

Configure ACE with Source NAT and Client IP Header Insert

Document ID: 107399

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

Related Information

Introduction

This document provides a sample configuration for the Application Control Module (ACE) configured for source Network Address Translation (NAT) while inserting the original client IP address in the HTTP header. When using source NAT, the client IP address is not passed to the load balanced server. The insertion of the Client IP address into the header allows the servers to see the IP that made the connection. The servers default gateway points to the MSFC in the server VLAN. The only communication that needs to be load balanced will pass through the ACE.

This sample uses two contexts:

- the admin context is used for remote management and Fault Tolerant (FT) configuration
- the second context, C1, is used for load balancing

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

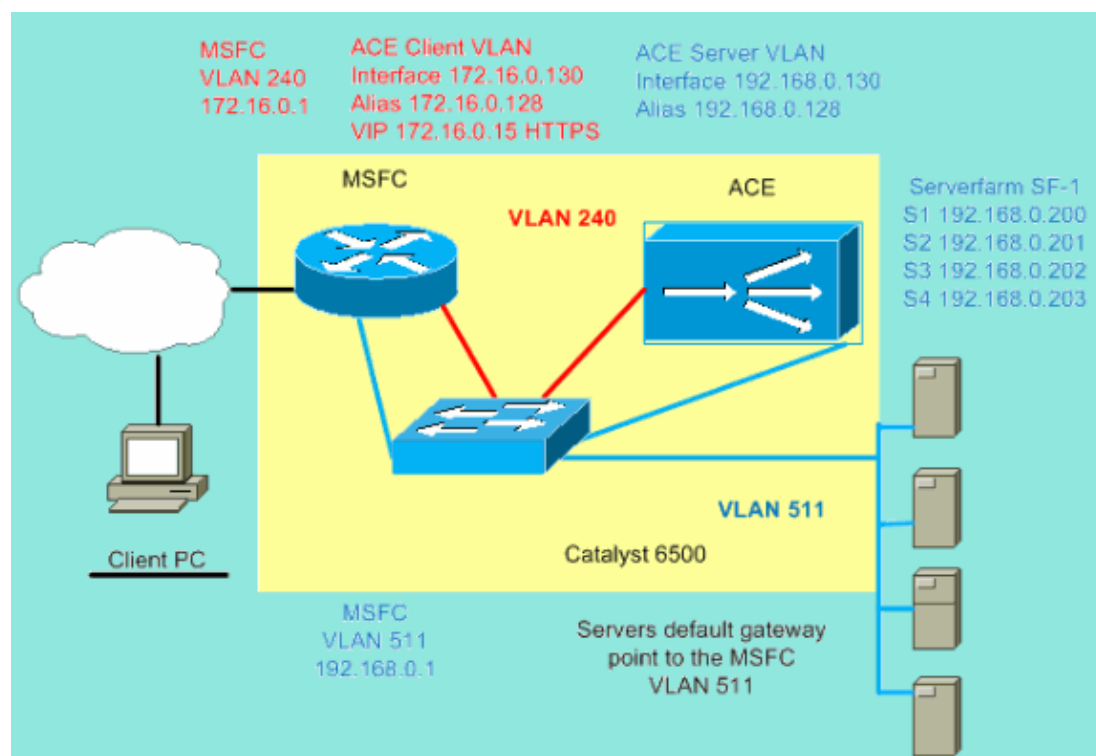
Configure

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

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- Catalyst 6500 ACE slot 2 C1 context
- Catalyst 6500 ACE slot 2 Admin context
- Catalyst 6500 MSFC configuration

