目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[相关产品](#)
[规则](#)
[配置](#)
[网络图](#)
[配置](#)
[验证与故障排除](#)
[验证和故障排除命令示例](#)
[TAC服务请求数据](#)
[相关信息](#)

简介

内容服务交换机(CSS) 11500支持内部安全套接字层SSL加速度模块，可以用于解密更加好的负载均衡决策的(前端的SSL/SSL终端)客户端的流量。使用卸载的CSS从服务器的SSL极大增加服务器性能并且允许流量后端处理应用程序的更加好分布式。CSS11500能再加密SSL终止的连接和发送加密流量到后端SSL服务器(后端SSL)。这为要求安全客户端的环境是必要的对服务器通信和高级服务器负载均衡，例如用Cookie维护会话持续性。集成SSL功能允许CSS做出内容识别的决策保证数据发送对正确应用程序，当维护在网络中时的数据加密。

本文描述从客户端的SSL流量到CSS和到后端SSL服务器。本文提供配置和不同的实施方案。

先决条件

要求

在尝试此配置前，请保证您符合这些要求：

- 基本概念安全套接层/传输层安全(SSL/TLS)
- CSS的基本设置
- 对Web服务器密钥和证书的访问从存在SSL Web服务器
- 授权更改在您的服务器的SSL配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- WebNS版本7.20构建206
- CSS11506
- 在站点证书的Verisign

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也可用于以下硬件和软件版本：

- 与内藏的SSL的CSS 11501或CSS 11503/506用安装的CSS5-SSL-K9 SSL模块。
- WebNS软件版本7.20和以上。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

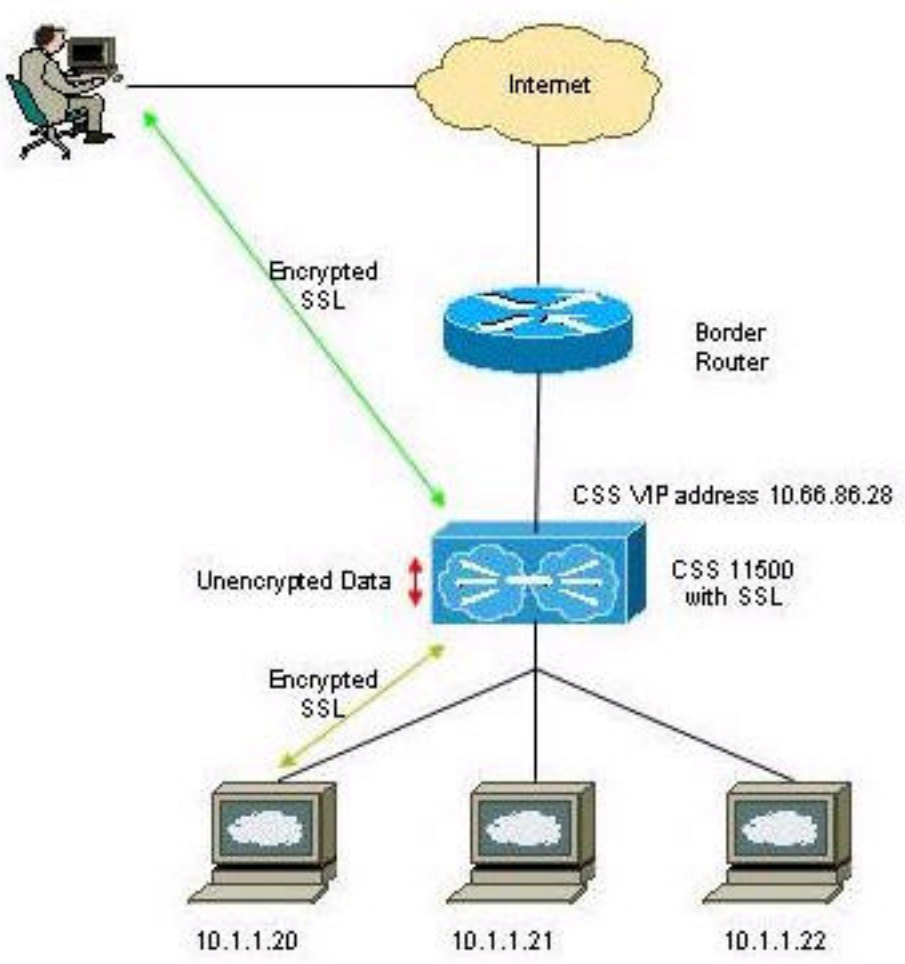
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 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）。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- CSS11506 (NWS-5-9)

