配置CSM负载 平衡SSL到SCAs组群的单臂代理模式

Contents

Introduction

本文为安全套接字层SSL数据流内容交换模块(CSM)负荷平衡提供一配置示例给组群安全内容加速器(SCAs)。配置是为SCAs在与连接的不透明的代理模式下在一端口模式。

在不透明的模式下， SCA使用SCA IP地址作为来源与Web服务器的明文连接。

Note: 请使用两个不同的VLANs/IP子网络SCAs和Web服务器;一个子网络是为所有SCAs，并且一个分开的子网络是为所有Web服务器。如果在同一个第2层(L2)域安置两个组群，源网络地址转换(NAT)是必要的。来源NAT保证信息包回到CSM，并且Catalyst系列硬件不L2交换机信息包。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

本文的信息根据这些VLAN/子网络：

- 客户端：虚拟IP (VIP)和上游路由器(多层交换特性卡[MSFC])
- 有CSM的Catalyst 6500/6000在Slot 5
- 服务器端1 ：Web服务器
- 服务器端2 ：SCAs

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

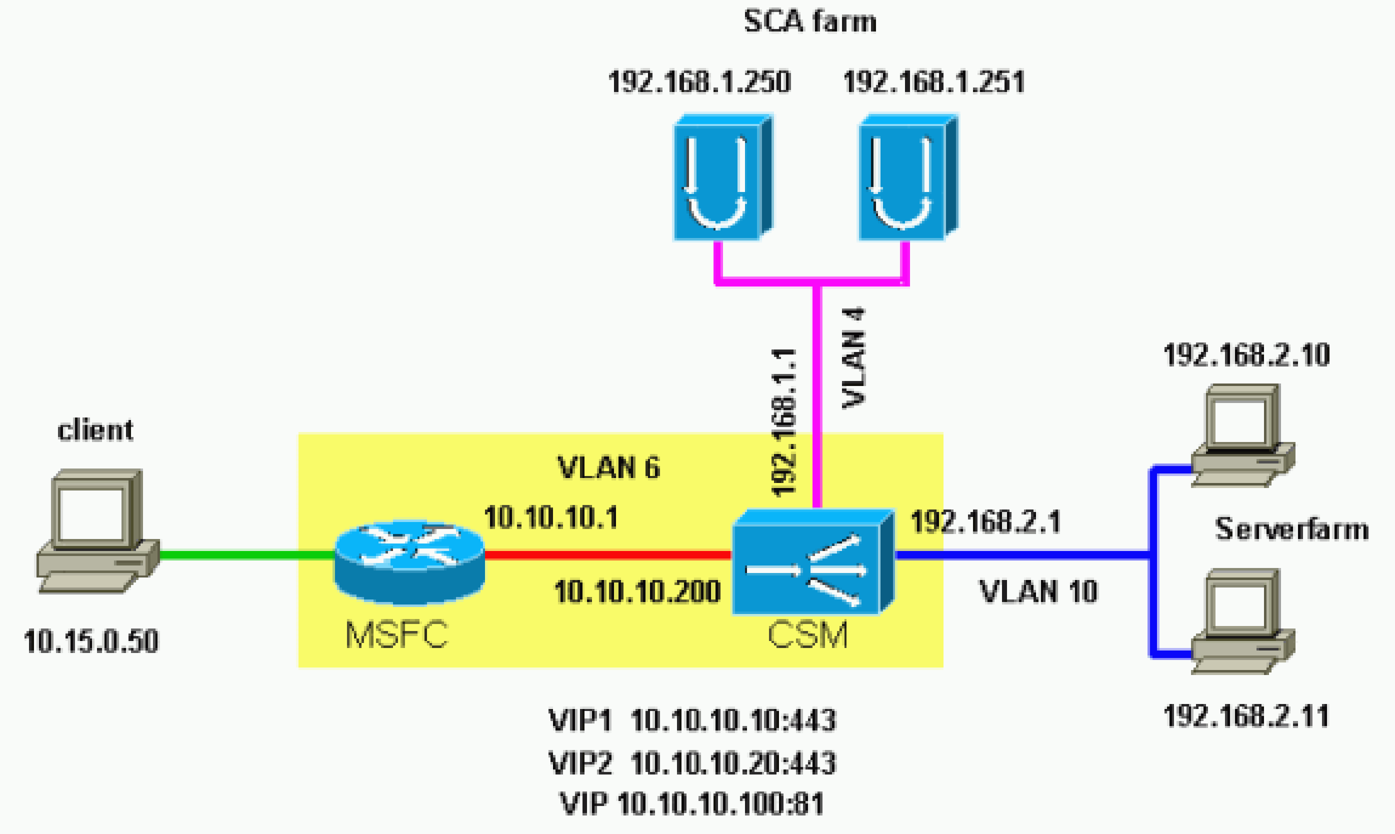
Configure

本部分提供有关如何配置本文档所述功能的信息。

Note: 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

Network Diagram

本文档使用以下网络设置：



配置

本文档使用以下配置：

- Catalyst 6000/CSM Slot 5
- SCA 1
- SCA 2

Catalyst 6000/CSM Slot 5

```
!--- This is the configuration of nontransparent SSL
load balance. Cat6k# show running-config | begin Module
5
module ContentSwitchingModule 5
 vlan 6 client
  ip address 10.10.10.200 255.255.255.0
  gateway 10.10.10.1
!--- This is the CSM IP address on the client side and
!--- CSM upstream gateway (the MSFC). ! vlan 4 server ip
address 192.168.1.1 255.255.255.0 !--- This is the CSM
IP address on the SCA server farm VLAN. !--- SCAs use
this IP address as the default gateway. ! vlan 10 server
ip address 192.168.2.1 255.255.255.0 !--- This is the
CSM IP address on the web server farm VLAN. !--- The web
servers use this IP address as the default gateway. !
static drop real 192.168.2.0 255.255.255.0 !--- This
drops every new connection that the web servers
originate, !--- unless the connection matches a VIP. !
serverfarm SCA443 nat server !--- When connections are
directed to this server farm, !--- the IP address of the
SCA selection replaces !--- the destination IP address.
no nat client real 192.168.1.250 443 inservice real
192.168.1.251 443 inservice !--- The configurations of
both SCAs are such that, !--- with the send of a
connection to this server farm, the destination port !--
- translates to 443. In this example, there is no
translation, as !--- the VIP listens to port 443. !---
This is different in the following server farm, SCA444.
