Troubleshooting

This topic contains the following sections:

- General Troubleshooting Best Practices, on page 1
- FIPS Mode Problems, on page 2
- Authentication Problems, on page 2
- Blocked Object Problems, on page 4
- Browser Problems, on page 5
- DNS Problems, on page 5
- Failover Problems, on page 5
- Feature Keys Expired, on page 6
- FTP Problems, on page 6
- Upload/Download Speed Issues, on page 7
- Hardware Issues, on page 8
- HTTPS/Decryption/Certificate Problems, on page 9
- Identity Services Engine Problems, on page 11
- Problems with Custom and External URL Categories, on page 14
- Logging Problems, on page 16
- Policy Problems, on page 17
- Problems with File Reputation and File Analysis , on page 22
- Reboot Issues, on page 23
- Site Access Problems, on page 24
- Upstream Proxy Problems, on page 25
- Virtual Appliances , on page 26
- WCCP Problems, on page 27
- Packet Capture, on page 27
- Working With Support , on page 29

General Troubleshooting Best Practices

Configure your Access Logs to include the following custom fields:

%u, %g, %m, %k, %L (These values are case-sensitive.)

For descriptions of these fields, see Access Log Format Specifiers and W3C Log File Fields.

For configuration instructions, see Customizing Access Logs and Adding and Editing Log Subscriptions.

FIPS Mode Problems

Check the following topics if you encounter encryption and certificate problems after you upgraded your Web Security Appliance to AsyncOS 10.5, and enabled FIPS mode and CSP encryption.

- CSP Encryption, on page 2
- Certificate Validation, on page 2

CSP Encryption

For a feature that worked before you enabled FIPS-mode CSP encryption, but doesn't work after encryption is enabled, determine if the CSP encryption is the problem. Disable CSP encryption and FIPS mode and then test the feature. If it works, enable FIPS mode and test it again. If it works, enable CSP encryption and test it again. See Enabling or Disabling FIPS Mode.

Certificate Validation

Certificates which were accepted by your Web Security Appliance prior to upgrading to AsyncOS 10.5 might be rejected when they are uploaded again, regardless of upload method. (That is, via UI pages such as HTTPS Proxy, Certificate Management, Identity Provider for SaaS, ISE configuration, Authentication configuration, or via the `certconfig` CLI command.)

Ensure that the certificate's signer CAs have been added as "Custom Trusted Certificate Authorities" on the Certificate Management page (Network > Certificate Management). A certificate cannot be uploaded to the Web Security Appliance if the complete certificate path is untrusted.

Also, when reloading an older configuration, its likely that the included certificates will not be trusted and the reload will fail. Ensure these certificates are replaced while loading the saved configuration.

Note All certificate validation failures are logged in the audit logs (`/data/pub/audit_logs/audit_log.current`).

Authentication Problems

- Troubleshooting Tools for Authentication Issues , on page 3
- Failed Authentication Impacts Normal Operations, on page 3
- LDAP Problems, on page 3
- Basic Authentication Problems, on page 4
- Single Sign-On Problems, on page 4
- Also see:
  - General Troubleshooting Best Practices, on page 1
  - HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 18

• Cannot Access URLs that Do Not Support Authentication, on page 24
• Client Requests Fail Upstream Proxy, on page 25

Troubleshooting Tools for Authentication Issues

KerbTray or klist (both part of the Windows Server Resources Kit) for viewing and purging a Kerberos ticket cache. Active Directory Explorer for viewing and editing an Active directory. Wireshark is a packet analyzer you can use for network troubleshooting.

Failed Authentication Impacts Normal Operations

When certain user agents or applications fail to authenticate and are denied access, they repeatedly send requests to the Web Security Appliance , which in turn repeatedly sends requests to the Active Directory servers with machine credentials, sometimes to the point of impacting normal operations.

For best results, bypass authentication with these user agents. See Bypassing Authentication with Problematic User Agents.

LDAP Problems

• LDAP User Fails Authentication due to NTLMSSP, on page 3
• LDAP Authentication Fails due to LDAP Referral, on page 3

LDAP User Fails Authentication due to NTLMSSP

LDAP servers do not support NTLMSSP. Some client applications, such as Internet Explorer, always choose NTLMSSP when given a choice between NTLMSSP and Basic. When all of the following conditions are true, the user will fail authentication:

- The user only exists in the LDAP realm.
- The Identification Profile uses a sequence that contains both LDAP and NTLM realms.
- The Identification Profile uses the “Basic or NTLMSSP” authentication scheme.
- A user sends a request from an application that chooses NTLMSSP over Basic.

Reconfigure the Identification Profile or the authentication realm or the application such that at least one of the above conditions will be false.

LDAP Authentication Fails due to LDAP Referral

LDAP authentication fails when all of the following conditions are true:

- The LDAP authentication realm uses an Active Directory server.
- The Active Directory server uses an LDAP referral to another authentication server.
- The referred authentication server is unavailable to the Web Security Appliance .

Workarounds:

- Specify the Global Catalog server (default port is 3268) in the Active Directory forest when you configure the LDAP authentication realm in the appliance.
- Use the `advancedproxyconfig` > `authentication` CLI command to disable LDAP referrals. LDAP referrals are disabled by default.

Basic Authentication Problems

- Basic Authentication Fails, on page 4

Related Problems

- Upstream Proxy Does Not Receive Basic Credentials, on page 25

Basic Authentication Fails

AsyncOS for Web only supports 7-bit ASCII characters for passphrases when using the Basic authentication scheme. Basic authentication fails when the passphrase contains characters that are not 7-bit ASCII.

Single Sign-On Problems

- Users Erroneously Prompted for Credentials, on page 4

Users Erroneously Prompted for Credentials

NTLM authentication does not work in some cases when the Web Security Appliance is connected to a WCCP v2 capable device. When a user makes a request with a highly locked down version of Internet Explorer that does not do transparent NTLM authentication correctly and the appliance is connected to a WCCP v2 capable device, the browser defaults to Basic authentication. This results in users getting prompted for their authentication credentials when they should not get prompted.

Workaround

In Internet Explorer, add the Web Security Appliance redirect hostname to the list of trusted sites in the Local Intranet zone (Tools > Internet Options > Security tab).

Blocked Object Problems

- Some Microsoft Office Files Not Blocked, on page 4
- Blocking DOS Executable Object Types Blocks Updates for Windows OneCare, on page 5

Some Microsoft Office Files Not Blocked

When you block Microsoft Office files in the Block Object Type section, it is possible that some Microsoft Office files will not be blocked.

If you need to block all Microsoft Office files, add **application/x-ole** in the Block Custom MIME Types field. However, blocking this custom MIME type also blocks all Microsoft Compound Object format types, such as Visio files and some third-party applications.

Blocking DOS Executable Object Types Blocks Updates for Windows OneCare

When you configure the Web Security Appliance to block DOS executable object types, the appliance also blocks updates for Windows OneCare.