从客户端的流量来并且点击内容前面规则。此规则是端口443。此规则然后装载平衡流量对服务ssl_front。此服务然后参考SSL代理列表。

SSL代理列表定义了与客户端的SSL协商并且建立在CSS和客户端之间的一个安全SSL会话。配置定义了SSL代理IP地址、专用密钥和被串连的/单个证书使用。它也定义了明文内容规则您点击。

是指的内容规则是内容上一步。由于这样的事实此数据当前在明文，您能看到HTTP包头。为了维护stickyness到服务器，请使用ArrowPoint Cookie。CSS然后做出根据ArrowPoint Cookie的一个负载均衡决策，如果客户端通过基础负载均衡算法已经接收一或，如果他们没有。在这种情况下，交换机是被均衡的负载服务backend1。

请求然后发送服务backend1。此服务配置作为类型ssl-accel-backend。没有物理服务器在这里。

SSL代理列表再是指，并且从配置，您能看到服务器配置。此配置非常类似于SSL解密在前端，但是在反向。您能采取明文和转换它到SSL。您在客户端Hello能也定义密码器使用。

请求是发送对加密的物理服务器。

CSS11506 (NWS-5-9)

```
nws-5-2# sh run !Generated on 01/09/2004 01:16:00 !Active
version: sg0720206 configure !**************************
GLOBAL **************************   cdp run  ssl associate
rsakey privatekey myprivatekey  ssl associate cert
certificate mynewcert.pem !--- Define the SSL certificate and
key files to use for the Web site !--- These are for the
client to SSL module connection. ip route 0.0.0.0 0.0.0.0
10.66.86.17 1 !************************* INTERFACE
************************ interface 3/1 bridge vlan 41
!************************* CIRCUIT
************************** circuit VLAN1 ip address 10.1.1.1
255.255.255.0 circuit VLAN41 ip address 10.66.86.29
255.255.255.240 !********************** SSL PROXY LIST
********************** ssl-proxy-list my_secure_site ssl-
server 1 ssl-server 1 rsakey privatekey ssl-server 1 rsacert
certificate ssl-server 1 cipher rsa-with-rc4-128-md5
10.1.1.10 81 ssl-server 1 vip address 10.66.86.28 !--- SSL
server configuration. This is for the client to the SSL !---
module connection. backend-server 10 !--- Backend SSL
configuration. These specify the parameters for !--- the
connection from the CSS to the backend servers. backend-
server 10 ip address 10.1.1.20 backend-server 10 port 81 !---
This defines the clear text IP and port that are !--- used to
encrypt data headed for the backend servers. backend-server
10 server-ip 10.1.1.20 backend-server 10 server-port 8003 !--
- This is the physical server. As there is no server-port !--
- configured, the default 443 will be used. backend-server 10
cipher rsa-export-with-rc4-40-md5 !--- The CSS behaves as a
client. Specify what SSL cipher !--- you are going to present
to the backend server in the SSL !--- handshake client hello
packet. backend-server 20 backend-server 20 ip address
10.1.1.21 backend-server 20 port 81 backend-server 20 server-
ip 10.1.1.21 backend-server 20 server-port 8003 backend-
server 20 cipher rsa-export-with-rc4-40-md5 backend-server 30
backend-server 30 ip address 10.1.1.22 backend-server 30 port
81 backend-server 30 server-ip 10.1.1.22 backend-server 30
```

```
server-port 8003 backend-server 30 cipher rsa-export-with-
rc4-40-md5 active !************************* SERVICE
************************* service ssl_front slot 6 type ssl-
accel keepalive type none add ssl-proxy-list my_secure_site
active service backend1 ip address 10.1.1.20 type ssl-accel-
backend port 81 add ssl-proxy-list my_secure_site keepalive
port 8003 keepalive type ssl protocol tcp active service
backend2 ip address 10.1.1.21 type ssl-accel-backend port 81
keepalive port 8003 add ssl-proxy-list my_secure_site
keepalive type ssl protocol tcp active service backend3 ip
address 10.1.1.22 protocol tcp port 81 keepalive port 8003
keepalive type ssl type ssl-accel-backend add ssl-proxy-list
my_secure_site active !************************** OWNER
************************** owner my_secure_site content back
protocol tcp port 81 url "/*" vip address 10.1.1.10 add
service backend1 add service backend2 add service backend3
advanced-balance arrowpoint-cookie active content front
protocol tcp vip address 10.66.86.28 application ssl add
service ssl_front port 443 active
```