! serverfarm SCA444 nat server no nat client real
192.168.1.250 444 inservice real 192.168.1.251 444
inservice !--- With the selection of this server farm,
there is a !--- modification of connections that go to
either SCA. !--- The destination IP changes to match the
IP of one of the SCAs !--- (NAT server), and the
destination port becomes 444. ! serverfarm WEBFARM nat
server no nat client real 192.168.2.10 80 inservice real
192.168.2.11 80 !--- Specify port 80 to translate from
port 81 inservice. !--- (The SCA communicates on port
81, according to the SCA setup.) !--- This is a standard
web server farm. ! sticky 10 ssl timeout 60 sticky 20
ssl timeout 60 !--- This creates two distinct sticky
groups with SSL ID as a basis. !--- The timeout is 60
seconds. ! vserver TESTSITE1 virtual 10.10.10.10 tcp
https serverfarm SCA443 sticky 60 group 10 persistent
rebalance inservice !--- The vserver for the first site
(www.testsite1.com) listens !--- to 10.10.10.10 on port
443. !--- Connections go to the SCAs without a change in
the !--- destination port. (See the configuration of
server farm SCA443.) ! vserver TESTSITE2 virtual
10.10.10.20 tcp https serverfarm SCA444 sticky 60 group
20 persistent rebalance inservice !--- The vserver for
the second site (www.testsite2.com) listens !--- to
10.10.10.10 on port 443. !--- Connections go to the SCAs
and change the !--- destination port to 444. (See the
configuration of server farm SCA444.) ! vserver WEB-
DECRYPT virtual 10.10.10.100 tcp 81 serverfarm WEBFARM
persistent rebalance inservice ! !--- This is the
vserver for the plain-text connections. !--- This
vserver receives connections on port 81 from the SCAs.
!--- As the configuration of this vserver does not
specify a VLAN, !--- the vserver can also receive
connections directly !--- from the client side. !--- To
prevent direct client access of this VIP, !--- you can
use the VLAN 4 option. !--- You can also place this VIP
```

```
in the SCA subnetwork. In that case, !--- clients do not
even have a route to that subnetwork. (Clients only !---
have a route if you configure the upstream router !---
with a static route.)
```