Browser Problems

• WPAD Not Working With Firefox, on page 5

WPAD Not Working With Firefox

Firefox browsers may not support DHCP lookup with WPAD. For current information, see https://bugzilla.mozilla.org/show_bug.cgi?id=356831 .

To use Firefox (or any other browser that does not support DHCP) with WPAD when the PAC file is hosted on the Web Security Appliance , configure the appliance to serve the PAC file through port 80.

Procedure

Step 1 Choose **Security Services > Web Proxy** and delete port 80 from the **HTTP Ports to Proxy** field.

Step 2 Use port 80 as the PAC Server Port when you upload the file to the appliance.

Step 3 If any browsers are manually configured to point to the web proxy on port 80, reconfigure those browsers to point to another port in the HTTP Ports to Proxy field.

Step 4 Change any references to port 80 in PAC files.

DNS Problems

• Alert: Failed to Bootstrap the DNS Cache, on page 5

Alert: Failed to Bootstrap the DNS Cache

If an alert with the message “Failed to bootstrap the DNS cache” is generated when an appliance is rebooted, it means that the system was unable to contact its primary DNS servers. This can happen at boot time if the DNS subsystem comes online before network connectivity is established. If this message appears at other times, it could indicate network issues or that the DNS configuration is not pointing to a valid server.

Failover Problems

• Failover Misconfiguration, on page 6
• Failover Issues on Virtual Appliances , on page 6

Failover Misconfiguration

Misconfiguration of failover groups might result in multiple primary appliances or other failover problems. Diagnose failover problems using the `testfailovergroup` subcommand of the CLI `failoverconfig` command.

For example:

```
wsa.wga> failoverconfig
Currently configured failover profiles:
1.      Failover Group ID: 61
        Hostname: failoverV4P1.wga, Virtual IP: 10.4.28.93/28
        Priority: 100, Interval: 3 seconds
        Status: PRIMARY
Choose the operation you want to perform:
- NEW - Create new failover group.
- EDIT - Modify a failover group.
- DELETE - Remove a failover group.
- PREEMPTIVE - Configure whether failover is preemptive.
- TESTFAILOVERGROUP - Test configured failover profile(s)
[]> testfailovergroup
Failover group ID to test (-1 for all groups):
[]> 61
```

Failover Issues on Virtual Appliances

For deployments on virtual appliances, ensure that you have configured the interface/ virtual switch on the hypervisor to use promiscuous mode.

Feature Keys Expired

If the feature key for the feature you are trying to access (via the web interface) has expired, please contact your Cisco representative or support organization.

FTP Problems

- URL Categories Do Not Block Some FTP Sites, on page 6
- Large FTP Transfers Disconnect, on page 7
- Zero Byte File Appears On FTP Servers After File Upload, on page 7
- Chrome Browser Not Detected As User Agent in FTP-over-HTTP Requests, on page 7
- Also see:
  - Unable to Route FTP Requests Via an Upstream Proxy, on page 26
  - HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 18

URL Categories Do Not Block Some FTP Sites

When a native FTP request is transparently redirected to the FTP Proxy, it contains no hostname information for the FTP server, only its IP address. Because of this, some predefined URL categories and Web Reputation Filters that have only hostname information will not match native FTP requests, even if the requests are

destined for those servers. If you wish to block access to these sites, you must create custom URL categories for them using their IP addresses.

Large FTP Transfers Disconnect

If the connection between the FTP Proxy and the FTP server is slow, uploading a large file may take a long time, particularly when Cisco Data Security Filters are enabled. This can cause the FTP client to time out before the FTP Proxy uploads the entire file and you may get a failed transaction notice. The transaction does not fail, however, but continues in the background and will be completed by the FTP Proxy.

You can workaround this issue by increasing the appropriate idle timeout value on the FTP client.

Zero Byte File Appears On FTP Servers After File Upload

FTP clients create a zero byte file on FTP servers when the FTP Proxy blocks an upload due to outbound anti-malware scanning.

Chrome Browser Not Detected As User Agent in FTP-over-HTTP Requests

Chrome browsers do not include a user-agent string in FTP-over-HTTP requests; therefore, Chrome cannot be detected as the user agent in those requests.

Upload/Download Speed Issues

The Web Security Appliance is designed to handle thousands of client and server connections in parallel, and the sizes of the send and receive buffers are configured to deliver optimal performance, without sacrificing stability. Generally, actual usage is browse traffic, consisting of numerous short-lived connections for which we have receive-packet-steering (RPS) and receive-flow-steering (RFS) data, and for which the Web Security Appliance has been optimized.

However, at times you may experience a noticeable reduction in upload or download speeds; for example, when transferring large files via proxy. To illustrate: assuming a 10-Mbps line, downloading a 100-MB file that passes through a Web Security Appliance can be approximately seven to eight times slower than downloading the file directly from its server.

In non-typical environments that include a larger proportion of large-file transfers, you can use the `networktuning` command to increase send and receive buffer size to alleviate this issue, but doing so can also cause network memory exhaustion and affect system stability. See Web Security Appliance CLI Commands for details of the `networktuning` command.

Caution Exercise care when changing the TCP receive and send buffer control points and other TCP buffer parameters. Use the `networktuning` command only if you understand the ramifications.

To configure the buffer size in `networktuning`, ensure that you have enabled the automatic send and receive options that are provided under `networktuning`.

Here are examples of using the `networktuning` command on two different appliances:

On an S380

```
networktuning
sendspace = 131072
recvspace = 131072
send-auto = 1 [Remember to disable miscellaneous > advancedproxy > send buf auto tuning]
recv-auto = 1 [Remember to disable miscellaneous > advancedproxy > recv buf auto tuning]
mbuf clusters = 98304 * (X/Y)  where is X is RAM in GBs on the system and Y is 4GB.
sendbuf-max = 1048576
recvbuf-max = 1048576
```

Questions

What are these parameters?

The Web Security Appliance has several buffers and optimization algorithms which can be altered for specific needs. Buffer sizes are originally optimized to suit the "most common" deployment scenarios. However, larger buffer sizes can be used when faster per-connection performance is needed, but note that overall memory usage will increase. Therefore, buffer-size increases should be in line with the memory available on the system. The send- and receive-space variables control the size of the buffers available for storing data for communication over a socket. The send- and receive-auto options are used to enable and disable dynamic scaling of send and receive TCP window sizes. (These parameters are applied in the FreeBSD kernel.)

How were these example values determined?

We tested different sets of values on a customer's network where this "problem" was observed, and "zeroed in" on these values. We then further tested these changes for stability and performance increase in our labs. You are free to use values other than these at your own risk.

Why are these values not the defaults?

As mentioned, by default the Web Security Appliance is optimized for the most-common deployments, and operating in a very large number of locations without per-connection performance complaints. Making the changes discussed here will not increase RPS numbers, and in fact may cause them to drop.

