Blue Touch Essential™

How to Monitor and Manage Your Blue Coat ProxySG Environment

Version 2.0

Table of Contents

Introduction

This document is intended to assist in properly configuring your proxy device to have the highest probability of capturing the appropriate troubleshooting data in the event that a problem should occur.

Proper configuration of the device ahead of time and gathering the appropriate data in a timely manner increases the probability of determining root cause of a problem. The outlined proactive and reactive procedures are key in minimizing business impacting downtime.

This document will guide you through the recommended configuration and provides step-by-step procedures for collecting data in the event you should experience problems with the device.

Blue Touch Online

Blue Touch Online is the portal for all your support needs including…

- Open Service Requests
- Access the Knowledgebase
- Access Forums
- Read Tech Briefs
- View Field Alerts and Security Advisories
- Downloading the latest SGOS versions and SNMP MIB files
- Licensing
- Documentation

Service Management

Service Requests | Open New SR

Knowledgebase

Access the latest solutions and research technical issues in our product-specific knowledgebases.

Discussion Forums

Collaborate with peers and subject matter experts to answer your support questions. Share knowledge and news about Blue Coat products and related technologies.

Security Advisories

Potential security issues and their impact on Blue Coat products including public reporting of security vulnerability information.

Technical Briefs

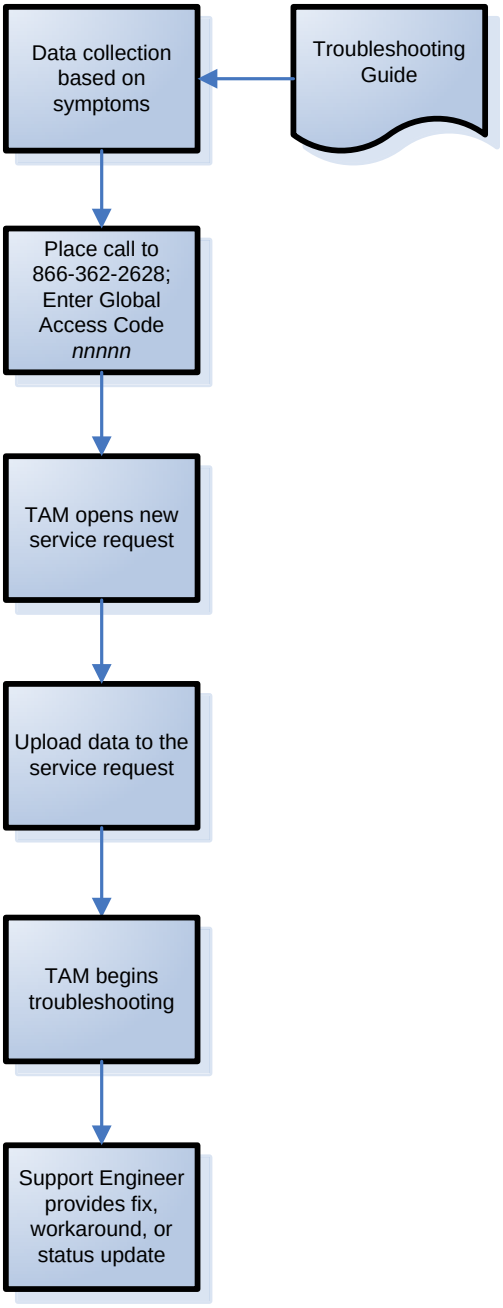
Technical briefs illustrate the features and capabilities of Blue Coat products, providing baseline configurations for common deployment scenarios.

Field Alerts

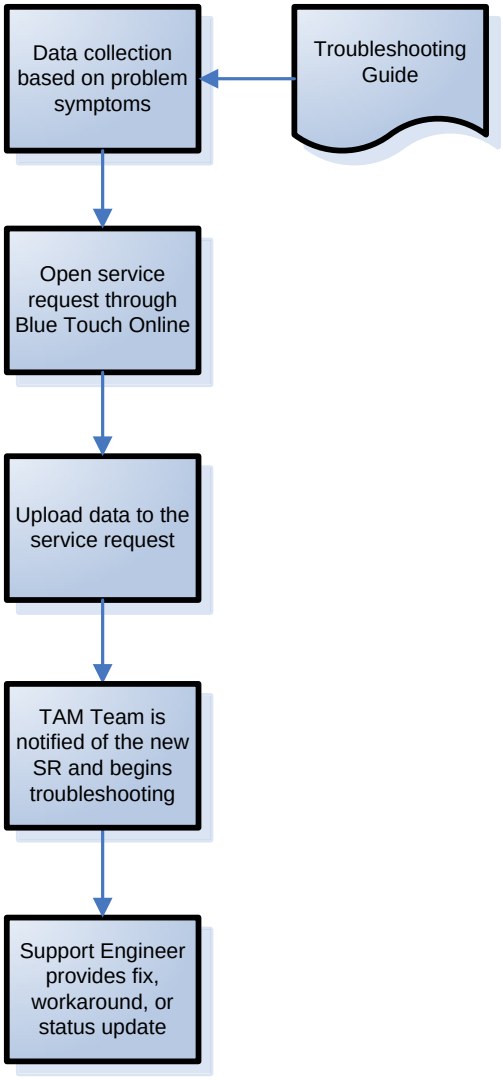
Technical field alerts provide you with information on critical product and software issues

