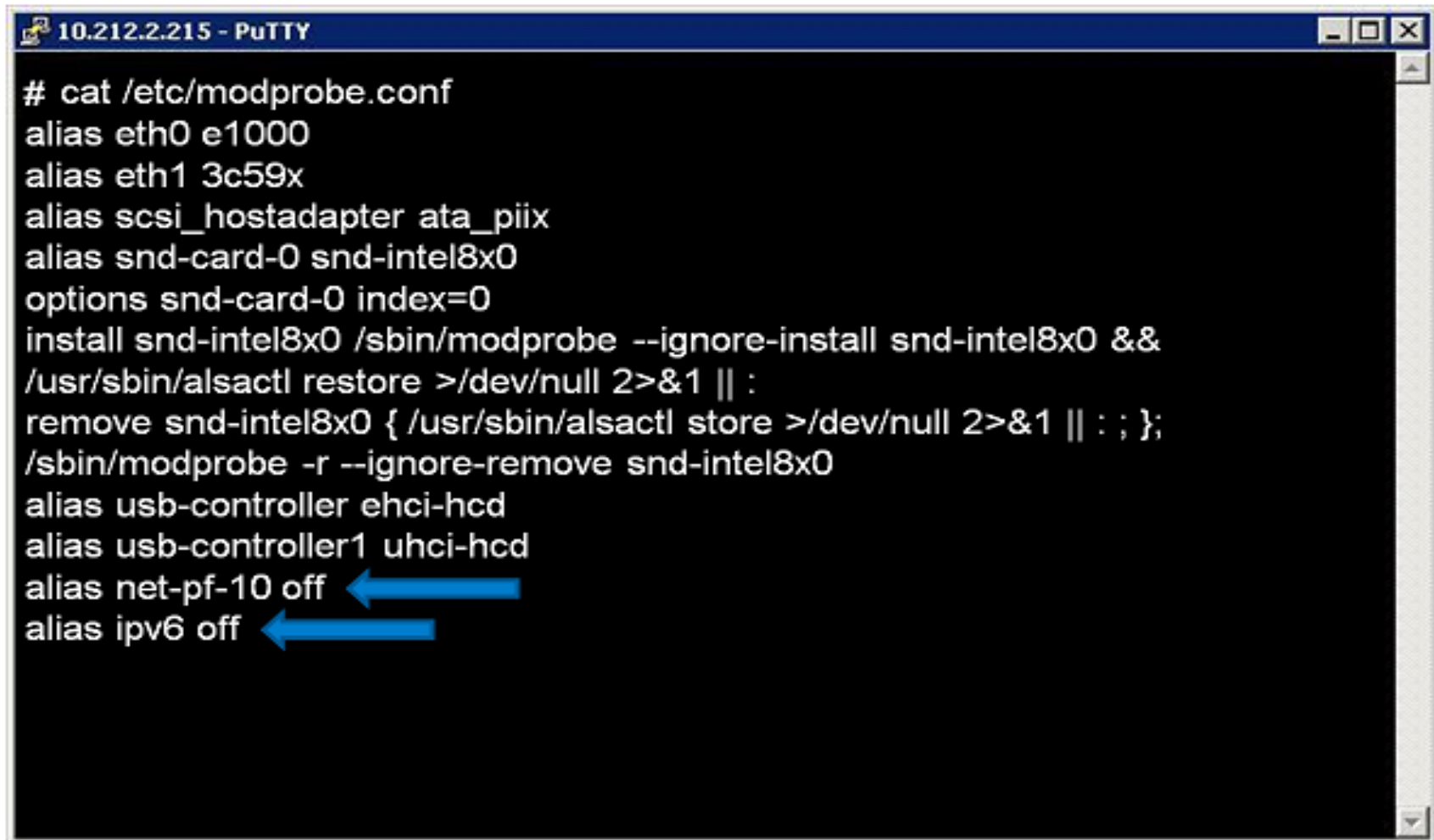
- Demonstration

Allowing HTTPS Web sites

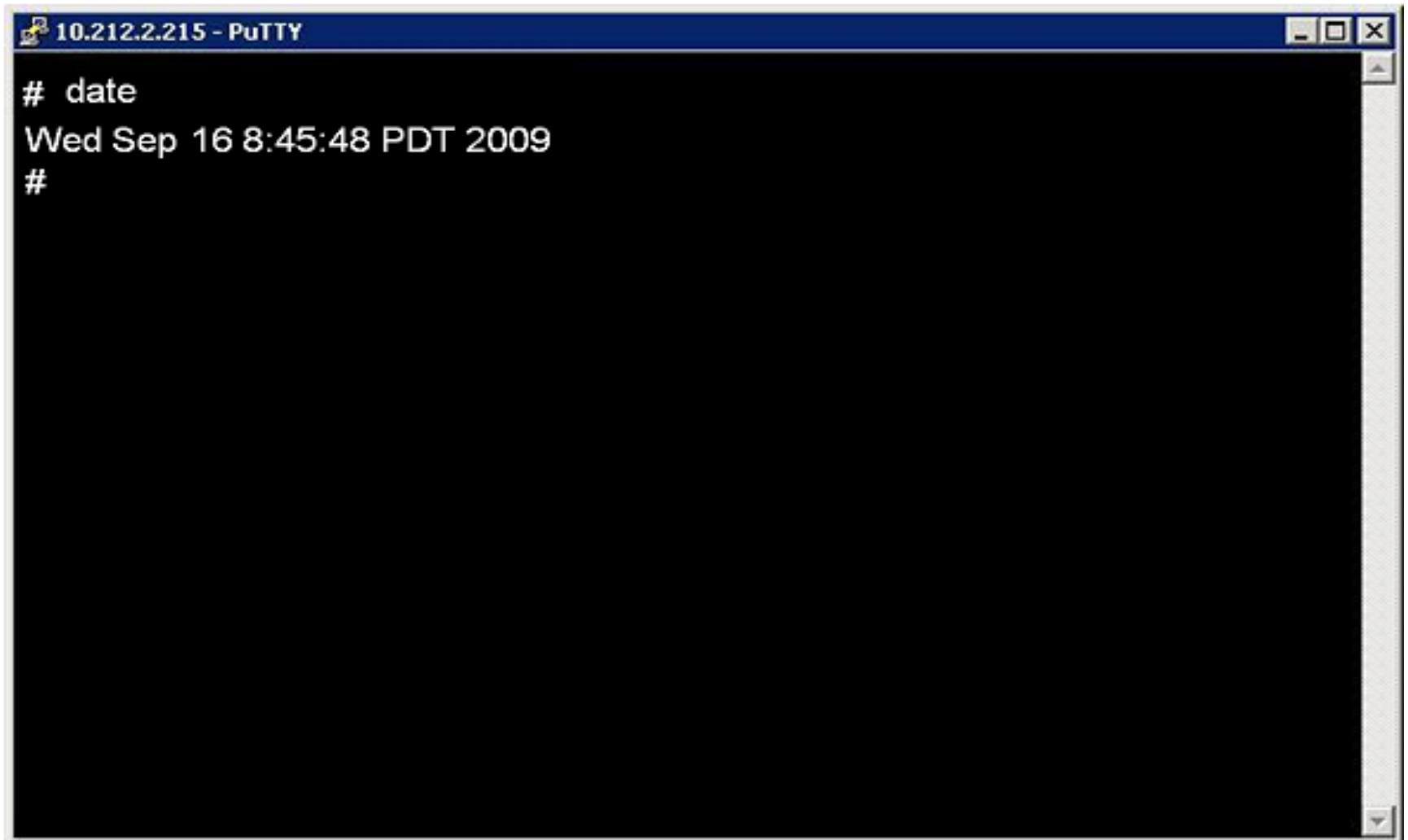
- Certificate validation
 - Working with incidents
 - Tunneling a Web site
-
- Demonstration