ACE C1 Context

```
switch/C1#show run
Generating configuration...

access-list any line 8 extended permit icmp any any
access-list any line 16 extended permit ip any any

!--- Access-list used to permit or deny traffic from entering the ACE.

probe tcp SERVERS
  interval 5
  passdetect interval 10
```

```
!--- TCP probe used to test the availability of the servers.
```

```
parameter-map type http HTTP_PARAMETER_MAP  
  persistence-rebalance
```

```
!--- Parameter-map used to configure advanced http behavior.
```

```
!--- Persistence-rebalance inspects every get and matches to specific content.
```

```
!--- Without this command only the first get in a tcp session will be inspected.
```

```
rserver host S1  
  ip address 192.168.0.200  
  inservice
```

```
rserver host S2  
  ip address 192.168.0.201  
  inservice
```

```
rserver host S3  
  ip address 192.168.0.202  
  inservice
```

```
rserver host S4  
  ip address 192.168.0.203  
  inservice
```

```
serverfarm host SF-1  
  probe SERVERS  
  rserver S1  
    inservice  
  rserver S2  
    inservice  
  rserver S3  
    inservice  
  rserver S4  
    inservice
```

```
!--- Serverfarm used for load balanced traffic.
```

```
class-map match-all L4VIPCLASS  
  2 match virtual-address 172.16.0.15 tcp eq www
```

```
!--- Layer 4 class-map defining IP address and port.
```

```
class-map type management match-any REMOTE_ACCESS  
  2 match protocol ssh any  
  3 match protocol telnet any  
  4 match protocol icmp any  
  5 match protocol snmp any  
  6 match protocol http any
```

```
!--- Remote management class-map defining protocols allowed to manage the ACE.
```

```
policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY  
  class REMOTE_ACCESS  
    permit
```

```
policy-map type loadbalance http first-match WEB_L7_POLICY  
  class class-default  
    serverfarm SF-1  
    insert-http x-forward header-value "%is"
```

```
!--- Policy-map will insert the IP address of the client when sending traffic to the serverfarm.
```

```
policy-map multi-match VIPs  
  class L4VIPCLASS  
    loadbalance vip inservice  
    loadbalance policy WEB_L7_POLICY  
    loadbalance vip icmp-reply active  
    loadbalance vip advertise active
```

```

nat dynamic 1 vlan 511
appl-parameter http advanced-options HTTP_PARAMETER_MAP

!--- Multi-match policy ties the class-map and policy-maps together.
!--- Clients matching class L4VIPCLASS will use source NAT.

interface vlan 240
 ip address 172.16.0.130 255.255.255.0
 alias 172.16.0.128 255.255.255.0
 peer ip address 172.16.0.131 255.255.255.0
 access-group input any
 service-policy input REMOTE_MGMT_ALLOW_POLICY
 service-policy input VIPs
 no shutdown

!--- Client side VLAN; This is the VLAN clients will enter the ACE.
!--- Apply access-lists and service-policies that are needed.

interface vlan 511
 ip address 192.168.0.130 255.255.255.0
 alias 192.168.0.128 255.255.255.0
 peer ip address 192.168.0.131 255.255.255.0
 access-group input any
 nat-pool 1 192.168.0.254 192.168.0.254 netmask 255.255.255.0 pat
 no shutdown

!--- Server side VLAN.

ip route 0.0.0.0 0.0.0.0 172.16.0.1

!--- Default gateway points to the MSFC.

switch/C1#

```

ACE Admin Context

```

switch/Admin#show running-config
Generating configuration....

boot system image:c6ace-t1k9-mz.A2_1_0a.bin

resource-class RC1
  limit-resource all minimum 50.00 maximum equal-to-min

!--- Resource-class used to limit the amount of resources a specific context can use.

access-list any line 8 extended permit icmp any any
access-list any line 16 extended permit ip any any

rserver host test

class-map type management match-any REMOTE_ACCESS
  2 match protocol ssh any
  3 match protocol telnet any
  4 match protocol icmp any
  5 match protocol snmp any
  6 match protocol http any

policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
  class REMOTE_ACCESS
    permit

interface vlan 240
 ip address 172.16.0.4 255.255.255.0
 alias 172.16.0.10 255.255.255.0