Support Engagement Process

P1 & P2 Requests
Critical and High Priority
Support Required



P3 & P4 Requests
Non-Critical Support Required



ProxySG 101

Common Terms	
SG	Blue Coat ProxySG
OCS	Origin Content Server (web server serving the actual content)
MC	GUI Management Console (https://x.x.x.x: 8082)
CLI	Command Line Interface (accessed via serial cable or SSH)
CPL	Content Policy Language (used for writing policy directly into local or central policy files)
VPM	Virtual Policy Manager (GUI for creating policy launched via "Configuration > Policy > Visual Policy Manager".
PCAP	Packet Capture
x.x.x.x	Variable indicating to place your SG's IP address here

How the ProxySG Works

The ProxySG as a forward proxy sits at the edge of the network and acts as a gateway between the LAN and the internet. The proxy can be deployed as an explicit proxy or a transparent proxy, however, no matter how it is deployed its basic function remains the same and that is to act as an intermediary between devices on the LAN and web servers located on the internet as well as to secure, control and accelerate that traffic.

It's important to understand that the ProxySG intercepts traffic. That means it will terminate the client connection and create a new connection to the OCS through which it will make requests on behalf of the client. The proxy acts as the server to the client and acts as the client to the server. It is the middleman.

Deployment Types

Explicit:
The client is configured to make requests directly to the proxy IP address. In this deployment the client is aware that it is talking to a proxy and will behave accordingly.

Transparent:
The client is unaware of the proxy's presence and believes that it is talking directly to the OCS. Transparency can be accomplished by deploying the proxy "in-line" (in-path) or via WCCP or layer 4 redirection.

Troubleshooting Methodology

1. Clear understanding of the issue
    - **Details, details, details!**
    - When did the issue start?
    - How often does it occur?
    - Is this a new or existing setup and was it ever working?
    - What changed?
        - Network changes (routers, firewall, new switch, etc)
        - Deployment (added subnet, changed to explicit, changed PAC file, etc).
        - Policy changes, configuration changes, etc.
    - How "exactly" does the end user experience the problem?
        - Provide URLs and screen shots of errors where possible
    - How many users are impacted?
    - What applications are involved?
    - What devices are involved?
    - Precise, detailed, step-by-step, duplication steps.
    - What is the impact to production?
2. Check the knowledgebase and forums for answers
    - Access Blue Touch Online: https://bto.bluecoat.com/support
3. Gather the necessary data
    - Data gathering guidelines for most issues are detailed in this document.
    - Verify the optimized setup is in place.
    - Find the issue that relates (same or similar) and follow the instructions for gathering the proper data.
    - If your issue is not covered here follow the "General Data Gathering Guidelines" (located just after the instructions for "Optimized Setup" below).
4. Open an SR and/or contact support
    - If the issue is not critical then use Blue Touch Online to open an SR
    - If the issue is critical then use the instructions for direct telephone access to support

Important Note Concerning Data Gathering:

As a forward proxy is the essentially the networks gateway to the internet it will often have a large amount of traffic passing through it especially during peak production hours. In order to effectively gather data useful for analysis and debugging ***the greatest effort should be made to limit the amount of noise (unrelated data) captured in PCAP's, traces, and logs where possible.*** The SG's logging and capturing features have size limitations that if reached could render the data useless as it will either stop logging/capturing or the data will begin to wrap and overwrite previously captured data. For example a busy proxy on a sizable network has been known to fill its PCAP buffer in as little as 6 seconds and a 6 second PCAP is doubtful to contain any useful information.

Optimized Setup

The Blue Coat ProxySG ships with a default configuration for capturing troubleshooting data such as logs and snapshots that can be made more useful via a few optimizations. Every SG in your organization should run the following basic setup. This setup will be more effective in capturing the data we need to troubleshoot issues the first time the problem happens.

