This article describes how to troubleshoot WAAS Express operation.

Guide Contents
Main Article
Understanding the WAAS Architecture and Traffic Flow
Preliminary WAAS Troubleshooting
Troubleshooting Optimization
Troubleshooting Application Acceleration
Troubleshooting the CIFS AO
Troubleshooting the HTTP AO
Troubleshooting the EPM AO
Troubleshooting the MAPI AO
Troubleshooting the NFS AO
Troubleshooting the SSL AO
Troubleshooting the Video AO
Troubleshooting the Generic AO
Troubleshooting Overload Conditions
Troubleshooting WCCP
Troubleshooting AppNav
Troubleshooting Disk and Hardware Problems
Troubleshooting Serial Inline Clusters
Troubleshooting vWAAS
Troubleshooting WAAS Express
Troubleshooting NAM Integration

Contents

WAAS Express is WAAS functionality built into IOS running on a device such as a router. The WAAS Central Manager can manage a WAAS Express device along with other WAAS devices in the WAAS network. This article describes how to troubleshoot WAAS Express device operation.

Note: WAAS Express Central Manager support was introduced in WAAS version 4.3.1. This section is not applicable to earlier WAAS versions.

Verifying WAAS Express Image Version

To verify the WAAS Express image version use the **show waas status** command on the WAAS Express router. To view the WAAS Express image version from the WAAS Central Manager, choose **My WAN > Manage Devices**.

```
waas-express# show waas status
```

```
IOS Version: 15.1(20101018:232707)       <----- IOS version
WAAS Express Version: 1.1.0              <----- WAAS Express version
. . .
```

Verifying WAAS Express License

The WAAS Express license comes in two varieties: evaluation license (valid for 12 years) and permanent license. Use the **show waas status** command on the WAAS Express device to display the license information.

```
waas-express# show waas status

IOS Version: 15.1(20101018:232707)
WAAS Express Version: 1.1.0
. . .

WAAS Feature License
License Type:                          Evaluation          <----- Indicates an evaluation license
Evaluation total period:               625 weeks 0  day
Evaluation period left:                622 weeks 6  days
```

Verifying WAAS Enabled Interfaces

Use the **show waas status** command on the WAAS Express device to list the set of interfaces on which WAAS is enabled. This command also displays the kind of optimization supported by the device. Some of the WAAS Express router models do not support DRE.

```
waas-express# show waas status

IOS Version: 15.1(20101018:232707)
WAAS Express Version: 1.1.0
WAAS Enabled Interface        Policy Map
GigabitEthernet0/1            waas_global        <----- Interfaces on which optimization is enable
GigabitEthernet0/2            waas_global
Virtual-TokenRing1            waas_global
Virtual-TokenRing2            waas_global
GigabitEthernet0/0            waas_global
Virtual-TokenRing10           waas_global
WAAS Feature License
License Type:                          Evaluation
Evaluation total period:               625 weeks 0  day
Evaluation period left:                622 weeks 6  days
DRE Status                        : Enabled                    <----- Indicates DRE is supported
LZ Status                         : Enabled + Entropy
Maximum Flows                     : 50                         <----- Number of optimized connecti
Total Active connections          : 0                          <----- Total number of connections
Total optimized connections       : 0                          <----- Total number of optimized co
```

Note: WAAS should be enabled on WAN interfaces only. If connections, to be optimized, are routed over multiple WAN interfaces, then, WAAS should be applied on all those WAN interfaces.

Note: If WAAS is enabled on a logical or virtual interface it need not be implemented on the corresponding physical interface.

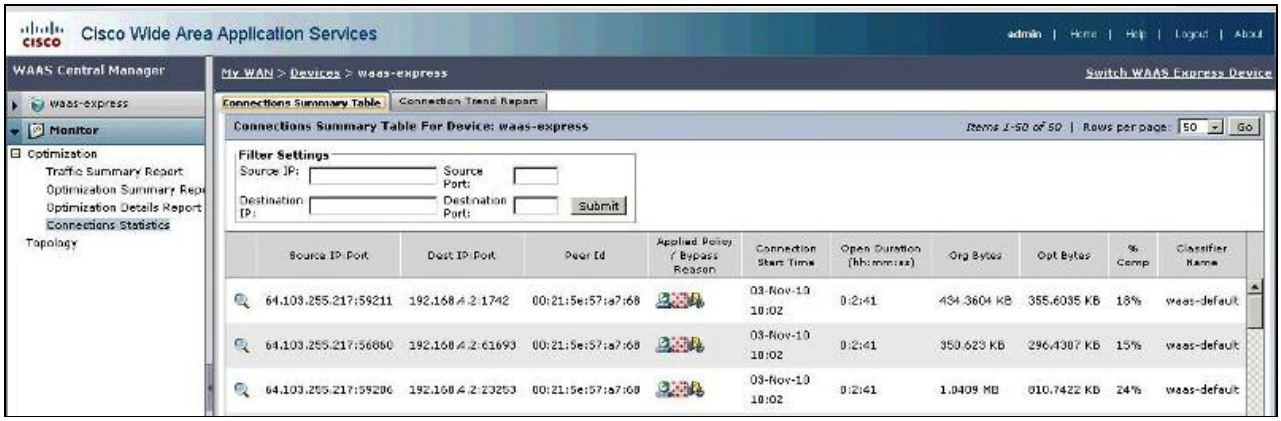
Verifying WAAS Optimized Connections

On the WAAS Express device, use the **show waas connection** command to list the set of optimized connections. Pass-through connections are not included.

```
waas-express#  show waas  status
ConnID      Source IP:Port          Dest IP:Port           PeerID             Accel
1999        64.103.255.217 :59211   192.168.4.2    :1742   0021.5e57.a768     TLD      <----- TFO, LZ
1910        64.103.255.217 :56860   192.168.4.2    :61693  0021.5e57.a768     TLD
1865        64.103.255.217 :59206   192.168.4.2    :23253  0021.5e57.a768     TLD
```

To view similar information from the Central Manager, choose the WAAS Express device, then choose **Monitor > Optimization > Connections Statistics** to see the Connections Summary Table.