- Disabling IPv6
 - /etc/modprobe.conf
 - Remove one entry
 - net-pf-10 ipv6
 - Add two entries
 - alias net-pf-10 off
 - alias ipv6 off
 - Disabling IPv6

Disabling IPv6



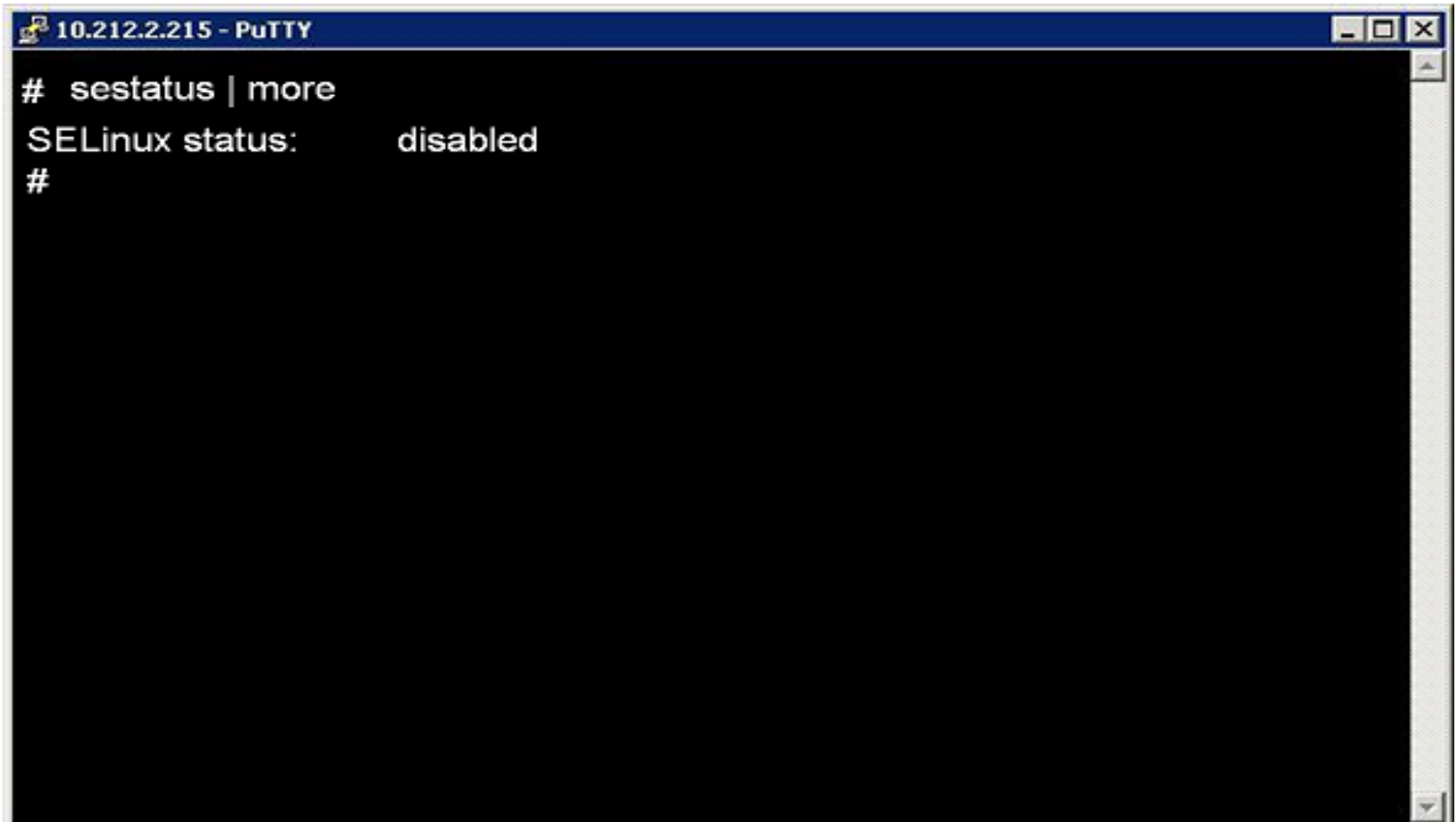
```
10.212.2.215 - PuTTY
# cat /etc/modprobe.conf
alias eth0 e1000
alias eth1 3c59x
alias scsi_hostadapter ata_piix
alias snd-card-0 snd-intel8x0
options snd-card-0 index=0
install snd-intel8x0 /sbin/modprobe --ignore-install snd-intel8x0 &&
/usr/sbin/alsactl restore >/dev/null 2>&1 || :
remove snd-intel8x0 { /usr/sbin/alsactl store >/dev/null 2>&1 || ;; };
/sbin/modprobe -r --ignore-remove snd-intel8x0
alias usb-controller ehci-hcd
alias usb-controller1 uhci-hcd
alias net-pf-10 off
alias ipv6 off
```