SCA 1

```
!--- This configures SCA in one-port, nontransparent
mode. sca1# show run
#
# Cisco CSCA Device Configuration File
#
# Written:      Sun Feb  6 01:46:35 2106
# Inxcfg:       version 2.3 build 200108071342
# Device Type:  CSS-SCA
# Device Id:    S/N 119cd6
# Device OS:    MaxOS version 2.5.1 build 200108071341
by Dan L. Reading

### Device ###

mode one-port
ip address 192.168.1.250 netmask 255.255.255.0
hostname sca1
password enable
"2431245A572441713173717748626D734B35516B794F64336A51652
F"
no ip domain-name
no rdate-server
timezone "MST7MDT"
no rip
ip route 0.0.0.0 0.0.0.0 192.168.1.1 metric 1

### Interfaces ###

interface network
  auto
end
interface server
  auto
end

### Remote Management ###

no remote-management access-list
remote-management enable

### SNMP Subsystem ###

no snmp
telnet enable
no telnet access-list
web-mgmt enable
no web-mgmt access-list

### SSL Subsystem ###

ssl
  server test1 create
    ip address 10.10.10.100
    sslport 443
    remoteport 81
    key default
    cert default
    secpolicy default
    cachesize 20
    no transparent
  end
  server test2 create
    ip address 10.10.10.100
    sslport 444
    remoteport 81
    key default
    cert default
    secpolicy default
    cachesize 20
    no transparent
  end
end
sca1#
```

SCA 2

```


!--- This configures SCA in one-port, nontransparent
mode. sca2# sca2# show run
#
# Cisco CSCA Device Configuration File
#
# Written:      Fri Feb 13 21:18:29 1970
# Inxcfg:       version 2.3 build 200108071342
# Device Type:  CSS-SCA
# Device Id:    S/N 119ca2
# Device OS:    MaxOS version 2.5.1 build 200108071341
by Dan L. Reading

### Device ###

mode one-port
ip address 192.168.1.251 netmask 255.255.255.0
hostname sca2
password enable
"2431245A572441713173717748626D734B35516B794F64336A51652
F"
no ip domain-name
no rdate-server
timezone "MST7MDT"
no rip
ip route 0.0.0.0 0.0.0.0 192.168.1.1 metric 1

### Interfaces ###

interface network
  auto
end
interface server
  auto
end

### Remote Management ###

no remote-management access-list
remote-management enable

### SNMP Subsystem ###

```

```
no snmp
telnet enable
no telnet access-list
web-mgmt enable
no web-mgmt access-list

### SSL Subsystem ###

ssl
  server test1 create
    ip address 10.10.10.100
    sslport 443
    remoteport 81
    key default
    cert default
    secpolicy default
    cachesize 20
    no transparent
  end
  server test2 create
    ip address 10.10.10.100
    sslport 444
    remoteport 81
    key default
    cert default
    secpolicy default
    cachesize 20
    no transparent
  end
end
sca2#
```