Figure 1. Connections Summary Table



Verifying WAAS Optimized Data

On the WAAS Express device, use the **show waas statistics application** command to list the optimized data classified into each application. The WAAS Express device does not show pass-through data. This data is used to generate the TCP related charts in the WAAS Central Manager.

```
waas-express# show waas statistics application

Number of applications :        1
Application:     waas-default
TCP Data Volumes
Connection Type     Inbound                          Outbound
Opt TCP Plus        53001765483                      41674120
Orig TCP Plus       0                                87948683030
Opt TCP Only        1165                               863
Orig TCP Only       60                                   0
Internal Client     0                                    0
Internal Server     0                                    0

TCP Connection Counts
Connection Type     Active               Completed
Opt TCP Plus        50                       126
Opt TCP Only        0                         71
Internal Client     0                          0
Internal Server     0                          0

Pass Through Connection Counts
Connection Type     Completed
```

```
PT Asymmetric       0
PT Capabilities     0
PT Intermediate     0
PT_Other            0
Connection Reset:   0
Cleared connections 0
```

Verifying WAAS Express Alarms

On the WAAS Express device, use the **show waas alarms** command to list the alarms that are present in the device and their status.

```
waas-express# show waas alarms
WAAS status:        enabled
Alarms
Connection limit exceeded:              on      <----- on indicates this alarm is active. off indi
Too many peers discovered:              off
WAAS license expired:                   off
WAAS license revoked:                   off
WAAS license deleted:                   off
High CPU:                               off
```

To view alarms for all devices from the Central Manager, choose **My WAN > Alerts**. In addition to the alarms listed above, an alarm is raised if the clocks of the WAAS Express and WAAS Central Manager devices are not synchronized.

Verifying WAAS Express Peers

On the WAAS Express device, use the **show waas statistics peer** command to list the peer devices of the WAAS Express device.

```
waas-express# show waas statistics peer
Number of Peers :   1
Peer:               0021.5e57.a768
TCP Data Volumes
Connection Type     Inbound                             Outbound
Opt TCP Plus        597068158                            5212151
Orig TCP Plus       0                                   6867128187
Opt TCP Only        0                                          0
Orig TCP Only       0                                          0
Internal Client     0                                          0
Internal Server     0                                          0

TCP Connection Counts
Connection Type     Active              Completed
Opt TCP Plus        50                         0
Opt TCP Only        0                          0
Internal Client     0                          0
Internal Server     0                          0

Pass Through Connection Counts
Connection Type     Completed
PT Asymmetric       0
PT Capabilities     0
PT Intermediate     0
PT_Other            0
Connection Reset:   0
Cleared connections 0

Router#show waas statistics aoim
```

```
Total number of peer syncs:                     1
Current number of peer syncs in progress:       0
Number of peers:                                1
Number of local application optimizations (AO): 3
Number of AO discovery successful:              1
Number of AO discovery failure:                 0

Local AO statistics
    Local AO:                                   TFO
        Total number of incompatible connections: 0
        Version:                                0.11
        Registered:                             Yes
    Local AO:                                   HTTP
        Total number of incompatible connections: 0
        Version:                                1.1
        Registered:                             Yes
    Local AO:                                   SSL
        Total number of incompatible connections: 0
        Version:                                1.0
        Registered:                             Yes

Peer AOIM Statistics
Number of Peers :   1
    Peer:                           0027.0d79.c215    <--- Peer ID
    Peer IP:                        20.0.0.2          <--- Peer IP
    Peer Expiry Time:               00:00:02
    Peer Compatible:                Yes
    Peer active connections:        0
    Peer Aoim Version:              1.0
    Peer sync in progress:          No
    Peer valid:                     Yes
    Peer Software Version:          4.4.3(b4)
    Peer AOs:
        Peer AO:                        TFO
            Compatible:                 Yes
            Version:                    0.20
        Peer AO:                        HTTP
            Compatible:                 Yes
            Version:                    1.4
        Peer AO:                        SSL
            Compatible:                 Yes
            Version:                    1.0

Router#show waas statistics dre peer
DRE Status:                             Enabled

Current number of connected peers       0
Current number of active peers          1

Peer-ID                                 0027.0d79.c215          <--- Peer ID
Hostname                                waasx1-b-wae.cisco.com  <--- Peer hostname
IP reported from peer                   20.0.0.2                <--- Peer IP
Peer version                            4.4.3(b4)

Cache:
    Cache in storage                    0 B
    Age                                 00:00:00

AckQ:
    AckQ in storage                     0 B

WaitQ:
    WaitQ in storage                    0 B
    WaitQ size                          0 B
```

```
Sync-clock:
    Local-head                          0 ms
    Local-tail                          0 ms
    Remote-head                         18609143000 ms
    Curr-sync-clock                     24215235228 ms

Encode Statistics
    DRE msgs:                           1
    R-tx total:                         0
    R-tx chunk-miss:                    0
    R-tx collision:                     0
    Bytes in:                           0
    Bytes out:                          0
    Bypass bytes:                       178
    Compression gain:                   0%
Decode Statistics
    DRE msgs:                           4
    Bytes in:                           299
    Bytes out:                          277
    Bypass bytes:                       51
    Compression gain:                   0%
    Nacks generated:                    0
```

To view similar information from the Central Manager, choose **Monitor > Topology**.

Offline Alarms

The WAAS Express device may go to an offline state in the Central Manager because of the following issues:

- **Central Manager does not have WAAS Express device credentials.**

  Credentials are not configured for this WAAS Express device in the Central Manager. The WAAS Central Manager needs the WAAS Express username and password to communicate with the WAAS Express device. You can configure credentials in the Central Manager by choosing **My WAN** (or a WAAS Express device or device group) **> Admin > WAAS Express Credentials**.

- **Authentication failed while communicating with WAAS Express device.**

  The Central Manager is not able to communicate with the WAAS Express because wrong credentials are configured. You can configure credentials in the Central Manager by choosing **My WAN** (or a WAAS Express device or device group) **> Admin > WAAS Express Credentials**.

- **SSL Handshake failed while communicating with WAAS Express devcie.**

  The WAAS Express device certificate is changed and the same certificate is not imported for this device in the Central Manager. To reimport the WAAS Express device certificate, choose the WAAS Express device, then choose **Admin > Certificate**.

- **No route to WAAS Express device.**

  The Central Manager is not able to reach the WAAS Express Device. Configure the correct WAAS Express management IP address by choosing the WAAS Express device, then choosing *DeviceName* **> Activation**.