A screenshot of a PuTTY terminal window. The title bar reads "10.212.2.215 - PuTTY". The terminal content shows a prompt "#", the command "date", and the output "Wed Sep 16 8:45:48 PDT 2009". The prompt "#" is visible again on the next line.

```
# date  
Wed Sep 16 8:45:48 PDT 2009  
#
```

Disabling SELinux

A terminal window titled "10.212.2.215 - PuTTY" with standard window controls. The terminal text shows a command being executed and its output.

```
# sestatus | more
SELinux status:      disabled
#
```

Disabling SELinux

```
10.212.2.215 - PuTTY
# sestatus | more
SELinux status:      enabled ←
SELinuxfs mount:    /selinux
Current mode:       enforcing
Mode from config file: enforcing
Policy version:     18
Policy from config file:targeted

Policy booleans:
allow_syslog_to_console inactive
allow_yplibind      inactive
dhcpd_disable_trans inactive
httpd_builtin_scripting active
httpd_disable_trans inactive
httpd_enable_cgi    active
httpd_enable_homedirs active
httpd_ssi_exec      active
--More--
```

Disabling SELinux

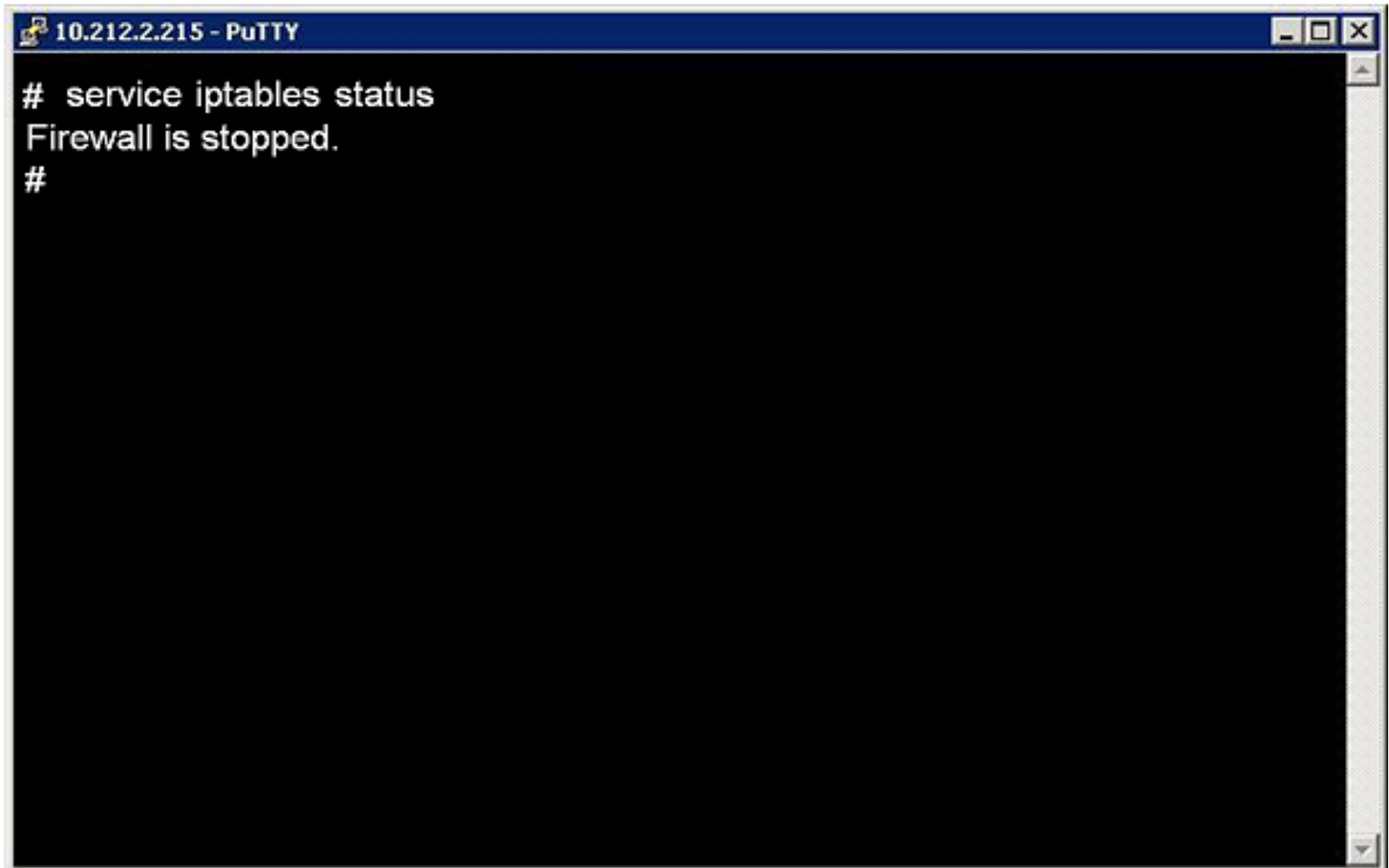
10.212.2.215 - PuTTY

```
# 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 - SELinux is fully disabled.
SELINUX=enforcing ←
# SELINUXTYPE= type of policy in use. Possible values are:
#   targeted - Only targeted network daemons are protected.
#   strict - Full SELinux protection.
SELINUXTYPE=targeted ←
#
```

Disabling SELinux

```
10.212.2.215 - PuTTY
# 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 - SELinux is fully disabled.
SELINUX=disabled ←
# SELINUXTYPE= type of policy in use. Possible values are:
#   targeted - Only targeted network daemons are protected.
#   strict - Full SELinux protection.
SELINUXTYPE=targeted
#
```


IPTables – The Linux Firewall



```
10.212.2.215 - PuTTY
# service iptables status
Firewall is stopped.
#
```