Verify

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

```
!--- A client opens a connection to www.testsite1.com. Cat6k# show module csm 5 vserver detail
TESTSITE1, state = OPERATIONAL, v_index = 10
  virtual = 10.10.10.10/32:443, TCP, service = NONE, advertise = FALSE
  idle = 3600, replicate csrp = none, vlan = ALL, pending = 0
  max parse len = 600, persist rebalance = TRUE
  conns = 1, total conns = 1
  Default policy:
    server farm = SCA443
    sticky: timer = 60, subnet = 0.0.0.0, group id = 10
  Policy            Tot Conn     Client pkts  Server pkts
  ------------------------------------------------------
  (default)         1            9            11
!--- The client connection to port 443 hits the vserver TESTSITE1 !--- and is load balanced to
an SCA. TESTSITE2, state = OPERATIONAL, v_index = 11 virtual = 10.10.10.20/32:443, TCP, service
= NONE, advertise = FALSE idle = 3600, replicate csrp = none, vlan = ALL, pending = 0 max parse
len = 600, persist rebalance = TRUE conns = 0, total conns = 0 Default policy: server farm =
SCA444 sticky: timer = 60, subnet = 0.0.0.0, group id = 20 Policy Tot Conn Client pkts Server
pkts ------------------------------------------------------ (default) 0 0 0 WEB-DECRYPT, state =
OPERATIONAL, v_index = 13 virtual = 10.10.10.100/32:81, TCP, service = NONE, advertise = FALSE
```

```
idle = 3600, replicate csrp = none, vlan = 4, pending = 0 max parse len = 600, persist rebalance
= TRUE conns = 1, total conns = 1 Default policy: server farm = WEBFARM sticky: timer = 0,
subnet = 0.0.0.0, group id = 0 Policy Tot Conn Client pkts Server pkts ------------------------
----------------------------- (default) 1 7 5 !--- The SCA opens a connection to 10.10.10.100
port 81, !--- which is load balanced to a web server. Cat6k# show module csm 5 conns detail

    prot vlan source                destination           state
----------------------------------------------------------------------
In  TCP  4    192.168.1.250:4376    10.10.10.100:81       ESTAB
Out TCP  10   192.168.2.11:81       192.168.1.250:4376    ESTAB
    vs = WEB-DECRYPT, ftp = No, csrp = False
!--- This provides details of the connection from the SCA to the web server. !--- The connection
comes from VLAN 4 (the SCA VLAN), destined to !--- 10.10.10.100 port 81. !--- This is different
from what happens in transparent mode. !--- In this case, the SCA opens the connections with use
of !--- the SCA IP address, 192.168.1.250. The server does not see the IP !--- of the original
client. !--- The connection goes to VLAN 10 (web servers VLAN) !--- to the web server selection.
(The destination IP address !--- changes accordingly. The port does not change.) !--- If the
servers listen to port 80 instead of port 81, you can configure !--- the translation of the
destination port. You can add a port !--- to the definition of the real servers. !--- NOTE: The
Out line swaps source with destination. !--- "Out" refers to the return traffic packets that the
CSM !--- receives from that VLAN.

In  TCP  6    10.15.0.50:2324       10.10.10.10:443       ESTAB
Out TCP  4    192.168.1.250:443     10.15.0.50:2324       ESTAB
    vs = TESTSITE1, ftp = No, csrp = False
 !--- This provides details of the connection from the client to the VIP. !--- The connection
comes from VLAN 6 (the client VLAN), destined to !--- 10.10.10.10 port 443. !--- The connection
goes to VLAN 4 (the SCA VLAN) !--- to the SCA selection. The destination IP changes !--- from
the 10.10.10.10 (the VIP) to 192.168.1.250 (the SCA), !--- as the server farm had the option NAT
server. !--- This is different in nontransparent mode. !--- The same client opens a second
connection, !--- this time to www.testsite2.com. Cat6k# Cat6k# show module csm 5 conns detail

    prot vlan source                destination           state
----------------------------------------------------------------------
In  TCP  4    192.168.1.250:4377    10.10.10.100:81       ESTAB
Out TCP  10   192.168.2.10:81       192.168.1.250:4377    ESTAB
    vs = WEB-DECRYPT, ftp = No, csrp = False
!--- This connection is from SCA to VIP .100, load balanced to !--- web server .10. In TCP 4
192.168.1.250:4376 10.10.10.100:81 ESTAB Out TCP 10 192.168.2.11:81 192.168.1.250:4376 ESTAB vs