- Configuring the ProxySG parameters

    1. Maintenance > Core Image > full
        a. Apply
    2. CPU Monitor
        a. Management Console
            i. Statistics>Advanced>Diagnostics > Start the CPU Monitor
    3. Snapshots
        a. Maintenance -> Service Information -> Snapshots
            i. Click “New”
            ii. Enter name: “CPU<proxyserialnumber>”
            iii. Highlight the newly created snapshot and click “Edit”
                1. target: /Diagnostics/CPU_Monitor/Statistics/Advanced
                2. interval: 5 (minutes)
                3. Maximum number to store: 100
                4. Check “Enabled” and click “OK”
                5. Apply
            iv. Click “New”
            v. Enter name: “sysinfo_stats5”
            vi. Highlight the newly created snapshot and click “Edit”
                1. target: /sysinfo-stats
                2. interval: 5 (minutes)
                3. Maximum number to store: 100
                4. Check “Enabled” and click “OK”
                5. Apply
            vii. Modify the existing snapshot_sysinfo_stats to store 100 snapshots
                1. Highlight the sysinfo_stats snapshot and click “Edit”
                2. Leave the interval the same.
                3. Maximum number to store: 100
                4. Click “OK”
                5. Apply
        b. Verify that the packet capture filter on the SG is empty. (Maintenance > Service Information > Packet Captures)

General Data Gathering Guidelines

This document is intended to assist in gathering the right data, the right way, the first time. However, it cannot possibly cover every possible scenario. In the event the issue is not specifically covered here or when in doubt use these instructions for gathering data ***in conjunction with*** the optimized setup.

1. Start a policy trace limited to a single IP (see Appendix D)
2. Start a packet capture (see Appendix E)
3. Reproduce the issue as simply and concisely as possible.
4. Stop the packet capture
5. Save the policy trace to your PC using the browsers FILE|SAVE function and save as TEXT.
6. Open an SR (see Appendix A)
7. Upload the following (see Appendix C)
    - Sysinfo
    - Event log
    - Snapshots (all)
    - Packet Capture
    - Policy trace (https://upload.bluecoat.com)

Restart Issues

Overview

Restarts are often able to be solved by Blue Coat code changes, but sometimes restarts can be caused by web servers using poorly written applications or other requests as well as high CPU or high memory pressure. In the majority of cases the cause of a restart will be determined via the analysis of a core file (context, memory, or full core), however it is always vital to gather the other logs and snapshots available on the SG as well.

For more information concerning cores please refer to Appendix F: Cores

Collecting Data for Restart Issues

If the optimized setup has been configured then your SG is already configured properly to write the necessary data we need for restart issues.

- Configuring the ProxySG parameters
    - Full cores take longer to write than do context cores. In some cases all we need is a context, but there are many cases when we need a full core. A full core is always preferred to a context core for proper analysis, however if you don't feel you can afford the downtime it takes to capture a full core then you have the option of changing the setting to write a "context only". It's important to remember, however, that if we can't get the information we need from the context then we will have to set the box up to write a full core and wait for the box to crash a second time in order to gather the information we need.

- Gathering Data
    - The SG will crash and come back up on its own. Before it comes back up the SG will write the core and other files to disk. During the time the SG is writing a core it will be inaccessible. Full cores can take 5-15 minutes to complete depending on the amount of memory, type of hardware, etc.

- Uploading Data to Blue Coat Support

    - Upload the following information
        - sysinfo
        - event log
        - snapshots (all 4 - sysinfo, syinfo_stats, cpu<serial#>, sysinfo_stats5)
        - PCAP
        - full (or memory) core and context

High CPU Conditions

Possible Causes for High CPU Conditions

1. Traffic
    - The SG is undersized for the amount of traffic it is required to process.
    - The SG is getting hammered by malicious traffic (virus or poor application behavior).
    - The SG has been exposed to the internet and is functioning as an “open proxy”.
    - The network is looping requests causing a race condition on the SG.

2. Lack of available resources to process data.
    - Content Filtering Memory Allocation is set incorrectly requiring the use of disk to accomplish policy application tasks thereby increasing the load on the CPU.
    - The SG is experiencing communication issues with an ICAP server or the ICAP server is having issues processing requests which will cause the SG to queue scanning requests thereby decreasing available resources and increasing load on the CPU.
    - The SG is sending inappropriate data to the ICAP server for scanning such as streaming data.
    - Other network related communication problems are causing requests to begin queuing due to slowness thereby increasing load on the CPU.