IPTables – The Linux Firewall

```
10.212.2.215 - PuTTY
# service iptables status | more
Table: filter
Chain INPUT (policy ACCEPT)
target    prot opt source          destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0        0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target    prot opt source          destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0        0.0.0.0/0

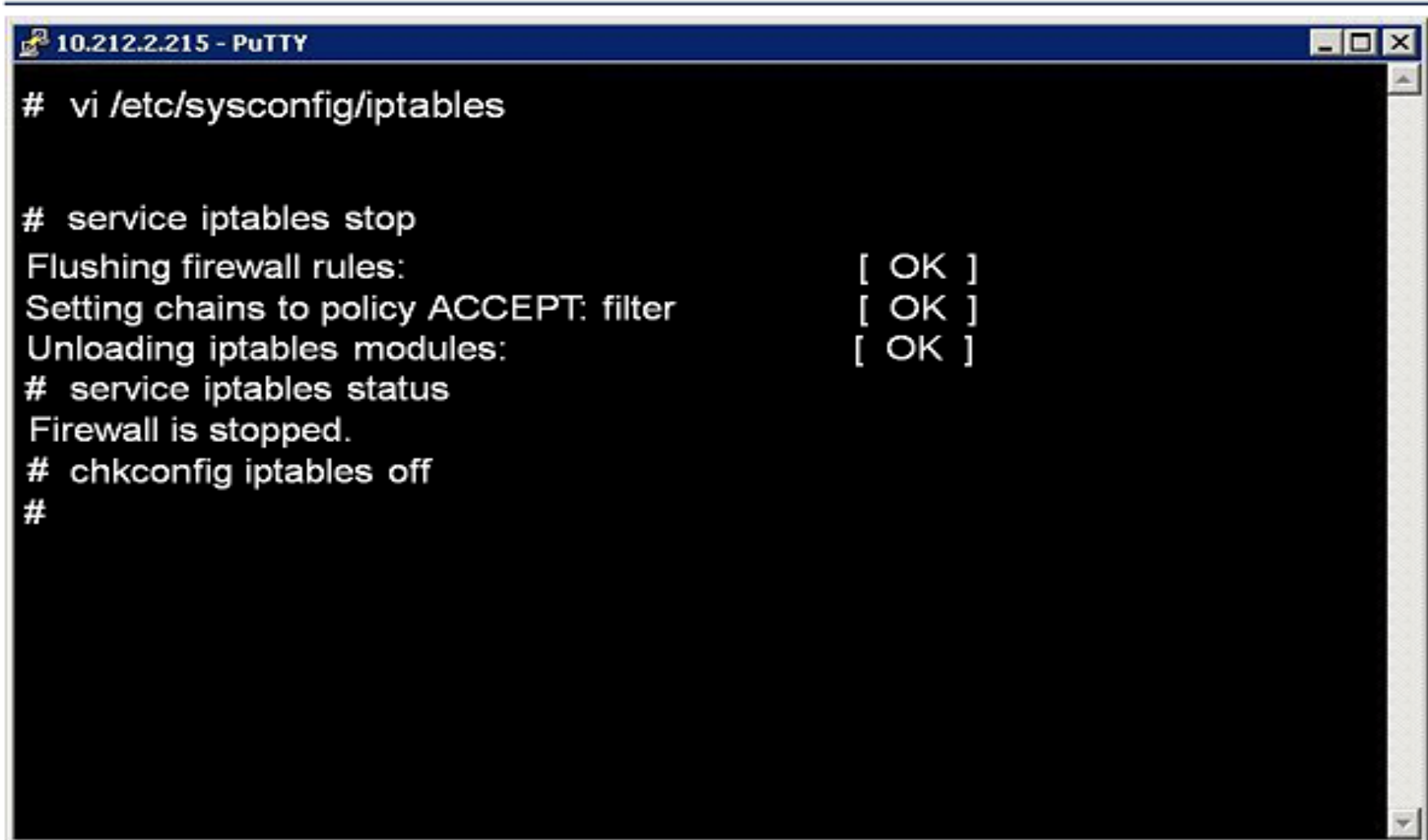
Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination

Chain RH-Firewall-1-INPUT (2 references)
target    prot opt source          destination
ACCEPT    all  --  0.0.0.0/0        0.0.0.0/0
ACCEPT    icmp --  0.0.0.0/0        0.0.0.0/0        icmp type 255
ACCEPT    esp  --  0.0.0.0/0        0.0.0.0/0
--More--
```

IPTables – The Linux Firewall

```
10.212.2.215 - PuTTY
ACCEPT  esp  --  0.0.0.0/0      0.0.0.0/0
ACCEPT  ah   --  0.0.0.0/0      0.0.0.0/0
ACCEPT  udp  --  0.0.0.0/0      224.0.0.251    udp dpt:5353
ACCEPT  udp  --  0.0.0.0/0      0.0.0.0/0      udp dpt:631
ACCEPT  all  --  0.0.0.0/0      0.0.0.0/0      state RELATED,ESTABLISHED
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:22
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:21
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:80
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:443
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:2121
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:8070
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:8071
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:8080
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:8081
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpts:8082:8090
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:30900
ACCEPT  tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:65535
REJECT  all  --  0.0.0.0/0      0.0.0.0/0      reject-with icmp-host-prohibited
#
```

IPTables – The Linux Firewall



```
10.212.2.215 - PuTTY
# vi /etc/sysconfig/iptables

# service iptables stop
Flushing firewall rules:           [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules:       [ OK ]
# service iptables status
Firewall is stopped.
# chkconfig iptables off
#
```

■ IPTables

- Knowledge Base article 4106
 - Title: *Configuring IPTables for Websense Content Gateway*
 - Batch script attached to KB article
 - Logon into www.mywebsense.com/support
 - Choose the *Websense Security Gateway* knowledge base

Reboot



```
10.212.2.215 - PuTTY
# reboot

Broadcast message from root (pts/1) (Wed Sep 16 8:48:26 2009):

The system is going down for reboot NOW!
#
```

- Install file
 - www.mywebsense.com
 - Knowledge Base article # 4191
 - Title: *v7: Accessing Websense Content Gateway downloads*
- Install Websense Content Gateway
 - Using putty
- Demonstration

Installing Websense Content Gateway

```
# pwd
/root
# mkdir /opt/wcg_v712
# cd /opt/wcg_v712
# ls
compat-libstdc++-33-3.2.3-47.3.i386.rpm  WebsenseCG712Setup_Lnx.tar.gz
# rpm -qa | grep compat-lib
compat-libstdc++-296-2.96-132.7.2
compat-libstdc++-33-3.2.3-47.3
compat-libgcc-296-2.96-132.7.2
compat-libcom_err-1.0-5
# rpm -ivh compat-libstdc++-33-3.2.3-47.3.i386.rpm
```


Installing Websense Content Gateway

```
# tar -xvzf WebsenseCG712Setup_Lnx.tar.gz
adm_help.tar
lx86_arms.tar
lx86inst.tar
lx86.tar
mds.tar
plugins.tar
subscription.txt
wcg_config.sh
wcg_install.sh
wcg.tar
# ls
adm_help.tar          plugins.tar
compat-libstdc++-33-3.2.3-47.3.i386.rpm  subscription.txt
lx86_arms.tar         wcg_config.sh
lx86inst.tar          wcg_install.sh
lx86.tar              wcg.tar
mds.tar               WebsenseCG712Setup_Lnx.tar.gz
#
```

Installing Websense Content Gateway

```
# ./wcg_install.sh
```

Installing Websense Content Gateway



Websense Content Gateway v7.1.2-1161
(c)1999 - 2009

IMPORTANT - THIS SUBSCRIPTION IS PROVIDED ONLY ON THE
CONDITION THAT THE SUBSCRIBER (REFERRED TO IN THIS AGREEMENT
--More--(3%)

```
Do you accept the above agreement [y/n]? Y
```

```
Websense Content Gateway Basic Installation Information
```

```
-----  
Enter the full path of the directory to install Websense Content Gateway:  
[/opt/WCG] >
```

Websense Content Gateway Administration Information

Enter the administrator password for the Websense Content Gateway management interface.