- **Connection is refused by WAAS Express device.**

  The HTTPS server port configured on the WAAS Express device is not the same as the port shown in the Central Manager *DeviceName* **> Activation** page. Configure the correct WAAS Express HTTPS server port in this page.

- **WAAS support is not available on WAAS Express device.**

  The WAAS Express device is downgraded to an IOS image version with no WAAS support. Install an IOS image with WAAS support.

- **Connection timed out while communicating with WAAS Express device.**

  The WAAS Express device is taking more than 30 seconds to respond to the Central Manager. It could be because the WAAS Express device is overloaded or the network is slow.

- **License is expired on WAAS Express device.**

  The Evaluation license on the WAAS Express device is expired. Install a Permanent license by using the WAAS Express **license install** command.

- **SSL connection closed incorrectly while communicating with WAAS Express device.**

  The WAAS Express device and Central Manager are using the cipher rc4-128-md5 for SSL communication. Sometimes the Central Manager fails to decrypt the SSL data sent by the WAAS Express. Configure the ciphers 3des-ede-cbc-sha, des-cbc-sha, and rc4-128 by using the WAAS Express command **ip http secure-ciphersuite 3des-ede-cbc-sha des-cbc-sha rc4-128-sha**.

- **Failed to check the status of WAAS Express device.**

  The Central Manager is not receiving configuration status from the WAAS Express device. Contact Cisco TAC for assistance troubleshooting.

- **Management Status is offline.**

  If you see this error message, contact Cisco TAC for assistance troubleshooting.

Verifying WAAS Express HTTPS Configuration

To verify the HTTPS server configuration on the WAAS Express device, use the **show ip http server secure status** command.

```
waas-express# show ip http server secure status

HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: local
HTTP secure server active session modules: ALL
```

WAAS-Express - WAE - WAAS CM Compatibility

WAAS-Express Version 1.0,1.5

This version of WAAS-Express supports the transport optimization which includes TFO, LZ, and DRE.

WAAS-Express version 1.0 is introduced in IOS software release 15.1(3)T1
WAAS-Express version 1.5 is introduced in IOS software release 15.1(4)M. In addition to optimization, this release adds support for embedded monitoring capability called Performance Agent (PA). For more information on PA, please see PA page on CCO

```
Recommended WAAS-Express IOS image: 15.1(3)T1
Recommended WAE version: >= 4.3.1
Recommended WCM version: 4.4.5a
```

Known Issues

IOS version	WAE version	WAAS CM version	Known Issues
15.1(3)T1	5.0.1	4.4.5a	Connections originating on data-center side will not be optimized: CSCtz82646

WAAS-Express Version 2.0.0

This version of WAAS-Express, in addition to supporting transport optimization, also support selected applicaiton optimization, specifically HTTP Express, SSL Express, and CIFS Express AO.

```
Recommended WAAS-Express IOS image: 15.2(4)M1
Recommended WAE version: 5.0.1
Recommended WCM version: 5.0.1
```

Known Issues

IOS version	WAE version	WAAS CM version	Known Issues
15.2(4)M1	≤ 4.4.3c	≤ 5.0.1	HTTP-Express Accelerator requires 4.4.3c or later. Connections will not have http optimization, however, will have TDL.
15.2(4)M1	≤ 5.0.1	≤ 4.4.5a	Missing classifier name in connection statistics seen on WCM.
15.2(4)M1	≤ 5.0.1	≤ 5.0.1	CSCub21189: Policy-map changes not properly sync'ed with WAAS-Express device CSCtw50988: SMB: connection reset while downloading a file CSCtr07216: Transaction with invalid hdr not handled correctly in WAAS-X <-> WAE case CSCua49764: Https created WExp certificate - WExp went to offline after upgrade
15.2(3)T1	≤ 5.0.1	≤ 5.0.1	CSCub21189: Policy-map changes not properly sync'ed with WAAS-Express device CSCtw50988: SMB: connection reset while downloading a file CSCtr07216: Transaction with invalid hdr not handled correctly in WAAS-X <-> WAE case CSCua49764: Https created WExp certificate - WExp went to offline after upgrade

15.2(3)T	≤ 5.0.1	≤ 5.0.1	CSCtx82427: IOS-WAAS: SSL connection reset at end of transfer (EOT) CSCtz08485: Incompatible HTTP-AO detection failure (%WAAS-3-WAAS_LZ_CONN_ABORT) CSCtu19564: Crash observed in dt21 with Waas+VPN+ZBFW+NAT+NETFLOW CSCtz85134: WAAS Express SSL-Express changes self-signed trustpoint after reload CSCua22313: HTTPS page dont get displayed with IE6 conn optim by WAAS Express 2.0 CSCtw50988: SMB: connection reset while downloading a file CSCty04359: Manually created WExp certificate - after upgrade Wexp went to offline CSCtr07216: Transaction with invalid hdr not handled correctly in WAAS-X <-> WAE case

Unexpected WAAS-Express License Expiration

- The WAAS-Express license is active in **show license**. However, WAAS-Express license is expired in **show waas status**. This is potentially a known bug, CSCtw86624. Verify this by issuing following show commands. WAAS CM thinks that license is expired and shows the device as offline. However, the connections should be optimized, since based on the license, the feature is active.

  Solution: Upgrade to a recommended WAAS-Express Version 2 image - 15.2(4)M1 or install a permanent license.

```
Router#sh license | beg WAAS_Express
Index 12 Feature: WAAS_Express
Period left: Life time
License Type: RightToUse
License State: Active, In Use <---- License is Active
License Count: Non-Counted
License Priority: Low

Router#show waas status
IOS Version: 15.2(2.9)T
WAAS Express Version: 2.0.0

WAAS Enabled Interface        Policy Map
GigabitEthernet0/1            waas_global

WAAS Feature License
License Type:                          Evaluation
Evaluation total period:               0 seconds <---- License is expired.
Evaluation period left:                0 seconds
```

WAAS-Express and WAAS CM interaction issues

For a step-by-step detailed WAAS-Express registration process, please check the following document:
WAAS Express Deployment Guide

Symptom: WAAS-Express fail to register with the WAAS CM

Possible Cause #1: Connectivity issue

- Can the WAAA-Express router reaches WAAS CM?

