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

© 2013 Websense, Inc.
Title:
- Support Specialist

Accomplishments:
- 9 years supporting Websense products

Qualifications:
- Technical Support Mentor
- Product Trainer
Goals And Objectives

- 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
Deployment Considerations

- **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
Deployment Considerations

- 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.
V-Series appliance

- Websense Content Gateway is the web proxy for Web Security Gateway
• 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
Red Hat Server Configuration

• Verify system hardware requirements
• Verify kernel version support

```
[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 ~]#
```
Red Hat Server Configuration

- Verify the IP address associated with the hostname

```
[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
```

Red Hat Server Configuration

- Verify the hostname and default gateway
Red Hat Server Configuration

• Verify the DNS specification

```
[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 ~]#`
```
Red Hat Server Configuration

- Verify DNS

```bash
[root@WS-GDID-50 ~]# nslookup www.yahoo.com
Server: 10.212.5.210
Address: 10.212.5.210#53

Non-authoritative answer:
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:
```
Red Hat Server Configuration

• Verify the routing table

```
[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
```
### Red Hat Server Configuration

- **Test hostname resolution**

```
[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 ttl=64 time=0.020 ms
^Z
[2]+ Stopped
[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 ttl=64 time=0.019 ms
^Z
[3]+ Stopped
[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
[root@WS-GDID-50 ~]# ping 10.212.5.209
```
Red Hat Server Configuration

- Verify the date and time
• Verify the network interface configuration

```
[root@WS-GID-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
```

© 2013 Websense, Inc.
Red Hat Server Configuration

- Verify that SELinux is disabled

```
[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
```

© 2013 Websense, Inc.
Verify the IPTables are stopped

```
[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 ~]# _
```
Red Hat Server Configuration

• 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
Accessing Content Gateway Manager

- Content Gateway Manager on the V-Series appliance

https://<C interface>:9447
https://<C interface>:8081
Accessing Content Gateway Manager

- Content Gateway Manager on Red Hat software

```
*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]#
Post Install Check

- Ensure features are enabled and data files downloaded
Post Install Check

- Confirm the Content Gateway successfully registered
Post Install Check

- 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
Enabling Features – Demonstrations

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

• 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
Reference

- 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
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
Training

• 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