Hardware Issues

- Cycling Appliance Power , on page 8
- Appliance Health and Status Indicators , on page 8
- Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware, on page 9

Cycling Appliance Power

Important! If you need to cycle power to your x80 or x90 appliance, wait at least 20 minutes for the appliance to come up again (all LEDs are green) before pushing the power button.

Appliance Health and Status Indicators

Lights on the front and/or rear panels of your hardware appliance indicate health and status of your appliance. For descriptions of these indicators, see the hardware guides, such as the *Cisco x90 Series Content Security Appliances Installation and Maintenance Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Specifications for your appliance, such as temperature ranges, are also available in these documents.

Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware

This alert may or may not indicate a problem. The battery relearn timeout, in itself, does not mean there is any problem with the RAID controller. The controller can recover in the subsequent relearn. Please monitor your email for any other RAID alerts for the next 48 hours, to ensure that this is not the side-effect of any other problem. If you do not see any other RAID-type alerts from the system, then you can safely ignore this alert.

HTTPS/Decryption/Certificate Problems

- Accessing HTTPS Sites Using Routing Policies with URL Category Criteria, on page 9
- HTTPS Request Failures, on page 9
- Bypassing Decryption for Particular Websites, on page 10
- Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content, on page 10
- Alert: Problem with Security Certificate, on page 11
- Also see:
  - Logging HTTPS Transactions, on page 16
  - Access Policy not Configurable for HTTPS, on page 17
  - HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 18

Accessing HTTPS Sites Using Routing Policies with URL Category Criteria

For transparently redirected HTTPS requests, the Web Proxy must contact the destination server to determine the server name and therefore the URL category in which it belongs. Due to this, when the Web Proxy evaluates Routing Policy Group membership, it cannot yet know the URL category of an HTTPS request because it has not yet contacted the destination server. If the Web Proxy does not know the URL category, it cannot match the transparent HTTPS request to any user-defined Routing Policy because of insufficient information.

As a result, transparently redirected HTTPS transactions only match Routing Policies if no Routing Policy Group and no identification profile has a membership criteria. If any user-defined Routing Policies or identification profiles define their membership by URL category, then the transparent HTTPS transactions match the Default Routing Policy Group.

HTTPS Request Failures

- HTTPS with IP-based Surrogates and Transparent Requests, on page 9
- Different Client “Hello” Behavior for Custom and Default Categories, on page 10

HTTPS with IP-based Surrogates and Transparent Requests

If the HTTPS request comes from a client that does not have authentication information available from an earlier HTTP request, AsyncOS either fails the HTTPS request or decrypts the HTTPS request in order to authenticate the user, depending on how you configure the HTTPS Proxy. Use the HTTPS Transparent Request setting on the Security Services > HTTPS Proxy page to define this behavior. Refer to the Enabling HTTPS Proxy section in Decryption Policies topic.

Different Client "Hello" Behavior for Custom and Default Categories

When scanning packet captures, you may notice that the "Client Hello" handshake is sent at different times for custom category and default (Web) category HTTPS Decryption pass-through policies.

For an HTTPS page passed through via the default category, the Client Hello is sent before receipt of a Client Hello from the requestor, and the connection fails. For an HTTPS page passed through via a custom URL category, the Client Hello is sent after the Client Hello is received from the requestor, and the connection is successful.

As a remedy, you can create a custom URL category with a pass-through action for SSL 3.0-only-compatible Web pages.

Bypassing Decryption for Particular Websites

Some HTTPS servers do not work as expected when traffic to them is decrypted by a proxy server, such as the Web Proxy. For example, some websites and their associated web applications and applets, such as high security banking sites, maintain a hard-coded list of trusted certificates instead of relying on the operating system certificate store.

You can bypass decryption for HTTPS traffic to these servers to ensure all users can access these types of sites.

Procedure

Step 1 Create a custom URL category that contains the affected HTTPS servers by configuring the Advanced properties.

Step 2 Create a Decryption Policy that uses the custom URL category created in Step 1 as part of its membership, and set the action for the custom URL category to Pass Through.

Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content

Referrer-based exceptions are supported only in Access policies. To use this feature with HTTPS traffic, before defining exceptions in Access policies, you must configure HTTPS decryption of the URL Categories that you will select for exception. However, this feature will not work under certain conditions:

Note When time ranges are configured, they receive the highest priority. The referrer will not function if the Time Range quota has been reached.

- If the connection is tunneled and HTTPS decryption is not enabled, this feature will not work for requests going to HTTPS sites.
- According to RFC 2616, a browser client could have a toggle switch for browsing openly/anonymously, which would respectively enable/disable the sending of Referer and from information. The feature is exclusively dependent on the Referer header, and turning off sending them would cause our feature not to work.

- According to RFC 2616, clients should not include a Referer header field in a (non-secure) HTTP request if the referring page was transferred with a secure protocol. So, any request from an HTTPS-based site to an HTTP-based site would not have the Referer header, causing this feature to not work as expected.
- When a Decryption policy is set up such that when a custom category matches the Decryption policy and the action is set to Drop, any incoming request for that category will be dropped, and no bypassing will be done.

Alert: Problem with Security Certificate

Typically, the root certificate information you generate or upload in the appliance is not listed as a trusted root certificate authority in client applications. By default in most web browsers, when users send HTTPS requests, they will see a warning message from the client application informing them that there is a problem with the website's security certificate. Usually, the error message says that the website's security certificate was not issued by a trusted certificate authority or the website was certified by an unknown authority. Some other client applications do not show this warning message to users nor allow users to accept the unrecognized certificate.

Note **Mozilla Firefox browsers:** The certificate you upload must contain "basicConstraints=CA:TRUE" to work with Mozilla Firefox browsers. This constraint allows Firefox to recognize the root certificate as a trusted root authority.

Identity Services Engine Problems

- Tools for Troubleshooting ISE Issues, on page 11
- ISE Server Connection Issues, on page 12
- ISE-related Critical Log Messages, on page 14

Tools for Troubleshooting ISE Issues

The following can be useful when troubleshooting ISE-related issues:

- The ISE test utility, used to test the connection to the ISE server, provides valuable connection-related information. This is the **Start Test** option on the Identity Services Engine page; see Connect to the ISE/ISE-PIC Services.
- ISE and Proxy Logs; see Monitor System Activity Through Logs
- ISE-related CLI commands `iseconfig` and `isedata` , particularly `isedata` to confirm security group tag (SGT) download. See Web Security Appliance CLI Commands for additional information.
- The Web Tracking and Policy Trace functions can be used to debug policy match issues; for example, a user that should be allowed is blocked, and vice versa. See Policy Troubleshooting Tool: Policy Trace, on page 19 for additional information.
- Packet Capture, on page 27 if Working With Support , on page 29.

- For checking certificate status, you can use the openssl Online Certificate Status Protocol (ocsp) utility, available from https://www.openssl.org/ .

