TP and FTP Proxy−caching Using a Cisco Cache Engine 550 an

Table of Contents

HTTP and FTP Proxy−caching Using a Cisco Cache Engine 550 and a PIX Firewall

Introduction

This tech note shows you how to set up a Cisco Cache Engine 550 to perform Hypertext Transfer Protocol (HTTP) / File Transfer Protocol (FTP) caching for Multipurpose Internet Mail Extensions (MIME) file types (RFC 2046) and for FTP directory listings.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco Cache Engine 550 running Cisco Cache Software Release 2.51
- Cisco 2600 Router running Cisco IOS® Software Release 12.2
- Cisco PIX Firewall running Secure PIX Firewall Software Release 6.0(1)
- Web server running Internet Information Server 4.0 on Windows NT 4.0 SP6a

The inside clients need to explicitly configure their browsers to use a manual HTTP/FTP proxy to the IP address of the Cache Engine on a specified port.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Background Theory

Inside clients need to explicitly configure their browsers to use a manual HTTP/FTP proxy to the IP address of the Cache Engine on a specified port. Specifically, the Cache Engine handles ftp:// style FTP requests over HTTP transport in proxy mode in passive and active mode and in an anonymous and authenticated mode (RFC 1738).

The Private Internet Exchange (PIX) firewall in front of the Cache Engine allows HTTP/FTP traffic coming only from the single IP address of the Cache Engine. This means that clients cannot HTTP/FTP directly to the outside. Because all requests come from just one IP address, the Cache Engine enforces the security policy of who and who is not allowed to HTTP/FTP outside.

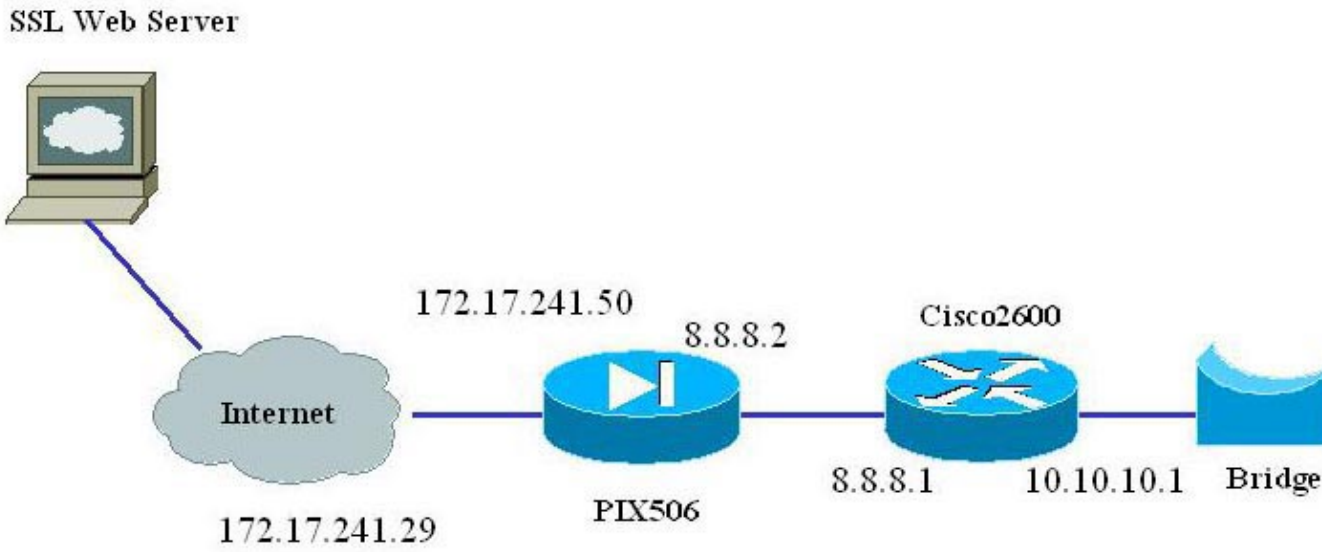
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the IOS Command Lookup tool.

Network Diagram

This document uses the network setup shown in the diagram below.



Configurations

This document uses the configurations shown below.

Cache Engine 550 Running Cisco Cache Software Release 2.51

```
!
!
hostname tikka
!
interface ethernet 0
ip address 10.10.10.50 255.255.255.0
ip broadcast-address 10.10.10.255
bandwidth 10
halfduplex
exit
!
interface ethernet 1
exit
!
ip default-gateway 10.10.10.1
ip name-server 144.254.15.102
ip domain-name cisco.com
ip route 0.0.0.0 0.0.0.0 10.10.10.1
inetd enable ftp 12
cron file /local/etc/crontab
clock timezone CET -7 0
!
no bypass load enable
http max-ttl hours text 4 binary 8
http proxy incoming 8080
```

```
!
radius-server authtimeout 21
radius-server key ****
authentication login local enable
authentication configuration local enable
rule no-cache url-regex .*cgi-bin.*
rule no-cache url-regex .*aw-cgi.*
ftp proxy anonymous-pswd ****
ftp proxy incoming 8080
!
!
```