  Troubleshoot steps: Verify that WAAS CM is ping?able from the router. In addition, if WAAS-Express router is behind NAT and/or firewall, a static NAT entry and/or firewall permit rule are required to allow WAAS CM to connect to WAAS-Express HTTPS server. To manage WAAS-Express devices behind NAT/Firewall, WAAS CM allows user to manually change/specify address of WAAS-Express device for WAAS CM to use. User can change the address from the device activation page.

  Solution: Check route and network topology to make sure WAAS CM is reachable from the router and vice versa, please enable the following debugs on WAAS-Express device.

  If required, check following debugs to figure out if SSL handshake during registration is failing:

```
debug ip http all
 debug ssl openssl errors
 debug ssl openssl ext
 debug ssl openssl msg
 debug ssl openssl states
```

  Note: The above ssl debugs are verbose.

- Did the certificate change upon router reload?

  Verify this by comparing the WAAS-Express router certificate expiration date stored on the WAAS CM. Navigate to this page from the WAAS-Express device page, Admin->Certificate. Compare the certificate information with the output of **show crypto pki certificate** output on the WAAS-Express router. If there is any mismatch, it is very likely the certificate ia re-generated.

  Solution: Upgrade to 15.2(3)T1 or 15.2(4)M1 and later

Symptom: WAAS CM shows WAAS-Express goes off-line after successful registration

Possible Cause #1: WAAS-Express device certificate changes

- Verify this by comparing the WAAS-Express router certificate expiration date stored on the WAAS CM. Navigate to this page from the WAAS-Express device page, ***Admin->Certificate***. Compare the certificate information with the output of **show crypto pki certificate** output on the WAAS-Express router. If there is any mismatch, it is very likely the certificate ia re-generated.

  Issue **show run | include crypto pki trustpoint**. Non-persistent trustpoint naming is in the format of **TP-self-signed-xxxxxxxxxx**.

```
router#show run | include crypto pki trustpoint
crypto pki trustpoint TP-self-signed-4046801426 <-- Indicate this is non-persistent trustpoint
```

  Solution: Follow this link to create persistent trustpoint.

- There are serveral instances where the certificate could be re-generated but the main reason is trustpoing is created as non-persistent. If you enable SSL Express AO with 15.2(3)T, you could also potentially hit CSCtz85134.

Solution: Upgrade to 15.2(4)M1 and re-create persistent trustpoint. Delete the certificate from WAAS CM and re-register.

- Was this an upgrade from 15.1(3)T to 15.2(3)T?

  In 15.2(3)T, there is a mandatory config within the crypto pki trustpoint, which requires rsa-keypair to be configured. If this config does not present before upgrade, this could potentially cause the router not be able to detect the trustpoint. This will cause HTTPS connectivity to fail. This problem is documented in CSCty04359.

  Solution: Remove the trustpoint and re-create. Delete the certificate from WAAS CM and re-register.

Possible Cause #2: Incorrect certificates or trustpoints are used

- Does the router have multiple trustpoints configured?

  During WAAS CM registration, WAAS-Express router selects the trustpoint which it uses for sending certificate to WAAS CM. This may be different trustpoint from what the local HTTPS server on the WAAS-Express router uses.

  Solution: Verify that the same trustpoing is configured in ip http secure-trustpoint <trustpoint_name> and ip http-client secure-trustpoint <trustpoint_name>

Possible Cause #3: Device authentication problem

- Is authentication failing?

  Verify that you can login to the WAAS-Express router, by directing your browser to WAAS-Express router using HTTPS and attempt the authentication manually.

  Solution: Verify that manual authentication is successful.

Debug Information

If you believe you are running into certificate related issuses, please provide below information to support team.

```
Router#show crypto pki trustpoints status
State:
Keys generated ..... Yes (General Purpose, non-exportable) <--- check if this shows ?No? f
Issuing CA authenticated ..... Yes <--- check if this shows ?No? for the self-signed certificate
Certificate request(s) ..... Yes <--- check if this shows ?No? for the self-signed certificate

Router#show crypto pki trustpoints status
Trustpoint TP-self-signed-2330253483:
Issuing CA certificate configured:
Subject Name:
cn=IOS-Self-Signed-Certificate-2330253483
Fingerprint MD5: 3F5E9EB4 6BD680FE 8A1C1664 0939ADCB <--- Check fingerprints before and after upgr
Fingerprint SHA1: DFF10AF4 83A90CAD 71528B3C CCD4EF0C E338E501
Router General Purpose certificate configured:
Subject Name:
cn=IOS-Self-Signed-Certificate-2330253483
Fingerprint MD5: 3F5E9EB4 6BD680FE 8A1C1664 0939ADCB
Fingerprint SHA1: DFF10AF4 83A90CAD 71528B3C CCD4EF0C E338E501
```

```
State:
Keys generated ..... Yes (General Purpose, non-exportable)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Yes

Router#show crypto pki certificates
?
Validity Date:
start date: 20:16:14 UTC May 26 2011 <--- Check whether these dates are valid
end   date: 20:16:14 UTC May 24 2016
?

Provide outputs for following commands:

show crypto pki certificates storage
show crypto pki trustpoints
show crypto key storage
show crypto key pubkey-chain rsa
show crypto key mypubkey all
show crypto key mypubkey rsa
show ip http server all
```

Symtom: Mismtach Statistic between WAAS CM and WAAS-Express

Possible Cause #1: Clocks are not synchronized

WAAS CM and WAAS-Express clock need to be in sync and hence configuring NTP server to sync clocks is highly recommended.

- Are clock-mismatch messages seen on WAAS CM?
  - Verify that the router clock is the same as WAAS CM clock in UTC format. Remove any timezone and summertime configuration and compare the UTC time between WAAS CM and WAAS-Express router.
  - Known DDTSs: **CSCtz32667, CSCtz97973, CSCtk74707, CSCtl24210**. Identify if your problem resembles any of these DDTS and follow the workaround suggested in the DDTS.

Solution: Configure NTP and verify that all devices' clock are synchronized. Follow the workaround in the DDTS mentioned above, or upgrade to the latest 15.2(4)M1 or later.