Username: admin

Password:> *****

Confirm password:> *****

Websense Content Gateway requires an email address for alarm notification.
Enter an email address using @ notation: [] > WebinarTest@Websense.com

Websense Content Gateway Integrations Configuration

Enter the Policy Server IP address (or leave blank for Data Security Suite-only integration): [] > 10.212.2.212

Enter the Filtering Service IP address: [10.212.2.212] >

Installing Websense Content Gateway

Websense Content Gateway Port Configuration

Websense Content Gateway uses 14 ports on your server.
Port Assignments:

'0'	Websense Content Gateway Proxy Port	8080
'1'	Web Interface port	8081
'2'	Overseer port	8082
'3'	Auto config port	8083
'4'	Process manager port	8084
'5'	Logging server port	8085
'6'	Clustering port	8086
'7'	Reliable service port	8087
'8'	Multicast port	8088
'9'	SNMP encapsulation port	8089
'E'	HTTPS inbound port	8070
'N'	HTTPS outbound port	8090
'M'	HTTPS management port	8071
'D'	Download Service port	30900

Enter the port assignment you would like to change:

'0-9,E,N,M,D' - specific port changes

'X' - no change

'H' - help

[X] > X

Websense Content Gateway Clustering Information

- '1' - Select '1' to configure Websense Content Gateway for full clustering. The nodes in the cluster will act as a single aggregate cache, including the functionality of a management cluster.
- '2' - Select '2' to configure Websense Content Gateway for management clustering. The nodes in the cluster will share configuration/management information automatically.
- '3' - Select '3' to operate this Websense Content Gateway as a single node.

Enter the cluster type for this Websense Content Gateway installation:

[3] > 3

Installing Websense Content Gateway

Websense Content Gateway Cache Disk Configuration

Would you like to enable raw disk cache [y/n]? Y

Select available disk resources to use for the cache. Remember that space used for the cache cannot be used for any other purpose.

Here are the available drives

[] (1) /dev/hdb 40020664320 0x0

Choose one of the following options:

'A' - Add disk(s) to cache

'R' - Remove disk(s) from cache

'S' - Add all available disks to cache

'U' - Remove all disks from cache

'X' - Done with selection, continue Websense Content Gateway installation.

Option: > A

[] (1) /dev/hdb 40020664320 0x0

Enter number to add item, press 'F' when finished:

[F] > 1

Item '1' is selected

[F] > F

Installing Websense Content Gateway

Here is the current selection
[X] (1) /dev/hdb 40020664320 0x0

Choose one of the following options:

'A' - Add disk(s) to cache

'R' - Remove disk(s) from cache

'S' - Add all available disks to cache

'U' - Remove all disks from cache

'X' - Done with selection, continue Websense Content Gateway installation.

Option: > X

Websense Content Gateway Optional Feedback Configuration

Websense Content Gateway can send information about scanned content to Websense, Inc. This information helps Websense, Inc. improve filtering and scanning technology and accuracy.

Websense software never includes information that would identify specific users.

Do you want to enable the Websense Content Gateway Feedback Agent [y/n]? Y

Installing Websense Content Gateway

Configuration Summary

Websense Content Gateway Install Directory : /opt/WCG
Admin Username for Websense Content Manager: admin
Alarm Email Address : WebinarTest@Websense.com

Policy Server IP Address : 10.212.2.212
Filtering Service IP Address : 10.212.2.212

Websense Content Gateway Cluster Type : NO_CLUSTER
Websense Content Gateway Cache Type : RAW_DISK
Cache Disk : /dev/hdb
Total Cache Partition Used : 1

* WARNING *

CACHE DISKS LISTED ABOVE WILL BE CLEARED DURING INSTALLATION!!
CONTENTS OF THESE DISKS WILL BE COMPLETELY LOST WITH NO CHANCE
OF RETRIEVAL.

Installer CANNOT detect all potential disk mirroring systems.
Please make sure the cache disks listed above are not in use
as mirrors of active file systems and do not contain any
useful data.

Do you want to continue installation with this configuration [y/n]? Y

Installing Websense Content Gateway

Writing values to file...done

Using configuration file: /tmp/WCGinstall.cfg

Extracting files...done

Installing Adaptive Redirection Module (ARM)...done

Configuring Websense Content Gateway cache. This may take a few minutes.
Do not interrupt cache configuration or you will have an unusable cache...done

Setting Websense Content Gateway environment...done

Installing SSL Manager...done

Starting services...

Starting Websense Download Service...

Starting Websense Content Gateway...

Installing Websense Content Gateway

COMPLETED Websense Content Gateway 7.1.2-1161 installation.
A log file of this installation process has been written to
/home/Websense/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 (Websense Content 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 /home/Websense.

#

- Failed install, review:
 - OS and kernel version
 - Proper libraries (RPMs) installed
 - Hostname and host file
 - Ethernet settings
 - DNS configuration
 - IPv6 disabled
 - Iptables correctly configured
 - SELinux disabled
 - Date and time match on Websense Content Gateway and Websense Web Security Gateway
 - Internet connectivity
- Once the problem is identified and corrected
 - Reinstall Websense Content Gateway

```
# ./wcg_install.sh -u
#####
#
#   Websense Content Gateway Uninstall
#   This will uninstall the Websense Content Gateway
#   on system ws-Webinar5.testadw2k3.techsupport2k3.com.
#
#####

Are you sure you want to remove Websense Content Gateway [y/n]?  Y
Using the installation in /opt/WCG
Disabling ARM for Linux26.
Looking at system files.
done

Checking for root privileges...
OK
Stopping Watchdog-Service...
Killing
Completed Websense Content Gateway Uninstall.
```

- Enter subscription key
 - Websense Content Gateway and Websense Web Security Gateway use the same key
- Websense Content Gateway services
 - Status check
- Verify Websense Web Security Gateway is integrated with Websense Content Gateway
 - Filtering Service install type
- Demonstration

- Logging into the Websense Content Gateway
 - `https://<IP address>:8081`

Activating Websense Content Gateway

WEBSense®
Content Gateway

Monitor | Configure

User: admin | Get Help!