3. Policy is highly complex or contains a large amount of REGEX resulting in resource intensive processing.

4. Bug.

Collecting Data for High CPU Conditions

1. Configuring the ProxySG parameters
    - In most cases the optimized setup will suffice, however, there may be times when the “interval” of the “CPU monitor” snapshot and the “sysinfo_stats” snapshot needs to be tweaked (increased/decreased) depending on the frequency and duration of the high CPU event.

2. Gathering Data
    - Wait for high CPU
    - Start a PCAP and let run for 30 seconds.
    - Stop and download the PCAP to your PC.
    - Save the sysinfo to your PC (https://x.x.x.x:8082/sysinfo)
    - Force a full core
        - enter the CLI
        - type “restart abrupt”
        - wait for the SG to come back on its own…it will take a little while (5-15 min).

3. Data to upload
    - Upload the following information
        - sysinfo
        - event log
        - snapshots (all 4 - sysinfo, syinfo_stats, cpu<serial#>, sysinfo_stats5)
        - PCAP
        - full core and context

Memory Pressure Conditions

Memory pressure is similar to economics law of supply and demand in that it is a measurement of SG's ability to free (supply) and allocate (demand) memory to requesting processes. If the demand outpaces the supply then memory pressure will rise. It is normal for memory pressure to fluctuate, however in cases where demand outpaces supply perpetually the SG will eventually run out of resources resulting in slowness, hangs, and in some cases restarts.

Memory pressure levels can be monitored via SNMP. The SG also allows warning thresholds to be set (Maintenance > Health Monitoring) and the event log will log "TCP regulation memory pressure" type messages in the event the SG may be experiencing problems with memory pressure.

Collecting Data for Memory Pressure Conditions

1. Configuring the ProxySG parameters
    - In most cases the optimized setup will suffice.

2. Gathering Data
    - Save the sysinfo to your PC (https://x.x.x.x:8082/sysinfo)
    - Force a full core
        i. enter the CLI
        ii. type "restart abrupt"
        iii. wait for the SG to come back on it's own…it will take a little while (10-15 min).

3. Upload via the MC
    - sysinfo
    - event log
    - snapshots (all 4 - sysinfo, syinfo_stats, cpu<serial#>, sysinfo_stats5)
    - full core and context

Slowness Issues

Possible Causes for Slowness Issues

Slowness can be caused by many different issues or a combination of issues. Some things to look at…

- Network problems (dropped packets, routing, firewalls, etc.)
- Speed/duplex mismatch
- DNS (slow response from server, failures, etc.)
- Authentication (large auth policy, not using auth caching, slow auth return, etc)
- Off-box services (AV slow processing or problems communicating, Content Filtering)
- Circuit capacity and speed (Is the pipe saturated?)
- High Memory pressure
- High CPU

Collecting Data for Slowness Issues

1. Configuring the ProxySG parameters
    - In most cases the optimized setup will suffice in conjunction with a ***packet capture***.

2. Gathering Data
    - The data required to analyze a slowness issue may vary depending on whether or not high CPU, high memory pressure, or authentication issues are involved. For example, if the SG is slow and CPU is high, then follow the instructions for gathering data for high CPU as it's possible that the slowness may only be a symptom of the real problem (that which is causing high CPU). An authentication related slowness issue might require a BCAAA debug in conjunction with the packet captures you will take. With any slowness issue packet captures are required.

        i. Start a packet capture on the client and the SG (2 captures are then running simultaneously).
        ii. Duplicate the slowness issue.
        iii. Stop the PCAP on the SG
        iv. Stop the PCAP on the client.

3. Upload via the MC
    - Sysinfo
    - Event log
    - Snapshots (all 4 - sysinfo, syinfo_stats, cpu<serial#>, sysinfo_stats5)
    - Packet capture from the SG
    - Client PCAP (upload via https://upload.bluecoat.com)

Connectivity Issues

Connectivity issues can be tricky to diagnose at first as there may be a number of things actually happening. Sometimes what is first thought to be a failure to communicate to the SG actually turns out to be something unrelated to network communications.