Connections are not getting optimized

Symptom: Connections are getting pass-through

Validate pass-through statistics/reason using **show waas statistics pass-through.** Look for the reason of why connections are getting pass-through.

```
Router#show waas statistics pass-through
Pass Through Statistics:
Overall:                                0
No Peer:                                0
Rejected due to Capabilities:           0
Rejected due to Resources:              0
Interface Application config:           0       <---- Traffic classified for pass-through?
Interface Global config:                0       <---- Asymmetric route in the setup?
Assymmetric setup:                      0
Peer sync was in progress:              0
IOS WAAS is intermediate router:        0
```

```
Internal error:                          0
Other end is in  black list:             0
AD version mismatch:                     0
Incompatable AO:                         0        <---- Incompatible peer?
Connection limit exceeded:               0
AOIM peertable full:                     0
AOIM multiple sync request passthrough: 0
Others:                                  0
```

Check auto-discovery statistics (and/or use auto-discovery debugs).

```
Use the following command to check the reason '''show waas statistics auto-discovery'''

Enable following debugs for more information:

debug waas infra error
debug waas infra events
debug waas auto-discovery error
debug waas auto-discovery event
debug waas auto-discovery op <---- Verbose debug
```

- If the counter for ***Interface Application Config***increments, it is likely your policy is configured to pass-through this particulate connection. Check your WAAS policy on both WAAS-Express and its peer.

  Solution: Check and validate your optimization policy. Use below debug to discover if traffic is marked as pass-through in the policy.

```
show policy-map type waas interface
debug waas infra events
```

- If the counter for ***Interface Global Config*** increments, this could be caused by asymetrical routing in your network. This is the case where WAAS-Express or its peer does not see both directions of the TCP traffic. This could be caused by true asymetrical routing in the network, or could be caused by some packets are getting dropped by devices in the traffic path (ACL, firewall, etc.)

  Solution: Check for asymetric routing of dropped packets in the network.See **what could cause asymetric routing or dropped packets in the network** below.

- Connections could also be pass-through if the peers are not compatible with each other. This may happen if you run the non-compatible version between WAAS-Express and WAE. Check the compatibility table above for recommedned software releases.

  Solution #1: Check if the peer is incompatible using **show waas statistics aoim**

  Solution #2: If you believe you have asymetrical routing scenario in your network, check the following.

What could cause asymetric routing or dropped packets in the network

- Multiple WAN links in either the WAAS-Express router or the peer. Note that WAAS-Express it not supported on active/active or active/standby routers because both traffic leaving and entering the WAN need to be on the same WAAS-Express router. If there are multiple WAN links, make sure all the WAN links have config **waas enable**. Make sure that all the WAN links and routers on the peer routers have config to redirect traffic to WAAS.

- Control packets (SYN, SYN-ACK, ACK) are not tagged with WAAS option.This could happen if the traffic is not redirected to WAAS on the peer side. ***Check your WCCP ACL.***

Information to be provided to development team:

```
Network topology
IOS version
Configuration

Following debugs and show commands:

debug waas auto-discovery error
debug waas auto-discovery event
debug waas auto-discovery operation
debug waas infra error
debug waas infra event

show waas statistics auto-disc
show waas statistics pass
show waas statistics aoim
```

 **Note**: Pass-through connections are not counted in the per-platform connection limit. WAAS-Express does not track pass-through connections, hence there are no statistics related to pass-through flows. There, however, are counters that indicate how many flows were put into pass-through and why.

Connections are not getting the desired optimization level

This is usually caused by misconfiguration. HTTP-Express Accelerator and CIFS-Express Accelerator are disabled by default in WAAS-Express Version 2 image.Check that the Express Accelerator is enabled globally.

Symtom: Established connections do not get the desired or configured policy to use CIFS, SSL, or HTTP-Express AO

- Verify that CIFS, SSL, or HTTP-Express AO is enabled globally

```
router#show waas status

IOS Version: 15.2(4)M1
WAAS Express Version: 2.0.0

WAAS Enabled Interface Policy Map
FastEthernet8 waas_global

WAAS Feature License
License Type: EvalRightToUse
Evaluation total period: 8 weeks 4 days
Evaluation period left: 7 weeks 4 days

DRE Status : Enabled
LZ Status : Enabled + Entropy
CIFS-Express AO Status : Disabled
SSL-Express AO Status : Enabled
HTTP-Express AO Status : Disabled <---- HTTP Express AO is disabled by default

Maximum Flows : 75
Total Active connections : 4
```

```
Total optimized connections : 4
```

Symtom: Expected connection optimization is THDL, but established connection has TDL

- This typically is caused by mis-configuration of the policy.

Note: HTTP-Express AO is not enabled by default.

Solution #1: Check if the core WAAS device is compatible. This check can be done using **show waas statistics aoim**
Solution #2: Check if HTTP-Express Accelerator is getting negotiated during auto-discovery using auto-discovery debugs. This may be because the accelerator is disabled globally (note that HTTP accelerator is not enabled by default), or HTTP class is missing ?accelerate http? in the action.

```
class HTTP
optimize tfo dre lz application Web accelerate http-express
```

- Check Configured, Derived and Applied Accelerator fields under **show waas connection detail**

```
Router#show waas connection detail
...
Negotiated Policy:                      TFO, LZ, DRE
Configured Accelerator:                 HTTP-Express
Derived Accelerator:                    HTTP-Express
Applied Accelerator:                    HTTP-Express
Hist. Accelerator:                      None
Bytes Read Orig:                        174
...
```

- Check handoff statistics/reason in **show waas statistics accelerator http-express [https|debug]**

Symtom: Expected connection optimization is TCDL, but established connection has TDL

- This may be because the accelerator is disabled, or CIFS/WAFS class is missing **accelerate cifs** in the action.