验证与故障排除

本部分提供的信息可用于对配置进行故障排除。左列是会话的生命周期的列表。右侧列是能使用检查生命周期的每部分状态**显示**命令和工具的列表。

逻辑生命周期	**命令/技术(下面示例)**
客户端	从客户端机器的嗅探器跟踪。寻找TCP 3方式握手和SSL客户端Hello和服务器问候。
内容规则前面	**show rule** ？寻找规则作为活动。设法ping规则的VIP地址;这应该响应。采取在连接的链路的嗅探器跟踪对在客户端的CSS。
服务ssl_front	**show service summary** ？确保服务运行。**show service ssl_front** ？确保服务运行，并且SSL代理my_secure_site是列出和活跃的。确认总本地连接是否增加。
SSL代理列表my_secure_site	**显示ssl代理列表**？确保状态是。**显示ssl代理列表my_secure_site** ？提供配置信息。**show ssl statistics** ？确保那里是没有错误增加。参见下面示例。**show ssl flows** ？显示当前流。
内容规则上一步	**show rule** ？寻找规则作为**活动**。
服务backend1或backend2或者backend3	**show service summary** ？确保服务运行。**show service**服务名称？确保至少一服务运行，并且SSL代理my_secure_site是列出和活跃的。确认总计本地连接是否增加。
SSL代理列表my_secure_site	**显示ssl代理列表**？确保状态是。**显示ssl代理列表my_secure_site** ？提供配置信息。**show ssl statistics** ？确保那里是没

	有错误增加。参见下面示例。**show ssl flows** ？显示当前流。
服务器	从客户端机器的嗅探器跟踪。寻找TCP 3方式握手和SSL客户端Hello和服务器问候。检查服务器是否在SSL侦听。发出**port netstat -a命令**Windows的和**netstat -l命令**Unix/Linux机器的。

验证和故障排除命令示例

此部分提供故障排除信息与在上述生命周期列出的命令有关，并且寻找什么在每命令。应该检查**粗体部分**他们是否显示一不同的状态。

show rule

```
Name:                    back    Owner:          my_secure_siteState:     Active    Type:
HTTPBalance:          Round Robin    Failover:                  N/APersistence:          Enabled    Param-
Bypass:         DisabledSession Redundancy:  DisabledIP Redundancy:    Not RedundantL3:          10.1.1.10
!--- Theses lines indicate the configuration of the rule.L4:          TCP/81Url:         /*          !---
This indicates a Layer 7 rule, where the CSS spoofs the !--- connection.Redirect: ""TCP RST client if
service unreachable: DisabledRule Services: 1: backend1-Alive >>>>>>>>Name: front Owner:
my_secure_siteState:                  Active    Type:       SSLBalance:          Round Robin    Failover:
N/APersistence:          Enabled    Param-Bypass:         DisabledSession Redundancy:  DisabledIP
Redundancy:    Not RedundantL3:          10.66.86.28  !--- Theses lines indicate the configuration of the
rule.L4:          TCP/443Url:                              !--- There is no configuration, so this is a
Layer 4 rule.Redirect: ""TCP RST client if service unreachable: DisabledRule Services: 1: ssl_front-Alive
```

show service summary

```
Service Name                      State     Conn  Weight  Avg    State
Load  Transitionsbackend1                          Alive          0      1     2            9backend2
Down          0      1   255            0backend3                          Down          0      1   255
0ssl_front                         Alive          0      1     2            4
```

噓服务ssl_front

```
Name: ssl_front          Index: 4       Type: Ssl-Accel         State: Alive  Rule ( 0.0.0.0  ANY  ANY )
Session Redundancy: Disabled  SSL-Accel slot: 6    !--- Make sure this is the slot where the SSL module
is installed. Session Cache Size: 10000 Redirect Domain: Redirect String: Keepalive: (NONE 5 3 5 ) Last
Clearing of Stats Counters: 01/28/2004 22:29:34 Mtu: 1500 State Transitions: 4 !--- Connection counters
should be increasing. Total Local Connections:   576          Total Backup Connections:     0  Current
Local Connections: 0           Current Backup Connections:   0  Total Connections:          576
Max Connections:              65534  Total Reused Conns:        0           Weight:                    1
Load:                         2  DFP:                        Disable       SSL Proxy Lists:   1:
my_secure_site-Active
```