Possible Causes for Connectivity Issues

1. Physical interface on the Proxy
2. Network settings on the Proxy
3. Bad Ethernet cable
4. Bridging
5. Network infrastructure (router/switch)
6. Transparent Redirection (i.e. WCCP)
7. Proxy Hang
8. Proxy Crash

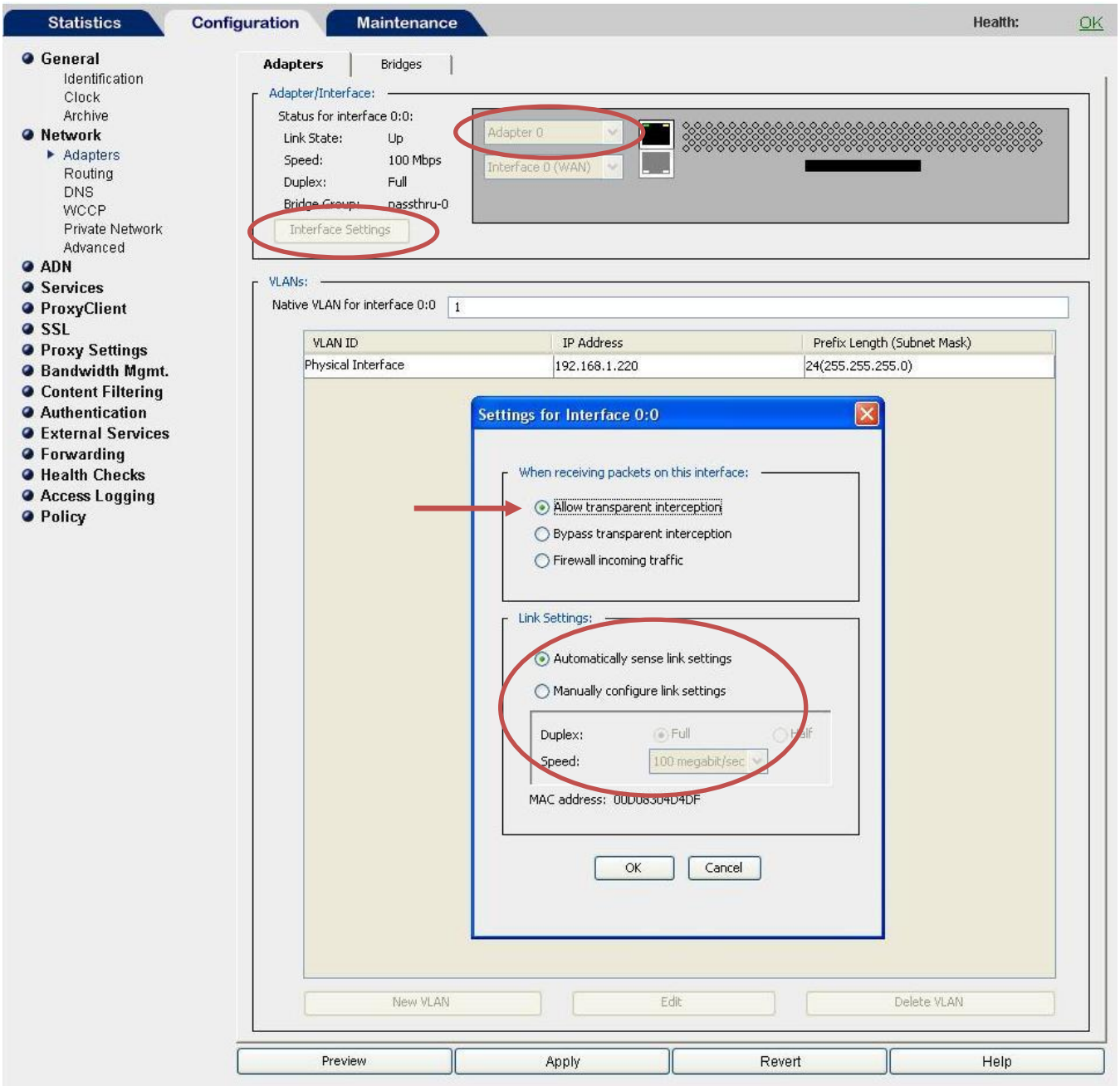
Proxy Network and Interface Settings

In order for the Proxy SG to communicate effectively it must have an active network adaptor (NIC) and properly configured network settings.

1. Verify the Proxy SG adaptor settings
    a. Configuration > Network > Adapters

b. Select the correct interface and check IP address and subnet mask
c. Click “Interface Settings”
    i. Verify speed/duplex
    ii. Verify “Allow transparent interception” on the internal interface. (DO NOT enable transparent interception on public (internet) facing interfaces unless the SG is being used as a reverse proxy.)