ISE Server Connection Issues

Certificate Issues

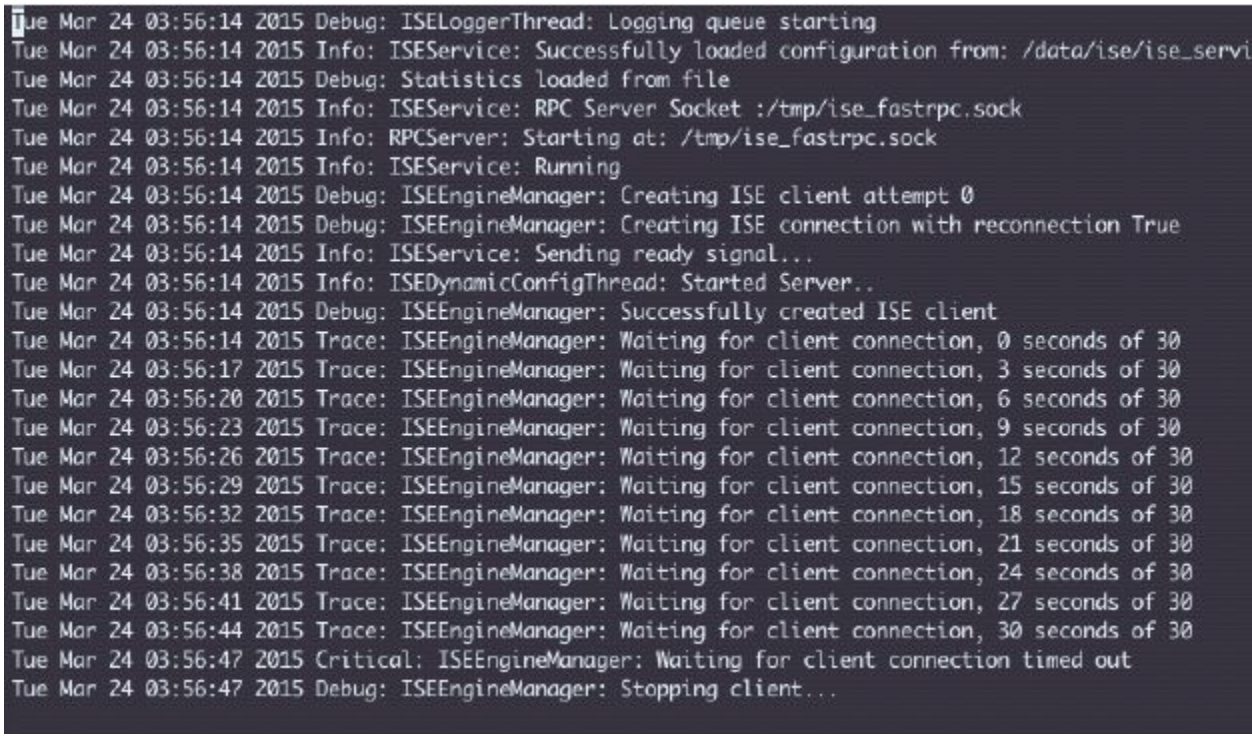
The Web Security Appliance and the ISE server(s) use certificates to mutually authenticate for successful connection. Thus, each certificate presented by one entity should be recognizable by other. For example, if the Web Security Appliance 's Client certificate is self-signed, the same certificate must be present in the trusted certificates list on the appropriate ISE server(s). Correspondingly, if the Web Appliance Client certificate is CA-signed, then the CA root certificate must be present on the appropriate ISE server(s). Similar requirements apply to the ISE server-related Admin and pxGrid certificates.

Certificate requirements and installation are described in Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service. If you encounter certificate-related issues, check the following:

- If using CA-signed certificates:
  - Verify that the root CA signing certificate(s) for the Admin and pxGrid certificates are present on the Web Security Appliance .
  - Verify that the root CA signing certificate for the Web Appliance Client certificate is present in the trusted-certificates list on the ISE server.
- If using self-signed certificates:
  - Verify that the Web Appliance Client certificate—generated on the Web Security Appliance and downloaded—has been uploaded to the ISE server and is present in the ISE servers trusted-certificates list.
  - Verify that the ISE Admin and pxGrid certificates—generated on the ISE server and downloaded—have been uploaded to the Web Security Appliance are present in the its certificate list.
- Expired certificates:
  - Confirm that certificates which were valid when uploaded have not expired.

Log Output Indicating Certificate Issue

The following ISE-service log snippet shows a client-connection timeout due to a missing or invalid certificate.



These Trace-level log entries on the Web Security Appliance show that after 30 seconds the attempts to connect to the ISE server are terminated.

Network Issues

If connection to the ISE server fails during the Start Test on the Identity Services Engine page (Connect to the ISE/ISE-PIC Services), check connectivity to the configured ISE server on ports 443 and 5222.

Port 5222 is the official client-to-server Extensible Messaging and Presence Protocol (XMPP) port, and is used for connection to the ISE server; it is also used by applications such as Jabber and Google Talk. Note that some firewalls are configured to block port 5222.

Tools that can be used to check connectivity include `tcpdump`

Other ISE Server Connectivity Issues

The following issues can cause failure when the Web Security Appliance attempts to connect with the ISE server:

- Licenses on the ISE server have expired.
- The pxGrid node status is “not connected” on the ISE server’s Administration > pxGrid Services page. Be sure Enable Auto-Registration is selected on this page.
- Outdated Web Security Appliance clients (specifically “test_client” or “pxgrid_client”) are present on the ISE server. These need to be deleted; see Administration > pxGrid Services > Clients on the ISE server.
- The Web Security Appliance is attempting to connect to the ISE server before all its services are up and running.

Some changes on the ISE server, such as certificate updates, require the ISE server or services running on it to restart. Any attempt to connect to the ISE server during this time will fail; however, eventually the connection will succeed.

ISE-related Critical Log Messages

This section contains explanations for ISE-related critical Log messages on the Web Security Appliance :

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out`

  The Web Security Appliance 's ISE process failed to connect to the ISE server for 30 seconds.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: WSA Client cert/key missing. Please check ISE config`

  The Web Appliance Client certificate and key were not uploaded or generated on the Web Security Appliance 's Identity Service Engine configuration page.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: ISE service exceeded maximum allowable disconnect duration with ISE server`

  The Web Security Appliance 's ISE process could not connect to the ISE server for 120 seconds and exited.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Subscription to updates failed ...`

  The Web Security Appliance 's ISE process could not subscribe to the ISE server for updates.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Could not create ISE client: ...`

  Internal error when creating the Web Security Appliance 's ISE client for ISE server connection.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Bulk Download thread failed: ...`

  Internal error indicating bulk download of SGTs failed on connection or re-connection.

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to start service. Error: ...`

  The Web Security Appliance 's ISE service failed to start.

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send ready signal ...`

  The Web Security Appliance 's ISE service was unable to send a ready signal to heimdall .

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send restart signal ...`

  The Web Security Appliance 's ISE service was unable to send a restart signal to heimdall .