= WEB-DECRYPT, ftp = No, csrp = False !--- This connection is from SCA to VIP .100, load
balanced to !--- webserver .11. In TCP 6 10.15.0.50:2325 10.10.10.20:443 ESTAB Out TCP 4
192.168.1.250:444 10.15.0.50:2325 ESTAB vs = TESTSITE2, ftp = No, csrp = False !--- This
connection is from client to VIP .20, load balanced to !--- SCA .250, port 444. In TCP 6
10.15.0.50:2324 10.10.10.10:443 ESTAB Out TCP 4 192.168.1.250:443 10.15.0.50:2324 ESTAB vs =
TESTSITE1, ftp = No, csrp = False !--- This connection is from client to VIP .10, load balanced
to !--- SCA .250, port 443. Cat6k#show module csm 5 real detail
192.168.2.10, WEBFARM, state = OPERATIONAL
  conns = 1, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 1
  total conns established = 1, total conn failures = 0
192.168.2.11, WEBFARM, state = OPERATIONAL
  conns = 1, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 1
  total conns established = 1, total conn failures = 0
192.168.1.250:443, SCA443, state = OPERATIONAL
  conns = 1, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 1
  total conns established = 1, total conn failures = 0
192.168.1.251:443, SCA443, state = OPERATIONAL
  conns = 0, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  total conns established = 0, total conn failures = 0
192.168.1.250:444, SCA444, state = OPERATIONAL
  conns = 1, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 1
  total conns established = 1, total conn failures = 0
192.168.1.251:444, SCA444, state = OPERATIONAL
  conns = 0, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  total conns established = 0, total conn failures = 0
!--- This output shows that each web server has received a !--- connection. !--- The SCA .250
has received two connections, one to port 443 and !--- one to port 444. !--- The SCA .251 has
not yet received any connection because !--- only two connections are open. One is open to each
site !--- (10.10.10.10 and 10.10.10.20). A different port (443 or 444) !--- on the SCAs handles
each site. The first !--- connection for each site goes to the first SCAs. !--- The following
connection to either .10 or .20 goes to !--- .251, port 443 or 444, respectively. !--- This is
SCA1 output. !--- There is one open connection. sca1# show netstat
Pro State Recv-Q Send-Q Local Address         Remote Address
R-Win S-Win
---------------------------------------------------------------------------
tcp ESTAB      0      0 192.168.1.250:443     10.15.0.50:2324
33580 16529
tcp ESTAB      0      0 192.168.1.250:4376    10.10.10.100:81
33304 17232
udp            0      0 *:4099                *:*
0     0
udp            0      0 *:4098                *:*
0     0
tcp LISTN      0      0 *:2932                *:*
0     0
udp            0      0 *:2932                *:*
0     0
udp            0      0 *:520                 *:*
0     0
udp            0      0 *:514                 *:*
0     0
tcp LISTN      0      0 *:444                 *:*
0     0
tcp LISTN      0      0 *:443                 *:*
32768     0
tcp LISTN      0      0 *:80                  *:*
0     0
tcp LISTN      0      0 *:23                  *:*
0     0
sca1#
!--- There are two open connections. sca1# show netstat
Pro State Recv-Q Send-Q Local Address         Remote Address
R-Win S-Win
---------------------------------------------------------------------------
tcp ESTAB      0      0 192.168.1.250:444     10.15.0.50:2325
33580 16529
tcp ESTAB      0      0 192.168.1.250:443     10.15.0.50:2324
33580 16529
tcp ESTAB      0      0 192.168.1.250:4377    10.10.10.100:81
33304 17232
tcp ESTAB      0      0 192.168.1.250:4376    10.10.10.100:81
33304 17232
udp            0      0 *:4099                *:*
0     0
udp            0      0 *:4098                *:*
0     0
tcp LISTN      0      0 *:2932                *:*
0     0
udp            0      0 *:2932                *:*
0     0
udp            0      0 *:520                 *:*
0     0
udp            0      0 *:514                 *:*
```

```
0     0
tcp LISTN      0      0 *:444                *:*
32768     0
tcp LISTN      0      0 *:443                *:*
32768     0
tcp LISTN      0      0 *:80                 *:*
0     0
tcp LISTN      0      0 *:23                 *:*
0     0
sca1#
```

Troubleshoot

目前没有针对此配置的故障排除信息。