```

```

peer ip address 172.16.0.5 255.255.255.0
access-group input any
service-policy input REMOTE_MGMT_ALLOW_POLICY
no shutdown
interface vlan 511
ip address 192.168.0.4 255.255.255.0
alias 192.168.0.10 255.255.255.0
peer ip address 192.168.0.5 255.255.255.0
access-group input any
no shutdown

ft interface vlan 550
ip address 192.168.1.4 255.255.255.0
peer ip address 192.168.1.5 255.255.255.0
no shutdown

!--- VLAN used for fault tolerant traffic.

ft peer 1
heartbeat interval 300
heartbeat count 10
ft-interface vlan 550

!--- FT peer definition defining heartbeat parameters and to associate the ft VLAN.

ft group 1
peer 1
peer priority 90
associate-context Admin
inservice

!--- FT group used for Admin context.

ip route 0.0.0.0 0.0.0.0 172.16.0.1

context C1
allocate-interface vlan 240
allocate-interface vlan 511
member RC1

!--- Allocate vlans the context C1 will use.

ft group 2
peer 1
no preempt
associate-context C1
inservice

!--- FT group used for the load balancing context C1.

username admin password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/ role Admin domain default-domain
username www password 5 $1$UZIiwUk7$QMvYN1JASaycabrHkhGcS/ role Admin domain default-domain

switch/Admin#

```

Router config

```

!--- Only portions of the config relevant to the ACE are displayed.

sf-cat1-7606#show run
Building configuration...

```

```

!--- Output Omitted.

svclc multiple-vlan-interfaces
svclc module 2 vlan-group 2
svclc vlan-group 2 220,240,250,510,511,520,540,550

!--- Before the ACE can receive traffic from the supervisor engine in the Catalyst 6500
!--- or Cisco 6600 series router, you must create VLAN groups on the supervisor engine,
!--- and then assign the groups to the ACE.
!--- Add vlans to the vlan-group that are needed for ALL contexts on the ACE.

interface Vlan240
description public-vip-172.16.0.x
ip address 172.16.0.2 255.255.255.0
standby ip 172.16.0.1
standby priority 20
standby name ACE_slot2

!--- SVI (Switch Virtual Interface). The standby address is the default gateway for the ACE.

!--- Output Ommited.

sf-cat1-7606#

```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show serverfarm name** Displays information about the serverfarm and the state of the rservers.

This example provides a sample output:

```

switch/C1#show serverfarm SF-1
serverfarm      : SF-1, type: HOST
total rservers  : 4

-----
--
--          real                weight state          current  total  failure
s -----+-----+-----+-----+-----+-----
--
rserver: S1
  192.168.0.200:0      8    OPERATIONAL  0         114    0
rserver: S2
  192.168.0.201:0      8    OPERATIONAL  0         113    0
rserver: S3
  192.168.0.202:0      8    OPERATIONAL  0         109    0
rserver: S4
  192.168.0.203:0      8    OPERATIONAL  0         106    0

```

- **show service-policy name** Displays http statistics.

This example provides a sample output:

```

switch/C1#show service-policy VIPs

```

Status : ACTIVE

```
-----
Interface: vlan 240
  service-policy: VIPs
  class: L4VIPCLASS
  nat:
    nat dynamic 1 vlan 511
    curr conns      : 0          , hit count      : 300
    dropped conns   : 0
    client pkt count : 1503      , client byte count: 195846
    server pkt count : 1731      , server byte count: 1760884
    conn-rate-limit  : 0          , drop-count     : 0
    bandwidth-rate-limit : 0      , drop-count     : 0
  loadbalance:
    L7 loadbalance policy: WEB_L7_POLICY
    VIP Route Metric      : 77
    VIP Route Advertise   : ENABLED-WHEN-ACTIVE
    VIP ICMP Reply        : ENABLED-WHEN-ACTIVE
    VIP State: INSERVICE
    curr conns            : 0          , hit count      : 300
    dropped conns         : 0
    client pkt count      : 1503      , client byte count: 195846
    server pkt count      : 1731      , server byte count: 1760884
    conn-rate-limit       : 0          , drop-count     : 0
    bandwidth-rate-limit  : 0          , drop-count     : 0
  Parameter-map(s):
    HTTP_PARAMETER_MAP
```

- **show stats http** Displays http statistics.