Note: CIFS-Express AO is disabled by default.

```
class CIFS
optimize tfo dre lz application CIFS accelerate cifs-express
```

- Check handoff statistics/reason in **show waas statistics accelerator cifs-express**

```
Router#show waas statistics accelerator cifs-express
CIFS-Express AO Statistics
...
Unsupported dialects / CIFS version:                              0
Currently active unsupported dialects / CIFS version:             0
Unsupported due to signing:                                       0
...
```

Symtom: Expected connection optimization is TSDL, but established connection has TDL

- In case of SSL-Express Accelerator, the core WAE SSL-AO may not be up and running. Check: Cisco Wide Area Application Services SSL Application Optimizer Deployment Guide
- The connection may also be getting pipe?ed. This can checked using **show waas statistics accelerator ssl**

```
Router#show waas statistics accelerator ssl
SSL-Express:
Global Statistics
-----------------
Time Accelerator was started:                    16:31:37 UTC Jul 26 2012
...
Pipe through due to C2S cipher mismatch:         0
Pipe through due to C2S version mismatch:        0
Pipe through due to W2W cipher mismatch:         0
Pipe through due to W2W version mismatch:        0
Pipe through due to detection of non-SSL traffic: 0
Pipe through due to unknown reasons:             0
Total pipe through connections:                  0
...
```

Expected connection optimization is TSHDL, but established connection has only TSDL or THDL

SSL-Express Accelerator introduces HTTP-Express Accelerator in the path. Make sure both SSL-Express and HTTP-Express Accelerator are enabled globally.

- The connection got pipe-through?ed and shows up as TG. As shown above, check reason in **show waas statistics accelerator ssl**
- **If** the connection shows up as TSDL could be due to one of the following
    - ♦ HTTP-Express Accelerator is disabled.
    - ♦ HTTP-Express Accelerator is not compatible with the HTTP AO on core WAAS device.
        - ◊ At least 3 optimization features of HTTP-Express Accelerator are not enabled.
    - ♦ The first data packet does not contain HTTP content.

- If the connection shows up as THDLcould be due to one of the following
    - ♦ SSL-Express Accelerator is not up and running on edge device.
    - ♦ SSL AO is not up and running on core device.
    - ♦ SSL-AO was not negotiated in AOIM.
    - ♦ For proxy, HTTP CONNECT request is to a port other than 443.
    - ♦ The 3-way DATA-INSPECT handshake where both edge and core devices notify each other regarding addition of SSL-AO to the optimization for this connection fails.
    - ♦ Post DATA-INSPECT handshake, the 3-way TFO handshake where both edge and core devices agree to add SSL-AO to the optimization for this connection fails.

```
Provide following show command outputs for debugging:

show waas status
show waas alarms
show waas accelerator detail
show waas accelerator http
show waas accelerator smb
show waas accelerator ssl
show waas statistic global
```

```
show waas statistic auto-discovery
show waas statistic aoim
show waas statistic pass-through
```

Symptom: Unexpected Connection Reset

Typically, there will also be error message which indicates the type of error along with the flow that is getting reset. For example,

```
Aug 18 03:02:52.861: %WAAS-3-WAAS_TFO_DEC_FRAME_FAILED: IOS-WAAS failed to decode TFO frame for cc
```

Steps to troubleshoot

- Turn on error debugs, depending on the module, **debug waas <module_name> error**.
- Check **End-Reason** in **show waas connection detail**
- Check **show waas statistics error** for possible reasons.
- Is a core-dump generated on core WAE when connection resets are seen?
    - ♦ Malformed TCP headers sent by WAAS-Express resulted in core-dumps on WAE.
    - ♦ DDTSs capturing this issue: **CSCto59459, CSCua61097**. Search for these DDTS and check whether the issue seen is similar to the one outlined by them.
- If this is an SSL-Express Accelerator connection is the reset being caused by W2W handshake failure?

Information to be provided to the development team:

Debug logs Show command logs show-tech show-running config Network topology Client and server details, along with the application (and version, e.g. IE6) being used for connection.

```
debug waas infra error
debug waas auto-discovery error
debug waas aoim error
debug waas tfo error
debug waas lz error
debug waas dre error
debug waas accelerator ssl error
debug waas accelerator http error
debug waas accelerator cifs error
```

Router crash/tracebacks

Router crashes and tracebacks may have been seen during testing. Search of previous cases and DDTSs for similar known issues. In addition we also need to isolate what feature is resulting in the crash. If an IOS feature other than ios-waas or layer4-forwarding is resulting in a crash/traceback, then that particular feature development team/ router TAC should be contacted accordingly.

- Do a topic search at topic.cisco.com
- Check previous customer cases for similar/known issues.

Information to be provided to the development team:

- **show tech** or if not possible**show running-config** output
- Exact IOS version.
- Exact steps to reproduce the problem.

- Decodes of traceback, or crashinfo in the case of crash.
- Topology of the network
- Any relevant information that will help with the reproduction of the problem internally.

Slow connection/degraded performance

Degraded performance may be caused by various reasons: the nature of the traffic, the load on the router, network topology or packet drops in the network. For dealing with slow connections, we need to determine relative degradation with respect to pass-through or non-optimized connections.

Step to troubleshoot

- What is the optimization action for the connection?
  - Check **Accel** field in **show waas connection**. Is it TDL, THDL, TSDL, etc?
  - If a particular Accelerator is being used, does turning it off recover from the poor performance?
  - If there is upload traffic, try disable uplink DRE in the WAAS-Express parameter-map.
  - If the connection is put in TFO-only mode, is there a degradation seen with respect to pass-through mode?
- What is the load on the router, check cpu utilization using: **show proc cpu history**
  - Check whether CPU throttling messages are seen in the log. When the CPU is too high, WAAS-Express slows down the optimization in order to protect the CPU from being too overloaded
- Check output of interface statistics to determine if there are packet drops.
- Check if there are any ACLs that are dropping packets. A good debug to find which feature drops any packets is **debug ip cef drop**.
- Check if any device in the middle is dropping packets.
  - WAEs turn on ECN by default, and send packets with ECT bit set. Old devices may not like packets with ECT bit set and hence can drop these packets leading to retransmissions and hence degraded performance. In a particular customer case, a device (with an old IOS image) in the middle was dropping packets that had ECT bit set in the TCP header.
  - ECN can be turned off on core WAE by using the following command in config mode: **no tcp ecn enable**
- Does the setup have WAAS-Express enabled on multiple WAN links? If so, is the load-sharing being used a supported option?
  - Per-packet load-sharing is not a supported option.
  - Per-destination load-sharing is a supported option. There should be no performance impact seen with this load-sharing.
  - Asymmetric routing in the network, causing packet drops and retransmissions.
  - If the router does not see all packets of a particular flow, this may lead to slow/hung connections.
- Slow connection with uplink-dre
  - Re-transmissions due to NACKs: Check show waas statistics dre. Check the **R-tx ..** fields
  - ACK-queue full: Check **show waas statistics dre**. Check the **AckQ full** and **AckQ high** fields
- Connection slowed after enabling CIFS-Express/SSL-Express/HTTP-Express Accelerators.
  - Unsupported version/dialect.
- Low compression ratio.
  - Check statistics under **show waas connection detail, show waas statistic lz, show waas statistic dre**
  - Check for connection handoff/pipe-through.