Problems with Custom and External URL Categories

- Issues Downloading An External Live Feed File, on page 15
- MIME Type Issue on IIS Server for .CSV Files, on page 15
- Malformed Feed File Following Copy and Paste, on page 16

Issues Downloading An External Live Feed File

When Creating and Editing Custom and External URL Categories and providing an **External Live Feed** file (either **Cisco Feed Format** or **Office 365 Feed Format**), you must click the **Get File** button to initiate connection to the specified server, and download and parsing of the file. Progress and results of this process are displayed; if errors occur they are described. Rectify the problems and try downloading the file again.

There are four types of possible error:

- Connect exceptions

  `Failed to resolve server hostname` – the URL provided as the feed-file location is invalid; provide a correct URL to resolve this issue.

- Protocol errors

  `Authentication failed due to invalid credentials` – Server authentication failed; provide the correct user name and passphrase for server connection.

  `The requested file is not found on the server` – The URL provided for the feed file points to an invalid resource. Ensure the correct file is available on the specified server.

- Content validation errors

  `Failed to validate the content of the field` – The content of the feed file is invalid.

- Parsing errors

  - The Cisco Feed Format .csv file must contain one or more entries, where each entry is a site address or a valid regex string, followed by a comma and then the addresstype (which can be either `site` or `regex`). If this convention is not followed for any entry in the feed file, a parsing error is thrown.

    Also, do not include `http://` or `https://` as part of any `site` entry in the file, or an error will occur. In other words, `www.example.com` is parsed correctly, while `http://www.example.com` produces an error.

  - The XML feed file obtained from a Microsoft server is parsed by a standard XML parser. Any inconsistencies in the XML tagging are also flagged as parsing errors.

  The line number of a parsing error is included in the log. For example:

  `Line 8: 'www.anyurl.com' - Line is missing address or address-type field.` Line 8 in the feed file doesn't include a valid address or regex pattern, or an addresstype.

  `Line 12: 'www.test.com' - Unknown address type.` Line 12 has a invalid addresstype; the addresstype can be either `site` or `regex`.

MIME Type Issue on IIS Server for .CSV Files

When providing a .csv file for the **External Live Feed Category** > **Cisco Feed Format** option while Creating and Editing Custom and External URL Categories, you may encounter a "406 not acceptable" error when fetching the file if the Cisco Feed Format server is running Internet Information Services (IIS) version 7 or 8 software. Similarly, the `feedsd` log will report something like: `31 May 2016 16:47:22 (GMT +0200) Warning: Protocol Error: 'HTTP error while fetching file from the server'.`

This is because the default MIME type for .csv files on IIS is `application/csv` rather than `text/csv`. You can remedy the problem by logging into the IIS server and editing the MIME type entry for .csv files to be `text/csv`.

Malformed Feed File Following Copy and Paste

If you copy and paste the contents of a .csv (text) feed file from a UNIX or OS X system to a Windows system, an extra carriage return (`\r`) is added automatically and this can make the feed file malformed.

If you manually create the .csv file, or if you transfer the file from a UNIX or OS X system to a Windows server using SCP, FTP, or POST, there should be no problem.

Logging Problems

- Custom URL Categories Not Appearing in Access Log Entries, on page 16
- Logging HTTPS Transactions, on page 16
- Alert: Unable to Maintain the Rate of Data Being Generated, on page 16
- Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs, on page 17

Custom URL Categories Not Appearing in Access Log Entries

When a web access policy group has a custom URL category set to Monitor and some other component, such as the Web Reputation Filters or the DVS engine, makes the final decision to allow or block a request for a URL in the custom URL category, then the access log entry for the request shows the predefined URL category instead of the custom URL category.

Logging HTTPS Transactions

HTTPS transactions in the access logs appear similar to HTTP transactions, but with slightly different characteristics. What gets logged depends on whether the transaction was explicitly sent or transparently redirected to the HTTPS Proxy:

- **TUNNEL.** This gets written to the access log when the HTTPS request was transparently redirected to the HTTPS Proxy.
- **CONNECT.** This gets written to the access log when the HTTPS request was explicitly sent to the HTTPS Proxy.

When HTTPS traffic is decrypted, the access logs contain two entries for a transaction:

- TUNNEL or CONNECT depending on the type of request processed.
- The HTTP Method and the decrypted URL. For example, “GET https://ftp.example.com”.

The full URL is only visible when the HTTPS Proxy decrypts the traffic.

Alert: Unable to Maintain the Rate of Data Being Generated

AsyncOS for Web sends a critical email message to the configured alert recipients when the internal logging process drops web transaction events due to a full buffer.

By default, when the Web Proxy experiences a very high load, the internal logging process buffers events to record them later when the Web Proxy load decreases. When the logging buffer fills completely, the Web Proxy continues to process traffic, but the logging process does not record some events in the access logs or in the Web Tracking report. This might occur during a spike in web traffic.

However, a full logging buffer might also occur when the appliance is over capacity for a sustained period of time. AsyncOS for Web continues to send the critical email messages every few minutes until the logging process is no longer dropping data.

The critical message contains the following text:

```
Reporting Client: The reporting system is unable to maintain the rate of data being generated.
Any new data generated will be lost.
```

If AsyncOS for Web sends this critical message continuously or frequently, the appliance might be over capacity. Contact Cisco Customer Support to verify whether or not you need additional Web Security Appliance capacity.

Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs

If you want to use a third party log analyzer tool to read and parse the W3C access logs, you might need to include the “timestamp” field. The timestamp W3C field displays time since the UNIX epoch, and most log analyzers only understand time in this format.

Policy Problems

- Access Policy not Configurable for HTTPS, on page 17
- Blocked Object Problems, on page 4
- Identification Profile Disappeared from Policy, on page 18
- Policy Match Failures, on page 18
- Policy Troubleshooting Tool: Policy Trace, on page 19
- Also see: Accessing HTTPS Sites Using Routing Policies with URL Category Criteria, on page 9

Access Policy not Configurable for HTTPS

With the HTTPS Proxy is enabled, Decryption Policies handle all HTTPS policy decisions. You can no longer define Access and Routing Policy group membership by HTTPS, nor can you configure Access Policies to block HTTPS transactions.

If some Access and Routing Policy group memberships are defined by HTTPS and if some Access Policies block HTTPS, then when you enable the HTTPS Proxy, those Access and Routing Policy groups become disabled. You can choose to enable the policies at any time, but all HTTPS related configurations are removed.

Blocked Object Problems

- Some Microsoft Office Files Not Blocked, on page 4
- Blocking DOS Executable Object Types Blocks Updates for Windows OneCare, on page 5

Some Microsoft Office Files Not Blocked

When you block Microsoft Office files in the Block Object Type section, it is possible that some Microsoft Office files will not be blocked.

If you need to block all Microsoft Office files, add **application/x-ole** in the Block Custom MIME Types field. However, blocking this custom MIME type also blocks all Microsoft Compound Object format types, such as Visio files and some third-party applications.