This example provides a sample output:

```
switch/C1#show stats http

+-----+
+----- HTTP statistics -----+
+-----+
LB parse result msgs sent : 109          , TCP data msgs sent      : 294

Inspect parse result msgs : 0            , SSL data msgs sent      : 0

TCP fin/rst msgs sent      : 0            , Bounced fin/rst msgs sent: 0

SSL fin/rst msgs sent      : 0            , Unproxy msgs sent       : 109

Drain msgs sent            : 79           , Particles read          : 520

Reuse msgs sent            : 0            , HTTP requests           : 109

Reproxied requests        : 38           , Headers removed         : 0

Headers inserted         : 109         , HTTP redirects          : 0

HTTP chunks                : 0            , Pipelined requests      : 0

HTTP unproxy conns        : 109         , Pipeline flushes        : 0

Whitespace appends        : 0            , Second pass parsing     : 0

Response entries recycled : 0            , Analysis errors         : 0

Header insert errors       : 0            , Max parselen errors     : 0

Static parse errors        : 0            , Resource errors         : 0
```

Invalid path errors : 0 , Bad HTTP version errors : 0

Headers rewritten : 0 , Header rewrite errors : 0

- **show conn** Displays current connections and the state they are in.

This example provides a sample output:

```
switch/Cl#show conn
```

```
total current connections : 2
```

conn-id	np	dir	proto	vlan	source	destination	state
11	1	in	TCP	240	172.16.10.221:1712	172.16.0.15:80	ESTAB
19	1	out	TCP	511	192.168.0.201:80	192.168.0.254:1369	ESTAB

- **sniffer trace** A sniffer trace to confirm that the header is being inserted.

This example provides a sample output:

```
GET / HTTP/1.1
```

```
x-forward: 172.16.10.221
```

```
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave
```

```
Accept-Language: en-us
```

```
Accept-Encoding: gzip, deflate
```

```
If-Modified-Since: Fri, 30 Nov 2007 16:59:08 GMT
```

```
If-None-Match: "0164b527233c81:767"
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
```

```
Host: www.cisco.com
```

```
Connection: Keep-Alive
```

```
HTTP/1.1 304 Not Modified
```

```
Content-Location: http://www.cisco.com/index.htm
```

```
Last-Modified: Fri, 30 Nov 2007 16:59:08 GMT
```

```
Accept-Ranges: bytes
```

```
ETag: "0164b527233c81:767"
```

```
Server: Microsoft-IIS/6.0
```

```
X-Powered-By: ASP.NET
```

```
Date: Tue, 20 May 2008 19:10:04 GMT
```

```
GET /header.html HTTP/1.1
```

```
x-forward: 172.16.10.221
```

```
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave
```

```
Referer: http://www.cisco.com/
```

```
Accept-Language: en-us
```

```
Accept-Encoding: gzip, deflate
```

```
If-Modified-Since: Fri, 30 Nov 2007 16:59:08 GMT
```

```
If-None-Match: "0164b527233c81:767"
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
```

```
Host: www.cisco.com
```

```
Connection: Keep-Alive
```

```
HTTP/1.1 304 Not Modified
```

```
Last-Modified: Fri, 30 Nov 2007 16:59:08 GMT
```

```
Accept-Ranges: bytes
```

```
ETag: "0164b527233c81:767"
```

```
Server: Microsoft-IIS/6.0
```

```
X-Powered-By: ASP.NET
```

```
Date: Tue, 20 May 2008 19:10:04 GMT
```


Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2013 – 2014 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 09, 2008

Document ID: 107399