Note: Per-packet load-sharing is not a supported deployment. This is not a default load sharing mode.

Hung connections

There are no known issues with hung connections, please provide the following information to the development team to help RCA the problem.

Step to troubleshoot and collect information

- Search the flow in WAAS-Express connection table using **show waas connection**.

```
Router#show waas connection
ConnID     Source IP:Port         Dest IP:Port           PeerID            Accel
3336       192.168.22.99  :37797  192.168.42.99  :80     0016.9d39.20bd    THDL
Router#
```

- Display the detail about the connection

```
Router#show waas connection client-port 37797 detail

connection  ID:                          3336
Peer Id:                                 0016.9d39.20bd
Connection Type:                         External
Start Time:                              19:45:34 UTC Dec 21 2011
Source IP Address:                       192.168.22.99
Source Port Number:                      37797        <------ Unique port number required for next
Destination IP Address:                  192.168.42.99
Destination Port Number:                 80
Application Name:                        Web
Classifier Name:                         HTTP
Peer Policy:                             TFO, LZ, DRE
Configured Policy:                       TFO, LZ, DRE
Negotiated Policy:                       TFO, LZ, DRE
Configured Accelerator:                  HTTP-Express
Derived Accelerator:                     HTTP-Express
Applied Accelerator:                     HTTP-Express
Hist. Accelerator:                       None
Bytes Read Orig:                         43056412
Bytes Written Orig:                      25
Bytes Read Opt:                          162
Bytes Written Opt:                       43359878
Auto-discovery information:
---<snip>---
```

- Find an equivalent flow in L4F table using **show l4f flows**.

```
Router#show l4f flows | include 37797
F4DF6EA0  Proxy  TCP         192.168.22.99:37797          192.168.42.99:80
Router#
```

- From the first column, collect the L4F flow id and use the information to get the detail L4F connection information.

```
Router#show l4f flow detail F4DF6EA0
Flow Address  : F4DF6EA0
Index         : 11
Idle Time     : 0.004
Family        : IPv4
```

```
Protocol      : TCP
VRF ID        : 0
Address1      : 192.168.22.99:37797
Address2      : 192.168.42.99:80
State         : L4F_STATE_PROXYING
Flags         : 0x00012000
App Context   : 0x41D4728C
CEF pak       : 0x0
Endpoint1 FD 1073748479
             State         : EP-ESTAB
             Flags         : 0x00000001
             Client        : L4F_FEATURE_WAAS
             Association   : OUTPUT
             CEF Fwd State : 0xC20D2C74
             Proc Fwd State: 0xC1E36EA8
             TCB Address   : 0xC01F0D9C   <------ Address required for next step
Endpoint2 FD 1073748480
             State         : EP-ESTAB
             Flags         : 0x00000001
             Client        : L4F_FEATURE_WAAS
             Association   : INPUT
             CEF Fwd State : 0xC20D2248
             Proc Fwd State: 0xC1E36F20
             TCB Address   : 0x4002AB6C  <------ Address required for next step
```

- The output of **show l4f flow detail <flow_id>** show the two TCP TCBs. Use the TCB information in **show tcp tdb <tcb_info>**

```
Router#show tcp tcb 0xC01F0D9C
Connection state is ESTAB, I/O status: 1, unread input bytes: 31504
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 192.168.42.99, Local port: 80
Foreign host: 192.168.22.99, Foreign port: 37797
Connection tableid (VRF): 0
Maximum output segment queue size: 50

Enqueued packets for retransmit: 0, input: 22  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x85115B0):
Timer          Starts    Wakeups            Next
Retrans             2          0             0x0
TimeWait            0          0             0x0
AckHold         10192          0             0x0
SendWnd             0          0             0x0
KeepAlive       20129          0       0x851FFF4
GiveUp              2          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
Linger              0          0             0x0
ProcessQ            1          1             0x0

iss:  688070906  snduna:  688070932  sndnxt:  688070932
irs:  684581592  rcvnxt:  713368125

sndwnd:   6144  scale:      9  maxrcvwnd:  32767
rcvwnd:   1263  scale:      7  delrcvwnd:      0

SRTT: 6687 ms, RTTO: 59312 ms, RTV: 52625 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 2857348 ms, ACK hold: 200 ms
Status Flags: passive open, Timestamp echo present
Option Flags: keepalive running, SACK option permitted, non-blocking reads
non-blocking writes, win-scale, 0x200000, 0x1000000, 0x10000000
0x20000000
```

```
IP Precedence value : 0

Datagrams (max data segment is 1432 bytes):
Rcvd: 20129 (out of order: 0), with data: 20127, total data bytes: 28786532
Sent: 30017 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data: 1,
Packets received in fast path: 53559, fast processed: 2, slow path: 21294
fast lock acquisition failures: 7, slow path: 0
Router#
Router#show tcp tcb 0x4002AB6C
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 192.168.22.99, Local port: 37797
Foreign host: 192.168.42.99, Foreign port: 80
Connection tableid (VRF): 0
Maximum output segment queue size: 50

Enqueued packets for retransmit: 50, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x8519A48):
Timer          Starts    Wakeups            Next
Retrans         27124          0       0x8519D3B
TimeWait            0          0             0x0
AckHold             2          0             0x0
SendWnd             0          0             0x0
KeepAlive       28560          0       0x85284A4
GiveUp          27121          0       0x8545964
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
Linger              0          0             0x0
ProcessQ        19975      19975             0x0

iss: 2832065240  snduna: 2867154917  sndnxt: 2867205953
irs: 2835554554  rcvnxt: 2835554717

sndwnd: 261120  scale:      7  maxrcvwnd:  65535
rcvwnd:  65535  scale:      7  delrcvwnd:      0
bic_last_max_cwnd:    8388480

SRTT: 1000 ms, RTTO: 1003 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 80 ms, maxRTT: 1000 ms, ACK hold: 200 ms
Status Flags: active open
Option Flags: keepalive running, SACK option permitted,
Timestamp option used, non-blocking reads, non-blocking writes
win-scale, 0x200000, 0x1000000, 0x10000000, 0x20000000
IP Precedence value : 0

Datagrams (max data segment is 1432 bytes):
Rcvd: 28560 (out of order: 0), with data: 2, total data bytes: 162
Sent: 28672 (retransmit: 0, fastretransmit: 28, partialack: 3, Second Congestion: 0), with data: 2
Packets received in fast path: 21244, fast processed: 21240, slow path: 29668
fast lock acquisition failures: 21374, slow path: 0
Router#
```