2. Verify the adaptor is active
    a. Ping the IP address bound to the interface from the CLI on the SG itself
    b. Check the link light on the adaptor itself
    c. Verify the cable is plugged into the proper adaptor
    d. Verify the cable is good (swap out for known good cable)



Collecting Data for Adaptor issues

1. Sysinfo
2. Event log
3. Snapshots (all)
4. Packet capture taken during the issue
5. Output from: https://x.x.x.x:8082/TCP/Statistics

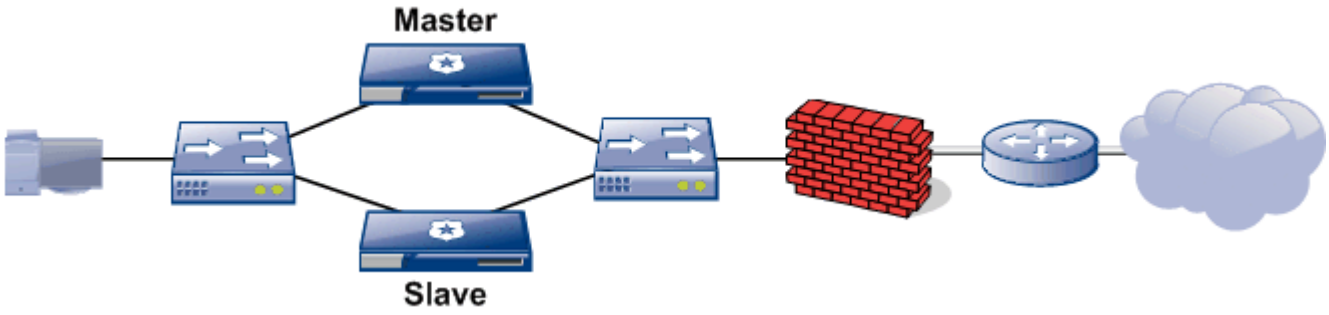
Bridging

The ProxySG provides bridging functionality by two methods:

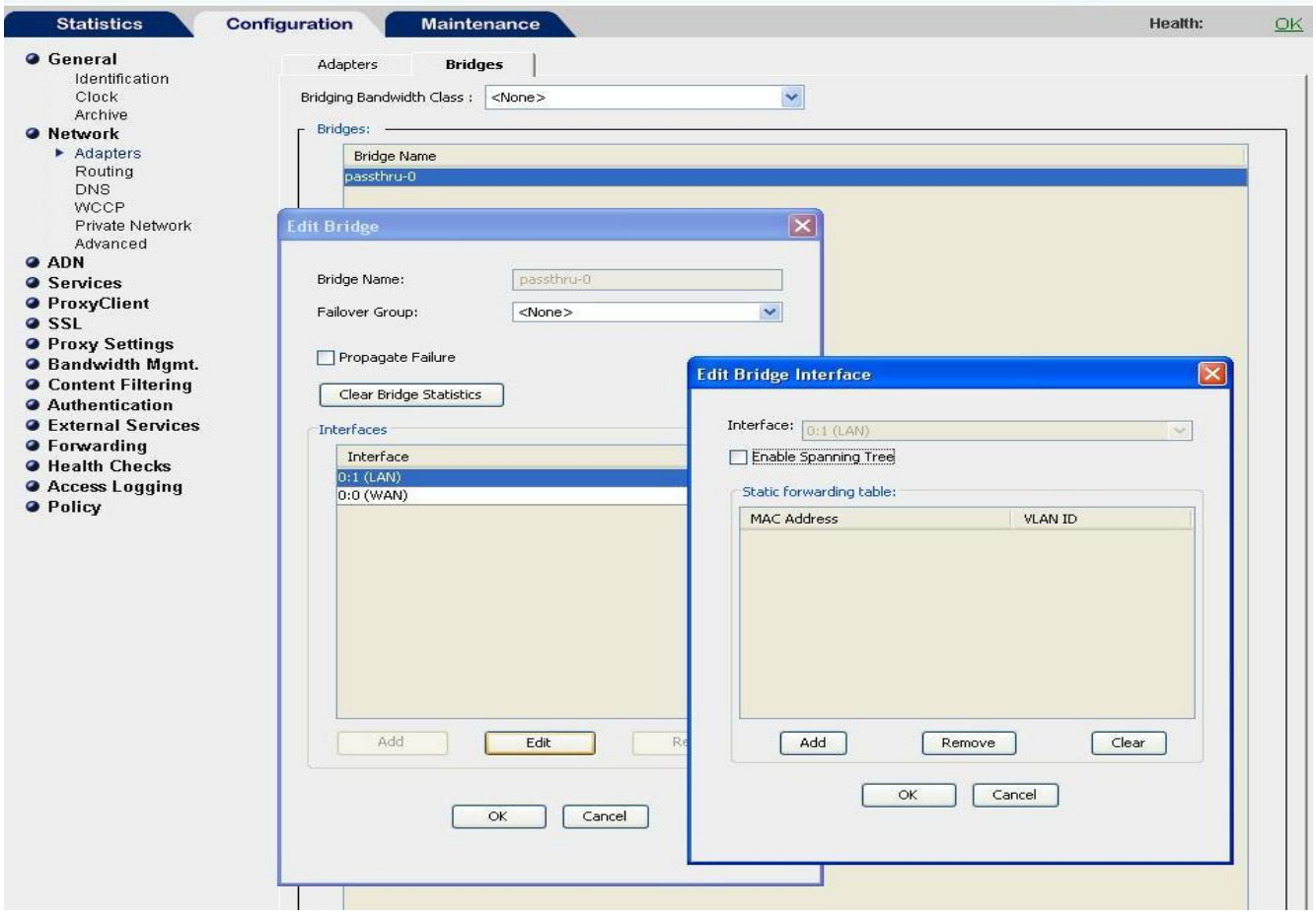
- **Software**: A software, or *dynamic*, bridge is constructed using a set of installed interfaces. Within each logical bridge, interfaces can be assigned or removed.
- **Hardware**: A hardware, or *pass-through*, bridge uses a 10/100 dual interface Ethernet adapter. This type of bridge provides pass-through support.