Blocking DOS Executable Object Types Blocks Updates for Windows OneCare

When you configure the Web Security Appliance to block DOS executable object types, the appliance also blocks updates for Windows OneCare.

Identification Profile Disappeared from Policy

Disabling an Identification Profile removes it from associated policies. Verify that the Identification Profile is enabled and then add it to the policy again.

Policy Match Failures

- Policy is Never Applied, on page 18
- HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 18
- User Matches Global Policy for HTTPS and FTP over HTTP Requests, on page 19
- User Assigned Incorrect Access Policy , on page 19

Policy is Never Applied

If multiple Identification Profiles have identical criteria, AsyncOS assigns the transactions to the first Identification Profile that matches. Therefore, transactions never match the additional, identical Identification Profiles, and any policies that apply to those subsequent, identical Identification Profiles are never matched or applied.

HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication

Configure the appliance to use IP addresses as the surrogate when credential encryption is enabled.

When credential encryption is enabled and configured to use cookies as the surrogate type, authentication does not work with HTTPS or FTP over HTTP requests. This is because the Web Proxy redirects clients to the Web Proxy itself for authentication using an HTTPS connection if credential encryption is enabled. After successful authentication, the Web Proxy redirects clients back to the original website. In order to continue to identify the user, the Web Proxy must use a surrogate (either the IP address or a cookie). However, using a cookie to track users results in the following behavior if requests use HTTPS or FTP over HTTP:

- **HTTPS.** The Web Proxy must resolve the user identity before assigning a Decryption Policy (and therefore, decrypt the transaction), but it cannot obtain the cookie to identify the user unless it decrypts the transaction.
- **FTP over HTTP.** The dilemma with accessing FTP servers using FTP over HTTP is similar to accessing HTTPS sites. The Web Proxy must resolve the user identity before assigning an Access Policy, but it cannot set the cookie from the FTP transaction.

Therefore, HTTPS and FTP over HTTP requests will match only Access Policies that do not require authentication. Typically, they match the global Access Policy because it never requires authentication.

User Matches Global Policy for HTTPS and FTP over HTTP Requests

When the appliance uses cookie-based authentication, the Web Proxy does not get cookie information from clients for HTTPS and FTP over HTTP requests. Therefore, it cannot get the user name from the cookie.

HTTPS and FTP over HTTP requests still match the Identification Profile according to the other membership criteria, but the Web Proxy does not prompt clients for authentication even if the Identification Profile requires authentication. Instead, the Web Proxy sets the user name to NULL and considers the user as unauthenticated.

Then, when the unauthenticated request is evaluated against a policy, it matches only a policy that specifies "All Identities" and apply to "All Users." Typically, this is the global policy, such as the global Access Policy.

User Assigned Incorrect Access Policy

- Clients on your network use Network Connectivity Status Indicator (NCSI)
- Web Security Appliance uses NTLMSSP authentication.
- Identification Profile uses IP based surrogates

A user might be identified using the machine credentials instead of the user's own credentials, and as a result, might be assigned to an incorrect Access Policy.

Workaround:

Reduce the surrogate timeout value for machine credentials.

Procedure

Step 1 Use the `advancedproxyconfig > authentication` CLI command.

Step 2 Enter the surrogate timeout for machine credentials.

Policy Trace Mismatch after Modifying Policy Parameters

When you modify policy parameters such as Access Policy, Identification Profiles and Users, Select One or More Identification Profiles, or Selected Groups and Users, the changes will take a few minutes to take effect.

Policy Troubleshooting Tool: Policy Trace

- About the Policy Trace Tool, on page 20
- Tracing Client Requests, on page 20
- Advanced: Request Details, on page 21
- Advanced: Response Detail Overrides, on page 22

About the Policy Trace Tool

The Policy Trace Tool can emulate a client request and then detail how the Web Proxy processes that request. It can be used to trace client requests and debug policy processing when troubleshooting Web Proxy issues. You can perform a basic trace, or you can enter advanced trace settings and override options.

Note When you use the Policy Trace tool, the Web Proxy does not record the requests in the access log or reporting database.

The Policy Trace tool evaluates requests against polices used by the Web Proxy only. These are Access, Encrypted HTTPS Management, Routing, Data Security, and Outbound Malware Scanning polices.

Note SOCKS and External DLP polices are not evaluated by the Policy Trace tool.

Tracing Client Requests

Note You can use the CLI command `maxhttpheadersize` to change the maximum HTTP header size for proxy requests. Increasing this value can alleviate Policy Trace failures that can occur when the specified user belongs to a large number of authentication groups, or when the response header is larger than the current maximum header size. See Web Security Appliance CLI Commands for more information about this command.

Procedure

Step 1 Choose **System Administration > Policy Trace**.

Step 2 Enter the URL you wish to trace to in the Destination URL field.

Step 3 (Optional) Enter additional emulation parameters:

To emulate...	Enter...
The client source IP used to make the request.	An IP address in the Client IP Address field. **Note** If an IP address is not specified, AsyncOS uses localhost. Also, SGTs (security group tags) cannot be fetched and policies based on SGTs will not be matched.
The authentication/identification credentials used to make the request.	A user name in the User Name field, and then choose Identity Services Engine or an authentication realm from the Authentication/Identification drop-down list. **Note** Only enabled option(s) are available. That is, authentication options and the ISE option are available only if they are both enabled. For authentication of the user you enter here, the user must have already successfully authenticated through the Web Security Appliance .

Step 4 Click **Find Policy Match.**

The Policy Trace output is displayed in the Results pane.

Note
For a Pass Through HTTPS transaction, the Policy Trace tool bypasses further scanning and no Access policy is associated with the transaction. Similarly, for a Decrypt HTTPS transaction, the tool cannot actually decrypt the transaction to determine the applied Access policy. In both cases, as well as for Drop transactions, the trace results display: “Access policy: Not Applicable.”

Note
If the client IP address provided is not routable, the trace results display: "Connection Trace: Connection to Origin Server: Failed".

What to do next

Related Topics

- Advanced: Request Details, on page 21
- Advanced: Response Detail Overrides, on page 22

Advanced: Request Details

You can use the settings in the Request Details pane of the Policy Trace page, Advanced section, to tune the outbound malware scan request for this policy trace.

Procedure

Step 1 Expand the **Advanced** section on the Policy Trace page.

Step 2 Complete the fields in the Request Details pane as required:

Setting	Description
Proxy Port	Select a specific proxy port to use for the trace request to test policy membership based on proxy port.
User Agent	Specify the User Agent to simulate in the request.
Time of Request	Specify the Date and Time of day to simulate in the request.
Upload File	Choose a local file to simulate uploading in the request. When you specify a file to upload here, the Web Proxy simulates an HTTP POST request instead of a GET request.
Object Size	Enter the size of the request object in bytes. You can enter K, M, or G to represent Kilobytes, Megabytes, or Gigabytes.
MIME Type	Enter the MIME type.

Setting	Description
Anti-malware Scanning Verdicts	To override a Webroot, McAfee, or Sophos scanning verdict, choose the specific type of verdict to be overridden.