- The following command output can be useful in debugging the WAAS-Express AO.

```
show waas statistics errors
show waas statistics accelerator http-express
show waas statistics accelerator cifs-express
show waas statistics accelerator ssl-express
show waas statistics accelerator ssl-express debug
```

- The following is a service-internal command (for debugging only)

```
show waas connection conn-id [id] debug
show waas statistics accelerator http-express debug
show waas statistics accelerator ssl-express debug
```

- Hung connections can be cleared using the following command.

```
clear waas connection conn-id [id]
Router(config-if)#no waas enable forced
```

SSL-Express Accelerator issues:

Having issues with SSL-Express Accelerator enable or disable

- Check if security license is enabled

```
Router#show waas status | include SSL-Express AO Status
SSL-Express AO Status             : Unavailable (security license not enabled)

Router#show license detail securityk9
Index: 1        Feature: securityk9                       Version: 1.0
    License Type: RightToUse
?
```

- Check if you have an NPE image (this image does not support SSL-Express Accelerator)

```
Router#show waas status | include SSL-Express AO Status
SSL-Express AO Status             : Unsupported

Router#show license detail securityk9
% Error: No license for securityk9 found - License feature not found
```

- Enable ssl, aoim and infra debugs during enable/disable operation and provide debug logs.

- Connection getting reset because of W2W handshake failure
  - ♦ Check SSL-Express Accelerator error statistics using **show waas statistics errors | i SSL-Express**
  - ♦ Check certificates:

```
Router#show running-config all | include waas-ssl-trustpoint
Router#show crypto pki trustpoints <trustpoint-name> status

WAAS#show crypto certificates
WAAS#show crypto certificate-detail WORD
```

- Check alarms:

```
Router#show waas alarms
...
WAAS SSL-Express CA enrolled trustpoint deleted:  off
WAAS SSL-Express router certificate deleted:      off
...
```

- Check configuration on edge and core devices. Check they are in-sync with respect to cipher-list, SSL version, and certificate verification and revocation checks.
- If self-signed certificates are being used, revocation-check and certificate verification should be disabled.
- Turn on **debug waas accelerator ssl error**

- Connection getting pipe-through?ed because of C2S Unsupported cipher
    - ♦ Check SSL-Express Accelerator error statistics using **show waas statistics errors | i SSL-Express**
    - ♦ Turn on **debug waas accelerator ssl**
    - ♦ Check cipher-list configured in the **accelerated-svc** on core WAAS device.

- No SSL optimization (Pipe-through)
    - ♦ Check SSL-Express status on WAAS Express device: **show waas accelerator ssl-express**
    - ♦ Check SSL AO status on peer WAAS device: **show accelerator ssl**
    - ♦ Check SSL-Express statistics: **show waas statistics accelerator ssl-express | i Pipe**

- Unable to access HTTPS page from internet
    - ♦ Since server is in internet, it?s private key and certificate can?t be installed on core WAAS device. Even after accepting warning for certificate in the browser some objects on page may not show-up.
    - ♦ These objects may be served from CDN (content-delivery network). This issue is not unique to WAAS-Express. That is, it should happen when connection is optimized between two WAAS devices as well.
    - ♦ Users will need to add exception to the browser to ignore certificate from CDN URL.
    - ♦ CDN URL can be found in page source.

```
Show commands used for further debugging and RCA:

show waas statistics accelerator ssl
show waas statistics accelerator ssl debug
show waas statistics accelerator ssl ciphers
show waas statistics accelerator ssl peering
```

Moving WAAS-Express device between Device-Groups on CM

If a WAAS-Express device is moved between device-groups on the WCM, it is sometimes seen that the policy definitions under the new device-group do not take effect. When a device is unassigned from a device-group, it gets the policies from the backup policy set of what the device last owned.

Use the following steps when moving the device between device-groups:

```
* Go to the Policy Definitions page of that device and select the new device-group and click on Su

OR

* Go to device-group-1 -> Assign Devices page and unassign the device from this DG.
* Go to device-group-2 -> Assign Devices page and assign the device to this DG.
* Go to device-group-2 -> Policy Definitions page and click on 'Force DG settings' button.
```

Other useful information

Statistics mismatch on WAAS-Express and WCM/WAE:

There are no known issues in this area. Please collect the logs using following procedure and provide them to the development team.

```
* Disable waas on Waas-Express device
* Clear statistics on WAAS-Express and core WAE
* Enable waas on Waas-Express device
* Let traffic run, disable waas on Waas-Express device
```

```
* Collect statistics
* Present screen-shots and show command outputs.
```

Information in addition to debugs and show commands, that needs to be provided to the development team:

```
show tech-support
show ip interface
show ip virtual-reassembly
show ip route
show ip cef detail
show ip cef internal
show ip cef switching statistics
show process cpu history
```

Troubleshooting router crash

http://www.cisco.com/en/US/products/hw/iad/ps397/products_tech_note09186a00800b4447.shtml

Capturing packets on router

To debug connection problems, you may need to capture packets on the WAAS Express device.

For details on IOS packet capture, see the document: IP Traffic Export.

```
Example to configure packet capture:

ip traffic-export profile waas_wan mode capture bidirectional

interface Serial0/0/0
  ip virtual-reassembly out
  encapsulation frame-relay
  ip traffic-export apply waas_wan size 20000000
  frame-relay map ip 10.0.0.2 557 broadcast
  no frame-relay inverse-arp
  frame-relay local-dlci 557

Use following commands to start, stop, copy and clear the buffer:

traffic-export int s0/0/0 start
traffic-export int s0/0/0 stop
traffic-export int s0/0/0 copy ftp://username:password@192.168.1.116//tftpboot/ngwo.pcap
traffic-export int s0/0/0 clear
```