A *pass-through adapter* is a 10/100 dual interface Ethernet adapter which provides an efficient fault-tolerant bridging solution. If this adapter is installed on a ProxySG, SGOS detects the adapter on system boot and automatically creates a bridge—the two Ethernet interfaces serve as the bridge ports. If the ProxySG is powered down or loses power for any reason, the **bridge fails *open***; that is, traffic passes from one Ethernet interface to the other.

Check to see if the bridge is created and the correct interfaces are associated with it:
Configuration > Network > Adaptors > Bridges



When running in a failover configuration (as above), “Enable Spanning Tree” must be checked on the bridge interface in order to avoid bridging loops. (see figure below)



Collecting Data for Bridging Issues

The following information is required for bridging issues…

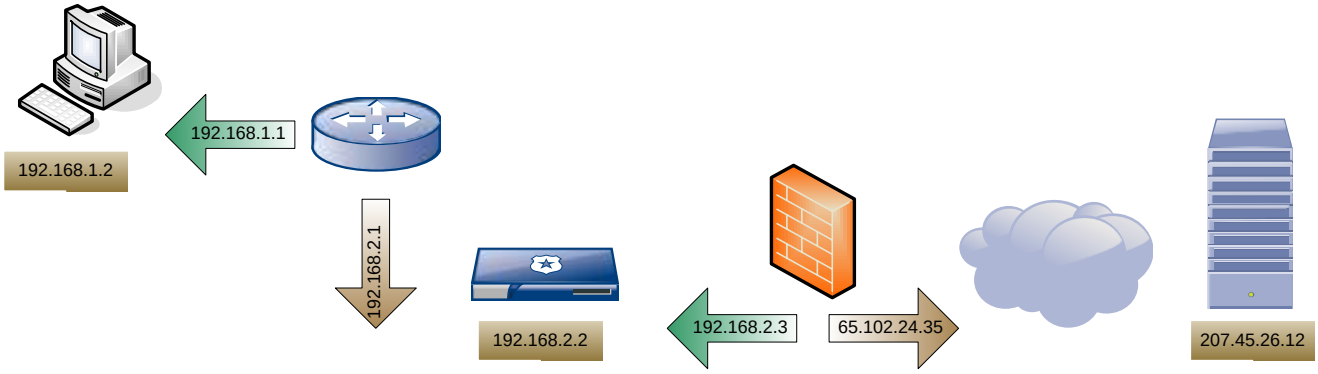
1. Sysinfo
2. Event log
3. Snapshots (all)
4. Packet capture
5. Output from the following locations:
    a. Via the console:
        i. https://x.x.x.x:8082/Bridge/fwtable
        ii. https://x.x.x.x:8082/Bridge/stats
    b. Via the command line interface:
        i. show bridge fwtable <bridge name>
        ii. show bridge conf <bridge name>
        iii. show bridge statistics <bridge name>

See "*Chapter 6: Software and Hardware Bridges*" in "Vol 1: Getting Started" of the ProxySG Configuration and Management Guide for more information on bridges.

Network Infrastructure

A common mistake in diagnosing connectivity issues is to discount the network infrastructure that lies between the workstation and the Proxy SG. Any one of these devices could suffer from hardware or configuration issues resulting in packet loss, blocking, misroutes, etc. The first step in diagnosing a connectivity issue is to run a ping from the workstation to the Proxy SG. If the ping fails the next step is to run a more comprehensive ping test that includes the network infrastructure making up the *physical path* between the workstation and Proxy SG to find out exactly where the failure might be.