Step 3 Click **Find Policy Match.**

The Policy Trace output is displayed in the Results pane.

Advanced: Response Detail Overrides

You can use the settings in the Response Detail Overrides pane of the Policy Trace page, Advanced section, to “tweak” aspects of the Web Access Policies response for this trace.

Procedure

Step 1 Expand the **Advanced** section on the Policy Trace page.

Step 2 Complete the fields in the Response Detail Overrides pane as required:

Setting	Description
URL Category	Use this setting to override the URL transaction category of the trace response. Choose a category which is to replace the URL category in the response results.
Application	Similarly, use this setting to override the application category of the trace response. Choose a category which is to replace the application category in the response results.
Object Size	Enter a size for the response object in bytes. You can enter K, M, or G to represent Kilobytes, Megabytes, or Gigabytes.
MIME Type	Enter a MIME type.
Web Reputation Score	Enter a web reputation score from -10.0 to 10.0. The web reputation score -100 means 'No Score.'
Anti-malware Scanning Verdicts	Use these options to override specific anti-malware scanning verdicts provided in the trace response. Choose verdicts which are to replace the Webroot, McAfee, and Sophos scanning verdicts in the response results.

Step 3 Click **Find Policy Match.**

The Policy Trace output is displayed in the Results pane.

Problems with File Reputation and File Analysis

See Troubleshooting File Reputation and Analysis

Reboot Issues

• Virtual Appliance Running on KVM Hangs on Reboot , on page 23
• Hardware Appliances: Remotely Resetting Appliance Power , on page 23

Virtual Appliance Running on KVM Hangs on Reboot

Note This is a KVM issue and may change at any time.

For more information, see https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html and https://bugs.launchpad.net/qemu/+bug/1329956.

Procedure

Step 1 Check the following:

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

Step 2 If the above value is set to Y:

a) Stop your virtual appliances and reinstall the KVM kernel module:

```
rmmod kvm_intel  modprobe kvm_intel enable_apicv=N
```

b) Restart your virtual appliance.

Hardware Appliances: Remotely Resetting Appliance Power

Before you begin

- Obtain and set up a utility that can manage devices using IPMI version 2.0.
- Understand how to use the supported IPMI commands. See the documentation for your IPMI tool.

If a hardware appliance requires a hard reset, you can reboot the appliance chassis remotely using a third-party Intelligent Platform Management Interface (IPMI) tool.

Restrictions

- Remote power cycling is available only on certain hardware. For specifics, see Enabling Remote Power Cycling.
- If you want be able to use this feature, you must enable it in advance, before you need to use it. For details, see Enabling Remote Power Cycling.
- Only the following IPMI commands are supported: status, on, off, cycle, reset, diag, soft. Issuing unsupported commands will produce an “insufficient privileges” error.

Procedure

Step 1 Use IPMI to issue a supported power-cycling command to the IP address assigned to the Remote Power Cycle port, which you configured earlier, along with the required credentials.

For example, from a UNIX-type machine with IPMI support, you might issue the command:

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

For S195, S395, and S695 models, use :

```
ipmitool -I lanplus -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

where `192.0.2.1` is the IP address assigned to the Remote Power Cycle port and remoteresetuser and passphrase are the credentials that you entered while enabling this feature.

Step 2 Wait at least eleven minutes for the appliance to reboot.

Site Access Problems

- Cannot Access URLs that Do Not Support Authentication, on page 24
- Cannot Access Sites With POST Requests , on page 25
- Also see: Bypassing Decryption for Particular Websites, on page 10

Cannot Access URLs that Do Not Support Authentication

This is a partial list of applications cannot be used when the Web Security Appliance is deployed in transparent mode because they do not support authentication.

- Mozilla Thunderbird
- Adobe Acrobat Updates
- HttpBridge
- Subversion, by CollabNet
- Microsoft Windows Update
- Microsoft Visual Studio

Workaround: Create a class of user for the URL that does not require authentication.

Related Topics

- Bypassing Authentication

Cannot Access Sites With POST Requests

When the user's first client request is a POST request and the user still needs to authenticate, the POST body content is lost. This might be a problem when the POST request is for a application with the Access Control single sign-on feature in use.

Workarounds:

- Have users first authenticate with the Web Proxy by requesting a different URL through the browser before connecting to a URL that uses POST as a first request.
- Bypass authentication for URLs that use POST as a first request.

Note When working with Access Control, you can bypass authentication for the Assertion Consumer Service (ACS) URL configured in the Application Authentication Policy.

Related Topics

- Bypassing Authentication.

Upstream Proxy Problems

- Upstream Proxy Does Not Receive Basic Credentials, on page 25
- Client Requests Fail Upstream Proxy, on page 25

Upstream Proxy Does Not Receive Basic Credentials

If both the appliance and the upstream proxy use authentication with NTLMSSP, depending on the configurations, the appliance and upstream proxy might engage in an infinite loop of requesting authentication credentials. For example, if the upstream proxy requires Basic authentication, but the appliance requires NTLMSSP authentication, then the appliance can never successfully pass Basic credentials to the upstream proxy. This is due to limitations in authentication protocols.

Client Requests Fail Upstream Proxy

Configuration:

- Web Security Appliance and upstream proxy server use Basic authentication.
- Credential Encryption is enabled on the downstream Web Security Appliance .

Client requests fail on the upstream proxy because the Web Proxy receives an "Authorization" HTTP header from clients, but the upstream proxy server requires a "Proxy-Authorization" HTTP header.

Unable to Route FTP Requests Via an Upstream Proxy

If your network contains an upstream proxy that does not support FTP connections, then you must create a Routing Policy that applies to all Identities and to just FTP requests. Configure that Routing Policy to directly connect to FTP servers or to connect to a proxy group whose proxies all support FTP connections.

Virtual Appliances

- Do Not Use Force Reset, Power Off, or Reset Options During AsyncOS Startup , on page 26
- Network Connectivity on KVM Deployments Works Initially, Then Fails , on page 26
- Slow Performance, Watchdog Issues, and High CPU Usage on KVM Deployments , on page 26
- General Troubleshooting for Virtual Appliances Running on Linux Hosts , on page 26

Do Not Use Force Reset, Power Off, or Reset Options During AsyncOS Startup

The following actions on your virtual host are the equivalent of pulling the plug on a hardware appliance and are not supported, especially during AsyncOS startup:

- In KVM, the Force Reset option.
- In VMWare, the Power Off and Reset options. (These options are safe to use after the appliance has come up completely.)

Network Connectivity on KVM Deployments Works Initially, Then Fails

Problem

Network connectivity is lost after previously working.

Solution

This is a KVM issue. See the section on "KVM: Network connectivity works initially, then fails" in the OpenStack documentation at
http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html

Slow Performance, Watchdog Issues, and High CPU Usage on KVM Deployments

Problem

Appliance performance is slow, watchdog issues occur, and the appliance shows unusually high CPU usage when running on an Ubuntu virtual machine.

Solution

Install the latest Host OS updates from Ubuntu.

General Troubleshooting for Virtual Appliances Running on Linux Hosts

Problem

Issues with virtual appliances running on KVM deployments may be related to host OS configuration issues.

Solution

See the troubleshooting section and other information in the *Virtualization Deployment and Administration Guide* available from:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf.

WCCP Problems

• Maximum Port Entries, on page 27

Maximum Port Entries

In deployments using WCCP, the maximum number of port entries is 30 for HTTP, HTTPS , and FTP ports combined.

Packet Capture

• Starting a Packet Capture, on page 27
• Managing Packet Capture Files, on page 28

The appliance provides the ability to capture and display TCP/IP and other packets being transmitted or received over the network to which the appliance is attached.

Note The packet capture feature is similar to the Unix tcpdump command.

Web Security Appliance does not support packet capture for the NIC paired interfaces. The packet capture will be applied only for the active interface. For example, if both P1 and P2 are paired, both P1 and P2 will not be configured in the user interface or the CLI.

Starting a Packet Capture

Procedure

Step 1 Choose **Support and Help > Packet Capture**.

Step 2 (Optional) Click **Edit Settings** to change the packet capture settings.

Option	Description
Capture File Size Limit	Specifies the maximum size that the capture file can reach. One the limit is reached, the data will be discarded and a new file started, unless the Capture Duration setting is 'Run Capture Until File Size Limit Reached.'
Capture Duration	Options for if and when the capture automatically stops. Choose from: • **Run Capture Until File Size Limit Reached**. The capture runs until the file limit set above is reached. • **Run Capture Until Time Elapsed Reaches.** The capture runs for a specified duration. If you enter the amount of time without specifying the units, AsyncOS uses seconds by default. • **Run Capture Indefinitely.** The packet capture runs until you manually stop it. **Note** The capture can be ended manually at any time.
Interfaces	The interfaces from which traffic will be captured.
Filters	The filtering options to apply when capturing packets. Filtering allows you to capture required packets only. Choose from: • **No Filters.** All packets will be captured. • **Predefined Filters.** The predefined filters provide filtering by port and/or IP addresses. If left blank, all traffic will be captured. • **Custom Filter.** Use this option if you already know the exact syntax of the packet capture options that you need. Use standard tcpdump syntax.

(Optional) Submit and commit your packet capture changes.

Note
When you change the packet capture settings without committing the changes and then start a packet capture, AsyncOS uses the new settings. This allows you to use the new settings in the current session without enforcing the settings for future packet capture runs. The settings remain in effect until you clear them.

Step 3 Click **Start Capture**. To manually stop a running capture, click **Stop Capture**.

Managing Packet Capture Files

The appliance saves the captured packet activity to a file and stores the file locally. You can send packet capture files using FTP to Cisco Customer Support for debugging and troubleshooting purposes.

• Downloading or Deleting Packet Capture Files, on page 28

Downloading or Deleting Packet Capture Files

Note You can also connect to the appliance using FTP and retrieving packet capture files from the captures directory.

Procedure

Step 1 Choose **Support and Help > Packet Capture**.

Step 2 Select the packet capture file you wish to use from the Manage Packet Capture Files pane. If this pane is not visible then no packet capture files have been stored on the appliance.

Step 3 Click **Download File** or **Delete Selected Files** as required.

Working With Support

- Gathering Information for Efficient Service , on page 29
- Opening a Technical Support Request, on page 29
- Getting Support for Virtual Appliances , on page 30
- Enabling Remote Access to the Appliance , on page 30

Gathering Information for Efficient Service

Before contacting Support:

- Enable custom logging fields as described in General Troubleshooting Best Practices, on page 1.
- Consider doing a packet capture. See Packet Capture, on page 27.

Opening a Technical Support Request

Before you begin

- Verify that your Cisco.com user ID is associated with your service agreement contract for this appliance. To view a list of service contracts that are currently associated with your Cisco.com profile, visit the Cisco.com Profile Manager at https://sso.cisco.com/autho/forms/CDClogin.html. If you do not have a Cisco.com user ID, register to get one.

You can use the appliance to send a non-urgent request for assistance to Cisco Customer Support. When the appliance sends the request, it also sends the configuration of the appliance. The appliance must be able to send mail to the Internet to send a support request.

Note If you have an urgent issue, please call a Cisco Worldwide Support Center.

Procedure

Step 1 Choose **Support And Help > Contact Technical Support**.

Step 2 (Optional) Choose additional recipients for the request. By default, the support request and configuration file is sent to Cisco Customer Support.

Step 3 Enter your contact information.

Step 4 Enter the issue details.

- If you have a customer support ticket already for this issue, enter it.

Step 5 Click **Send**. A trouble ticket is created with Cisco.

Getting Support for Virtual Appliances

If you file a support case for a Cisco content security virtual appliance, you must provide your Virtual License Number (VLN), your contract number, and your Product Identifier code (PID).

You can identify your PID based on the software licenses running on your virtual appliance, by referencing your purchase order, or from the following table:

Functionality	PID	Description
Web Security Essentials	WSA-WSE-LIC=	Includes: • Web Usage Controls • Web Reputation
Web Security Premium	WSA-WSP-LIC=	Includes: • Web Usage Controls • Web Reputation • Sophos and Webroot Anti-Malware signatures
Web Security Anti-Malware	WSA-WSM-LIC=	Includes Sophos and Webroot Anti-Malware signatures
McAfee Anti-Malware	WSA-AMM-LIC=	—
Advanced Malware Protection	WSA-AMP-LIC=	—

Enabling Remote Access to the Appliance

The Remote Access option allows Cisco Customer Support to remotely access your appliance for support purposes.

Procedure

Step 1 Choose **Support And Help > Remote Access**.

Step 2 Click **Enable**.

Step 3 Complete the Customer Support Remote Access options:

Option	Description
Seed String	If you enter a string, the string should not match any existing or future pass phrase. The string will appear near the top of the page after you click Submit. You will give this string to your support representative.
Secure Tunnel (recommended)	Specifies whether or not to use a secure tunnel for remote access connections. When enabled, the appliance creates an SSH tunnel over the specified port to the server upgrades.ironport.com, over port 443 (by default). Once a connection is made, Cisco Customer Support is able to use the SSH tunnel to obtain access to the appliance. Once the techsupport tunnel is enabled, it will remain connected to upgrades.ironport.com for 7 days. After 7 days, no new connections can be made using the techsupport tunnel, though any existing connections will continue to exist and work. The Remote Access account will remain active until specifically deactivated.
Appliance Serial Number	The serial number of the appliance.

Step 4 Submit and commit your changes.

Step 5 Look for the seed string in the Success message near the top of the page and make a note of it.

For security reasons, this string is not stored on the appliance and there is no way to locate this string later.

Keep this seed string in a safe place.

Step 6 Give the seed string to your Support representative.

Troubleshooting