PIX Version 6.0(1)

```
PIX Version 6.0(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 intf2 security10
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-cache
 fixup protocol ftp 21
 fixup protocol http 80
 fixup protocol h323 1720
 fixup protocol rsh 514
 fixup protocol smtp 25
 fixup protocol sqlnet 1521
 fixup protocol sip 5060
 fixup protocol skinny 2000
 names
 access-list restrict-access-out permit ip host 10.10.10.50 any
 access-list restrict-access-out deny ip any any

!--- This access-list is allowing any IP traffic for the CE (UDP DNS queries
 !--- are also needed to go through the PIX).

 pager lines 24
 logging on
 logging buffered debugging
 interface ethernet0 10baset
 interface ethernet1 10baset
 interface ethernet2 auto shutdown
 mtu outside 1500
 mtu inside 1500
 mtu intf2 1500
 ip address outside 172.17.241.47 255.255.255.0
 ip address inside 8.8.8.2 255.255.255.0
 ip address intf2 127.0.0.1 255.255.255.255
 ip audit info action alarm
 ip audit attack action alarm
 no failover
 failover timeout 0:00:00
 failover poll 15
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 failover ip address intf2 0.0.0.0
 pdm history enable
 arp timeout 14400
 global (outside) 1 172.17.241.48
 nat (inside) 1 0.0.0.0 0.0.0.0 0 0

!--- The lines nat and global are meant for any other traffic that is not supposed to be
 !--- proxied by the CE (mail for example), but you would need to explicitly define
```

```
!--- an entry in the restrict-access-out ACL to permit these outbound connections.

access-group restrict-access-out in interface inside
static (inside, outside) 172.17.241.50 10.10.10.50
! This static would be used to statically map the CE to a specific external address.
route outside 0.0.0.0 0.0.0.0 172.17.241.1 1
route inside 10.10.10.0 255.255.255.0 8.8.8.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
AAA-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
telnet 10.10.10.0 255.255.255.0 inside
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:7f08b39173bbe1302bd24273973c89de
: end
[OK]
```

2600

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname suicide
!
enable password ww
!
username all
!
!
!
!
ip subnet-zero
no ip domain-lookup
!
cns event-service server
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 8.8.8.1 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 speed 10
 half-duplex
!
interface Serial0/0
```

```
 no ip address
 shutdown
 no fair-queue
!
interface FastEthernet0/1
 ip address 10.10.10.1 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 speed 10
 half-duplex
!
interface Serial0/1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 8.8.8.2
ip http server
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
no scheduler allocate
end
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter tool, which allows you to view an analysis of **show** command output.

2600 Router

You do not need to configure the 2600 router for FTP proxy caching. In this example, the router only relays inbound/outbound packets. The following example shows how to set FTP proxy−caching to an external FTP server. With HTTP, the procedure is the same. The client configures the FTP proxy in the browser, pointing it to 10.10.10.50:8080.

All traffic goes through the Cache Engine. In the PIX, configure a static (with no conduit) for the Cache Engine. Users cannot access FTP sites without using the Cache Engine as a proxy. The following partial configuration shows an example of how to do this.

```
pix-cache#
pix-cache# show xlate
1 in use, 1 most used
Global 172.17.241.50 Local 10.10.10.50 static
pix-cache# show conduit
pix-cache# show outbound
pix-cache#
```

To enforce a security policy and block specific clients to access FTP to the outside, use the **rule block** command.

```
rule block src-ip 10.10.10.11 255.255.255.0
```

You can view the statistics of the traffic being cached (FTP hits) by using the **show statistics ftp** command in the Cache Engine.

```
tikka#show statistics ftp
FTP Statistics
--------------
FTP requests Received = 27
FTP Hits
                                  Requests      Percentage

Number of hits =                   17            63.0 %
Bytes =                            358209        39.6 %
FTP Misses

                                  Requests      Percentage
Number of misses =                 10            37.0 %
Bytes =                            547368        60.4 %
Requests sent to Outgoing Proxy    = 0
Requests sent to origin ftp server = 10
FTP error count = 0
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

2600 Router

The following logs came from the Cache Engine upon the request issued in the client browser.

```
tikka#debug http header all
tikka#debug ftp packets
tikka#
Http request headers received from client:
GET ftp://172.17.241.216/sample.txt HTTP/1.0
Referer: ftp://172.17.241.216/
Proxy-Connection: Keep-Alive
User-Agent: Mozilla/4.75 [en] (WinNT; U)
Pragma: no-cache
Host: 172.17.241.216
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Encoding: gzip
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
Mon Jul 2 06:40:59 2001: GET ftp://172.17.241.216/sample.txt HTTP/1.0
Referer: ftp://172.17.241.216/
Proxy-Connection: Keep-Alive
User-Agent: Mozilla/4.75 [en] (WinNT; U)
Pragma: no-cache
Host: 172.17.241.216
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Encoding: gzip
Accept-Language: en
Accept-Charset: ISO-8859-1,*,utf-8
Send Cmd : USER anonymous
Mon Jul 2 06:40:59 2001: Send Cmd : USER anonymous
Send Cmd : PASS XXXX
Mon Jul 2 06:40:59 2001: Send Cmd : PASS XXXX
Send Cmd : CWD sample.txt
```

```
Mon Jul 2 06:40:59 2001: Send Cmd : CWD sample.txt
Send Cmd : MDTM sample.txt
Mon Jul 2 06:40:59 2001: Send Cmd : MDTM sample.txt
get_reply_info(): Last Modified Time : 1942132164
Mon Jul 2 06:40:59 2001: get_reply_info(): Last Modified Time : 1942132164
Send Cmd : TYPE A
Mon Jul 2 06:40:59 2001: Send Cmd : TYPE A
Send Cmd : PASV
Mon Jul 2 06:40:59 2001: Send Cmd : PASV
Send Cmd : RETR sample.txt
Mon Jul 2 06:40:59 2001: Send Cmd : RETR sample.txt
Send Cmd : QUIT
Mon Jul 2 06:41:00 2001: Send Cmd : QUIT
```

Related Information

- **Cisco CSS 11000 Series Product Support Page**
- **Technical Support − Cisco Systems**

Updated: Oct 30, 2002 Document ID: 12560