My Proxy

- Summary
- Node
- Graphs
- Alarms

Protocols

Content Routing

Security

Subsystems

Networking

Performance

Version 7.1.2 build 1161 [More Detail](#)

Subscription Details

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

Node Details

Node	On/Off	Objects Served	Ops/Sec	Hit Rate	Throughput (Mbit/sec)	HTTP Hit (ms)	HTTP Miss (ms)
WS-Webinar5	On	0000000461	0.00	0.00%	0.00	0	0

Activating Websense Content Gateway

The screenshot displays the Websense Content Gateway configuration interface. At the top, the title bar reads "WEBSENSE® Content Gateway" and "websense". Below the title bar, there are tabs for "Monitor" and "Configure", and a user indicator "User: admin" with a "Get Help!" link.

The left sidebar contains a navigation menu with the following items:

- My Proxy
 - Basic
 - Subscription**
 - UI Setup
 - Snapshots
 - Logs
- Protocols
- Content Routing
- Security
- Subsystems
- Networking

The main content area shows the "Subscription Management" configuration page. It has two tabs: "Subscription Management" (selected) and "Scanning". Below the tabs is a "Basic Configuration" section with "Apply" and "Cancel" buttons. The "Subscription Key" section contains a text input field and a message: "◆ Enter your subscription key." Below this section are "Apply" and "Cancel" buttons.

Activating Websense Content Gateway

The screenshot displays the Websense Content Gateway configuration interface. At the top, the title bar reads "WEBSENSE® Content Gateway" and "websense". Below the title bar, there are tabs for "Monitor" and "Configure", and a user name "User: admin" on the left and a "Get Help!" link on the right. A left-hand navigation menu is visible, with "My Proxy" expanded to show "Basic", "Subscription", "UI Setup", "Snapshots", and "Logs". Other categories include "Protocols", "Content Routing", "Security", "Subsystems", and "Networking".

The main configuration area is titled "Basic Configuration" and has "General" and "Clustering" tabs. It includes "Apply" and "Cancel" buttons. The "Restart" section contains a "Restart" button and a description: "Restarts Websense Content Gateway proxy and manager services on all nodes in the cluster." The "Proxy Name" section has a text input field containing "ws-tswsgdemo.testad" and a description: "Specifies the name of the Websense Content Gateway node/cluster. In a Websense Content Gateway cluster, all nodes must share the same name." The "Alarm email" section has a text input field containing "WebinarTest@Webs" and a description: "Specifies the email address to which Websense Content Gateway will send alarm notifications."

Activating Websense Content Gateway

WEBSENSE®
Content Gateway

Monitor | Configure | User: admin | Get Help!

My Proxy

- Summary
- Node
- Graphs
- Alarms

Protocols

Content Routing

Security

Subsystems

Networking

Performance

Version 7.1.2 build 1161 [More Detail](#)

Subscription Details

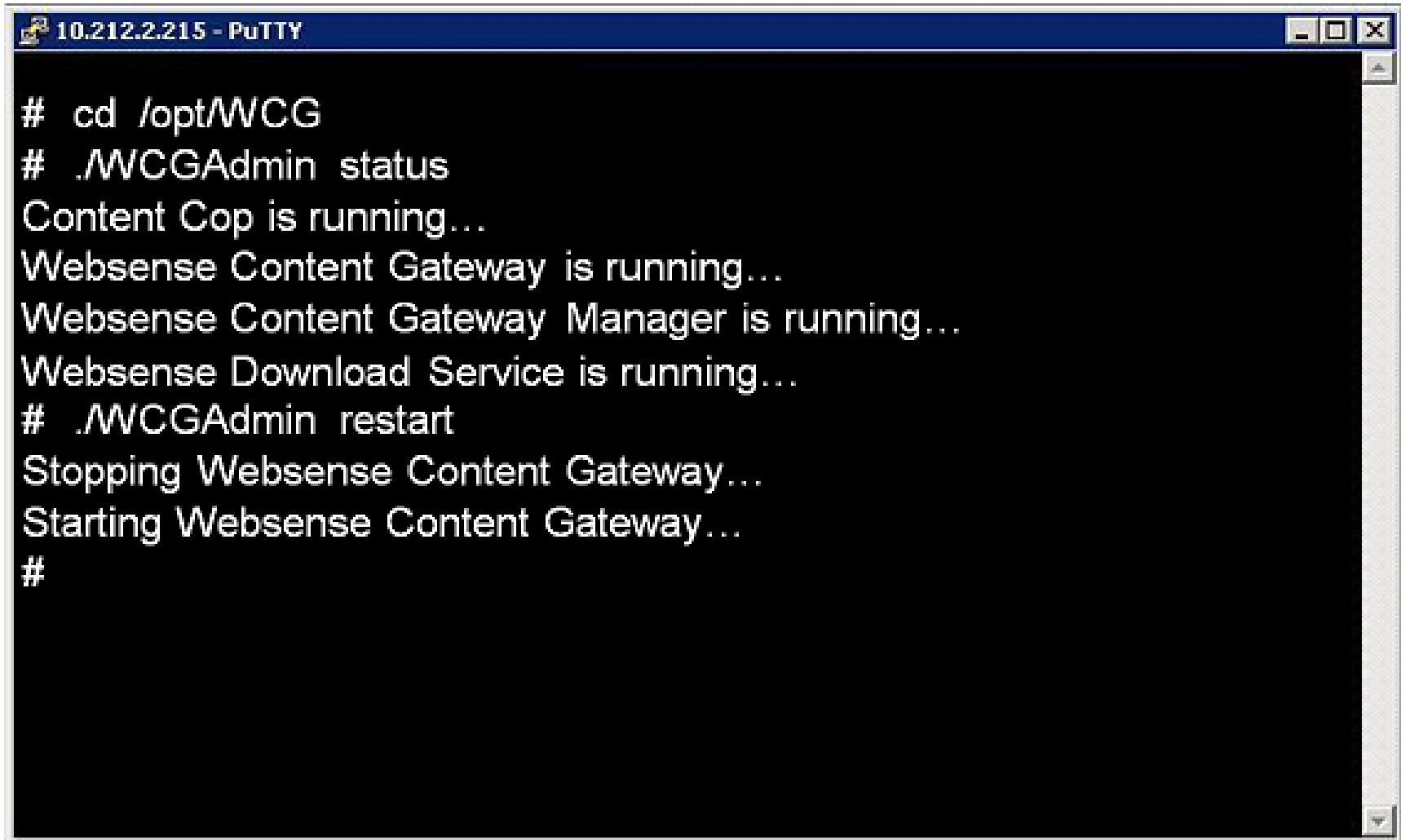
Feature	Purchased Status	Expiration Date
Content Categorization	Purchased	Sunday, September 27, 2009
Threat Detection	Purchased	Sunday, September 27, 2009
SSL Manager	Purchased	Sunday, September 27, 2009