显示ssl代理列表

```
Ssl-Proxy-List Table Entries (1 Entries)    1) Name:  my_secure_site       State:  Active       !--- The
number of services pointing to the SSL proxy list. This !--- includes the back-end services as well.
Services Associated:  4
```

显示ssl代理列表my_secure_site

```
- Ssl-proxy-list Entries for list my_secure_site -Number of SSL-Servers:  1    Ssl-Server 1 -
Vip address: 10.66.86.28     Vip port:  443     RSA Certificate:  certificate       !--- This is the
certificate file associated for the SSL site. RSA Keypair:      privatekey        !--- This is the
private key file associated for the SSL site. DSA Certificate: none DSA Keypair: none DH Param: none
Session Cache Timeout: 300 SSL Version: SSL and TLS Re-handshake Timeout: 0 Re-handshake Data: 0 Virtual
TCP Inactivity TO: 240 Server TCP Inactivity TO: 240 Virtual TCP Syn Timeout: 30 Server TCP Syn Timeout:
30 Virtual TCP Nagle Algorithm: enable Server TCP Nagle Algorithm: enable TCP Receive Buffer: 32768 TCP
```

Transmit Buffer: 65536 SSL Shutdown Procedure: normal Cipher Suite(s) Weight Port Server ---------- ------ ---- ------ **rsa-with-rc4-128-md5 1 81 10.1.1.10** *!--- This is the cipher suite used in the server SSL hello back to the client. !--- The clear text IP address and port of the decypted traffic.* URL Rewrite Rule(s) - None Number of Ssl Proxy backend-servers: 3 Backend-server 10 - *!--- This is the back-end server clear text IP and port.* **IP address: 10.1.1.20 Port: 81** *!--- This is the back-end server SSL server IP and port.* **Server IP address: 10.1.1.20 Server port: 8003** Session Cache Timeout: 300 SSL Version: SSL and TLS Re-handshake Timeout: 0 Re-handshake Data: 0 Virtual TCP Inactivity TO: 240 Server TCP Inactivity TO: 240 Virtual TCP Syn Timeout: 30 Server TCP Syn Timeout: 30 Virtual TCP Nagle Algorithm: enable Server TCP Nagle Algorithm: enable TCP Receive Buffer: 32768 TCP Transmit Buffer: 65536 Cipher Suite(s) Weight ---------- ------ **rsa-export-with-rc4-40-md5 1** *!--- This is the cipher suite used in the client hello to the SSL server. !--- In this case, the SSL module is encypting the traffic and acting as !--- a client.* Backend-server 20 - IP address: 10.1.1.21 Port: 81 Server IP address: 10.1.1.21 Server port: 8003 Session Cache Timeout: 300 SSL Version: SSL and TLS Re-handshake Timeout: 0 Re-handshake Data: 0 Virtual TCP Inactivity TO: 240 Server TCP Inactivity TO: 240 Virtual TCP Syn Timeout: 30 Server TCP Syn Timeout: 30 Virtual TCP Nagle Algorithm: enable Server TCP Nagle Algorithm: enable TCP Receive Buffer: 32768 TCP Transmit Buffer: 65536 Cipher Suite(s) Weight ---------- ------ rsa-export-with-rc4-40-md5 1 Backend-server 30 - IP address: 10.1.1.22 Port: 81 Server IP address: 10.1.1.22 Server port: 8003 Session Cache Timeout: 300 SSL Version: SSL and TLS Re-handshake Timeout: 0 Re-handshake Data: 0 Virtual TCP Inactivity TO: 240 Server TCP Inactivity TO: 240 Virtual TCP Syn Timeout: 30 Server TCP Syn Timeout: 30 Virtual TCP Nagle Algorithm: enable Server TCP Nagle Algorithm: enable TCP Receive Buffer: 32768 TCP Transmit Buffer: 65536 Cipher Suite(s) Weight ---------- ------ rsa-export-with-rc4-40-md5 1