Scanning Data Files

Engine Name	Engine Version	Data File Version	Last Update
Content Categorization	1.1	100244	Wednesday, September 02, 2009 08:55:39
Security Scanning	2.0	201820	Friday, September 11, 2009 10:00:16
Advanced File Scanning	2.0	97465	Saturday, September 12, 2009 17:38:55
Integrated Anti-Virus	SDK version: 5.1.0 - Scan Engine version: 4.4.3	200909121705	Saturday, September 12, 2009 12:11:06

Last time Content Gateway checked for data file updates - Saturday, September 12, 2009 20:09:28

Activating Websense Content Gateway



```
10.212.2.215 - PuTTY
# cd /opt/WCG
# ./WCGAdmin status
Content Cop is running...
Websense Content Gateway is running...
Websense Content Gateway Manager is running...
Websense Download Service is running...
# ./WCGAdmin restart
Stopping Websense Content Gateway...
Starting Websense Content Gateway...
#
```

Activating Websense Content Gateway

WEBSense®
WebSecurity

Policy Server: 10.212.2.212

Logon type: Websense account ⓘ Network account ⓘ

User name:

Password:

[Forgot my password](#)

Language: [Edit](#)

[MyWebsense](#) [Documentation](#)
[Patches \(Hotfixes\)](#) [Knowledge Base](#)
[Websense Security Labs](#) [Tips and Tutorials](#)

©2009 Websense, Inc.

Activating Websense Content Gateway

WEBSense®
WebSecurityGateway

Policy Server: 10.212.2.211

Logon type: Websense account ⓘ
 Network account ⓘ

User name:

Password:

[Forgot my password](#)

Language: [Edit](#)

[MyWebsense](#) [Documentation](#)
[Patches \(Hotfixes\)](#) [Knowledge Base](#)
[Websense Security Labs](#) [Tips and Tutorials](#)

©2009 Websense, Inc.

Activating Websense Content Gateway

The screenshot displays the Websense WebSecurity management interface. The top navigation bar includes the 'WebSecurity' logo and a 'Policy Server: 10.2' indicator. Below the navigation bar, there are tabs for 'Main' and 'Settings', and a status bar indicating 'Today: Health, Security, and Value Since Midnight'. The left sidebar contains a menu with categories like 'Status', 'Reporting', 'Policy Management', and 'Clients'. The main content area is divided into several panels:

- Health Alert Summary:** Contains three green checkmarks indicating no problems detected, a warning about the filtering service at 10.212.2.212 loading the master database, and a subscription expiration notice.
- Today's Value:** Lists blocked content types: Malicio (with a flame icon), Adult (with a red X icon), and Spywa (with a magnifying glass icon).
- Filtering Service Summary:** Shows a green checkmark next to the IP address 10.212.2.212 with the status 'Running'. A blue arrow points to this IP address.

Activating Websense Content Gateway

The screenshot displays the Websense WebSecurity management console. The left sidebar contains a navigation menu with sections: Status (Today, History, Alerts, Audit Log), Reporting (Presentation Reports, Investigative Reports), and Policy Management (Clients, Policies, Filters, Filter Components, Delegated Administration, Filter Lock). The main content area is titled 'Filtering Service Details' and shows the following information:

- Filtering Service: 10.212.2.211
- Status: Running
- Version: 7.1.0
- Operating System: Windows 2003 Service Pack 2
- Platform: Websense Content Gateway(TM)

A blue arrow points from the 'Platform' field to a sub-section titled 'Active Network Agent Connections', which lists:

- 10.212.2.211 - Status: Running

The top of the interface shows 'Policy Server: 10.2' and a breadcrumb trail: 'Today: Health, Security, and Value Since Midnight > Filtering S'.

Initial Configuration of Websense Web Security Gateway

- Downloading the Master Database via the proxy
- Scanning options
- Identify the Log Server location
- Configure Network Agent

- Demonstration

Initial Configuration of Websense Web Security Gateway

- Logging into the Manger
 - `https://<IP address>:9443`

Initial Configuration of Websense Web Security Gateway

WEBSENSE[®]
WebSecurityGateway

Policy Server: 10.212.2.211

Logon type: Websense account ⓘ Network account ⓘ

User name:

Password:

[Forgot my password](#)

Language: [Edit](#)

[MyWebsense](#) [Documentation](#)
[Patches \(Hotfixes\)](#) [Knowledge Base](#)
[Websense Security Labs](#) [Tips and Tutorials](#)

©2009 Websense, Inc.

Initial Configuration of Websense Web Security Gateway

The screenshot displays the Websense Web Security Gateway management console. The interface is divided into several sections:

- Header:** "WebSecurity" logo on the left and "Policy Server: 10.2" on the right.
- Navigation:** "Main" and "Settings" tabs are visible.
- Left Sidebar:** A menu with categories: "Status" (Today, History, Alerts, Audit Log), "Reporting" (Presentation Reports, Investigative Reports), "Policy Management" (Clients, Policies, Filters, Filter Components, Delegated Administration, Filter Lock).
- Main Content Area:**
 - Today: Health, Security, and Value Since Midnight** - Includes "Database Download", "Customize", and "Print" options.
 - Health Alert Summary:** Lists three alerts: "No problems detected", "The Filtering Service at 10.212.2.212 is loading the Master Database", and "Your subscription will expire within 1 month".
 - Filtering Service Summary:** Shows "10.212.2.212 - Status: Running".
 - Today's Value:** Lists blocked categories: "Malicio" (with a flame icon), "Adult:" (with a red X icon), and "Spywa" (with a magnifying glass icon).