show ssl statistics

SSL Acceleration StatisticsComponent: SSL Proxy Server Slot: 6 Count Description---------- --- ---------- **576 Handshake started for incoming SSL connections 576 Handshake completed for incoming SSL connections***!--- These are the SSL handshake statistics for the client to CSS connection.* **560 Handshake started for outgoing SSL connections 560 Handshake completed for outgoing SSL connections***!--- These are the SSL handshake stats for the CSS to backend servers.* **12 Active SSL flows high water mark***!--- This is the maximum number of active SSL flows.*SSL Acceleration StatisticsComponent: Crypto Slot: 6 Count Description---------- -- --------- 14 RSA Private 3 RSA Public 0 DH Shared 0 DH Public 0 DSA Sign 0 DSA Verify 0 SSL MAC 7,515 TLS HMAC 0 3DES 7,918 ARC4 69,876 HASH **0 RSA Private Failed 0 RSA Public Failed 0 DH Shared Failed 0 DH Public Failed 0 DSA Sign Failed 0 DSA Verify Failed 0 SSL MAC Failed 0 TLS HMAC Failed 0 3DES Failed 0 ARC4 Failed 0 HASH Failed 0 Hardware Device Not Found 0 Hardware Device Timed Out 0 Invalid Crypto Parameter 0 Hardware Device Failed 0 Hardware Device Busy 0 Out Of Resources 0 Cancelled -- Device Reset***!--- At this point, any errors need to be investigated.*SSL Acceleration StatisticsComponent: SSL Slot: 6 Count Description---------- ---------- -- 14 RSA Private Decrypt calls 3 RSA Public Decrypt calls 0 DH Compute key calls 0 DH Generate key calls 0 DSA Verify calls 0 DSA Sign calls 34,220 MD5 raw hash calls 34,220 SHA1 raw hash calls 0 3-DES calls 7,918 RC4 calls 0 SSL MAC(MD5) calls 0 SSL MAC(SHA1) calls 7,515 TLS MAC(MD5) calls 0 TLS MAC(SHA1) calls 0 Level 2 Alerts Received 725 Level 1 Alerts Received 0 Level 2 Alerts Sent 1,134 Level 1 Alerts Sent **1,200,211 SSL received bytes from TCP 1,155,278 SSL transmitted bytes to TCP 1,006,669 SSL received Application Data bytes 1,970,856 SSL transmitted Application Data bytes 124,497 SSL received non-application data bytes 152,147 SSL transmitted non-application data bytes** *!--- These are the traffic stats for the SSL module; they should be incrementing.* 0 RSA Private Decrypt failures 0 MAC failures for packets received 0 Re-handshake TimerAlloc failed 0 Blocks SSL could not allocate 0 Dup Blocks SSL could not allocate 0 Too many blocks for Block2AccelFragmentArray 0 Too many blocks in a SSL message

show ssl flows

SSL Acceleration Flows for slot 6 Virtual Port TCP Proxy Flows Active SSL Flows SSL Flows in Handshake---------- ---- ---------- ---------- ---------- **10.66.86.28 443 6 2 0 10.1.1.20 81 6 2 0** 10.1.1.22 81 0 0 0 10.1.1.21 81 0 0 0*!--- This is the number of active flows in the CSS. These can be difficult to see on a !--- box with little load.*

show service backend1

```
Name: backend1          Index: 1         Type: Ssl-Accel-Backend State: Alive  Rule ( 10.1.1.20  TCP  81
)  Session Redundancy: Disabled  Redirect Domain:    Redirect String:    Keepalive: (SSL-8003   5   3   5
)  Last Clearing of Stats Counters: 01/28/2004 22:29:34  Mtu:                        1500        State
Transitions:            9  Total Local Connections:   689         Total Backup Connections:     0
Current Local Connections: 0           Current Backup Connections:   0  Total Connections:         689
Max Connections:              65534  Total Reused Conns:        0           Weight:                    1
Load:                         2  DFP:                       Disable       SSL Proxy Lists:   1:
my_secure_site-Active
```

TAC服务请求数据

在打开技术支持中心(TAC)服务请求前，请收集此信息：

1. 使用以上的生命周期，请搜集被提及的所有命令并且每个生命周期步骤分组他们。
2. 提供**script play showtech命令**输出。
3. 提供一幅详细的拓扑图。
4. 提供从CSS和服务器端的客户端的嗅探器跟踪。这可选，但是可能缩短解决时间。
5. 如果提供嗅探器跟踪，请识别客户端IP地址。

相关信息

- Cisco WebNS CSS11500 软件下载页(注册用户)
- Cisco WebNS CSS 11000 Software Download页(仅限注册用户)
- 技术支持和文档 - Cisco Systems