Initial Configuration of WebSense Web Security Gateway

WebSense WebSecurityGateway Policy Server: 10.212.2.211 Role: Super Adm

Main Settings

General

Account

Filtering

Database Download >>>

Directory Services

Logon Directory

Logging

Risk Classes

User Identification

Remote Filtering

Scanning

Policy Servers

Alerts and Notifications

Network Agent

Reporting

Enable real-time security updates

Proxy Server or Firewall

If Websense software must go through a proxy server or firewall to access the Internet, configure these settings.

Use proxy server or firewall

Server IP or name: 10.212.4.27

Port: 8080

Authentication

If the proxy server or firewall requires authentication, configure these settings.

Use authentication

User name:

Password:

OK Cancel

Initial Configuration of Websense Web Security Gateway

The screenshot displays the Websense Web Security Gateway configuration window. The title bar includes the Websense logo and the text "WebSecurityGateway". On the right side of the title bar, there are fields for "Policy Server:" with a dropdown menu showing "10.212.2.211" and "Role:" with a dropdown menu showing "Super Adm".

The main interface is divided into a left-hand navigation pane and a right-hand content area. The navigation pane has a "Main" tab and a "Settings" sub-tab. Under "Settings", there is a list of categories: General, Account, Filtering, Database Download, Directory Services, Logon Directory, Logging, Risk Classes, User Identification, Remote Filtering, Scanning (highlighted in yellow with a right-pointing arrow), Policy Servers, Alerts and Notifications, Network Agent, and Reporting.

The right-hand content area is titled "Common Options" and "Exceptions". It contains two main sections:

- Content Categorization**: A section with the description "Categorize content for sites not in the Master Database and for sites with dynamic content as identified by Websense Security Labs." It has two radio button options: "Off" and "On (recommended)". The "On (recommended)" option is selected.
- Security Threats**: A section with a sub-section titled "Security Scanning". The description is "Inspect Web content in incoming traffic and immediately block malicious content such as phishing, malware, and viruses." It has three radio button options: "Off", "Content from dynamic sites as identified by Websense Security Labs (recommended)", and "All content from all sites (this option is resource intensive)". The "Content from dynamic sites as identified by Websense Security Labs (recommended)" option is selected.

At the bottom of the window, there are two buttons: "OK" and "Cancel".

Initial Configuration of Websense Web Security Gateway

The screenshot displays the Websense Web Security Gateway configuration interface. At the top, the title bar reads "WebSense® WebSecurityGateway" and includes a "Policy Server:" dropdown menu set to "10.212.2.211" and a "Role:" dropdown menu set to "Super Adm". Below the title bar, there are navigation tabs for "Main", "Settings", and "Logging", with "Logging" being the active tab. A "Help" button is visible in the top right corner of the settings area.

The left sidebar contains a list of configuration categories: General, Account, Filtering, Database Download, Directory Services, Logon Directory, Logging (highlighted with a yellow background and three right-pointing chevrons), Risk Classes, User Identification, Remote Filtering, Scanning, Policy Servers, Alerts and Notifications, Network Agent, and Reporting.

The main content area is titled "About Logging Settings" and contains the following text: "Websense software lets you determine what information should be logged. Information that is not logged cannot be included in Internet usage reports." Below this, there is a section titled "Reporting Log Records" with the text: "These settings determine what user information is logged and available in your Internet usage reports. If you deselect both check boxes, no user data will appear in your reports. For all logged categories and protocols:"

Two checkboxes are present, both of which are checked:

- Log IP addresses
- Log user names

Below the checkboxes, there are two input fields:

- Log Server IP address or name:
- Port:

A "Check Status" button is located below the input fields. At the bottom right of the configuration window, there are "OK" and "Cancel" buttons.

Initial Configuration of Websense Web Security Gateway

The screenshot displays the Websense Web Security Gateway configuration interface. The top navigation bar includes the title "WebSecurityGateway" and the "Settings" tab. The "Policy Server" is set to "10.212.2.211" and the user role is "Super Adm". The left sidebar contains a menu with options: "Main", "Settings", "Log Database", "General", "Alerts and Notifications", "Network Agent", "Reporting", "Preferences", "Log Database" (highlighted with a yellow background and a right-pointing arrow), and "Log Server".

The main content area is titled "Log Database" and shows "Options for: 10.212.2.211 \ wslogdb70". It features a "Refresh" button with a globe icon. The configuration is divided into three sections:

- Database Rollover Options:** "Roll over every:" is set to "1500" MB. A "Save Now" button is located at the bottom right of this section.
- Full URL Logging:** The checkbox "Record full URL of each site requested." is checked. Below it, a note states: "If this option is left unchecked, only the domain name will be saved in the Log Database. Saving full URLs produces a larger Log Database, but provides greater detail." A "Save Now" button is at the bottom right.
- Internet Browse Time Configuration:** "Job start time:" is set to "02 : 00". "Read time threshold:" is set to "3". "Last read time:" is set to "3". A "Save Now" button is at the bottom right.

Initial Configuration of Websense Web Security Gateway

WebSense® WebSecurityGateway Policy Server: 10.212.2.211 Role: Super Adm

Main **Settings**

General

Alerts and Notifications

Network Agent

Global

10.212.2.211 >>>

Reporting

Proxies and Caches

Network Agent must know IP addresses of all proxy or cache servers used by the machines this Network Agent monitors. This information is needed to ensure accurate filtering and logging.
List any proxy and cache servers.

IP Address

10.212.4.27

Add Delete

Network Interface Cards

Name	IP Address	Description
<u>NIC-1</u>	10.212.2.211	Broadcom NetXtreme Gigabit Ethernet Driver

OK Cancel

- Enable HTTPS
- Create a *self-signed* certificate
- Backup the *self-signed* certificate
- Restart Websense Content Gateway
- Import the certificate into the *Trusted Root CA Store*
- Test SSL

- Demonstration

Allowing HTTPS Web sites

- Certificate validation
 - Working with incidents
 - Tunneling a Web site
-
- Demonstration



Tech Alerts

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



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.



ask.websense.com

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

Webinar Update

Title: Common Configuration Methodologies for
Websense Content Gateway

Date: October 28, 2009

Time: 8:30 AM Pacific Time

How to register:

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

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?