Comprehensive PING Test



Ping test performed from the 192.168.1.2 workstation.

1. ping 192.168.1.2 (device itself)
2. ping 192.168.1.1 (gateway router for the 1.0 network)
3. ping 192.168.2.1 (router interface 2.0 net)
4. ping 192.168.2.2 (SG interface)
5. ping 192.168.2.3 (firewall 2.0 internal net interface)
6. ping 65.102.24.35 (firewall external interface)
7. ping 207.45.26.12 (web server)

In this example the proxy is deployed “in-line” so it is bridging (layer 2 function). If ping is successful to the firewalls internal interface then the proxy has connectivity and is passing traffic (at least on a network level). One thing to remember is that ping uses ICMP and if any of the devices along the physical path is configured to block ICMP then ping tests will not be beneficial. Telneting to one of the service ports on the SG (port 80 for example) might be a better test, but often packet captures are required to see what is actually happening.

WCCP Issues

The following information is required for WCCP issues:

1. Sysinfo
2. Event log
3. Snapshots (al)
4. Packet capture from the SG taken while the issue is occurring.
5. Router logs: output from the following commands when issued on the router (when WCCP is active):
    - sho ver
    - sho conf
    - sho ip wccp

- show ip wccp <service-group> detail
- show ip wccp <service-group> view
- display WCCP events

Gathering data

1. Start the PCAP on the SG (unfiltered…if a filter exists delete, apply, and start the PCAP)
2. Reproduce the issue
3. Stop the PCAP

Upload via the MC

- Sysinfo
- Event log
- Snapshots (all)
- Packet Capture
- Zip the router logs together and upload via https://upload.bluecoat.com.

Proxy Hangs and Crashes

Sometimes the SG may appear hung when the real problem may be an issue with connectivity. Likewise what may at first appear to be a connectivity issue is in reality an SGOS hang or crash. If the proxy is hung, it will not respond to ping or serial access. If the proxy has crashed and is writing a full core, for example, it will not respond to ping until it has restarted itself. This condition might last anywhere from 2-20 minutes depending.

In order to better determine the actual state of the SG it is important to know the answer to the following (before rebooting the box):

Is the device accessible via the following methods?

- Ping
- Telnet
- Serial Cable
- HTTP
- HTTPS GUI

Failure to access the SG via HTTP/HTTPS console, SSH, or telnet from a workstation might indicate some sort of a connectivity issue (whether with the proxy or the network), but if the SG cannot be accessed via serial cable then most likely it is hung or has crashed and is restarting or writing a core.

Hang

1. Force a core
    a. Serial Session: **ctrl-x ctrl-h**
    b. DO THIS ONLY ONCE!! - it may seem like nothing is happening, but it may be dumping the core. If **ctrl-x ctrl-h** is entered a second time it will overwrite the first core and the dump will be useless.
    c. If after 20-25 min the SG has not restarted on its own then proceed to step #2 below.
2. Reboot the SG and upload the following
    a. Sysinfo
    b. Event log
    c. Snapshots (all)
    d. Core (if one was written)

Crash

Check to see if the SG has crashed by looking at the “Core Image” section of the SYSINFO.

1. Using the browser enter: http://x.x.x.x:8082/cm/core_image/details?All
2. Check the latest minicontext date and time to see if it correlates with the time when connectivity was lost.

   Example:
   Minicontext produced on: 2009-02-13 07:30:31+00:00UTC

3. If the SG has crashed follow the instructions in this document concerning “Restart Issues”.

Authentication Issues

The following information is required for any authentication related issue:

1. Sysinfo
2. Event Log
3. Snapshots (all)
4. Packet Capture
5. Policy Trace (limited to a single IP)
6. bcaaa.ini file
7. BCAAA debug (Windows SSO debug if applicable)
8. Authentication method (NTLM, Radius, LDAP, etc.)
9. Authentication server type and OS version.
10. Details of the issue and IP address information of involved devices.

Collecting Data for Authentication Issues

1. Log the affected (or test) user off of the SG
   a. SGOS 4 – clear credential cache (configuration > authentication > Realms)
   b. SGOS 5 – log out the user (statistics > authentication > display by user (or IP))
2. Start the BCAAA debug (instructions below) on the server to which the SG is configured to make authentication requests. This server should be running the BCAAA
   a. If using Windows Single Sign On (WinSSO) start an SSO debug also (instructions below).
3. Start a policy trace
4. Start a packet trace on the SG
5. Reproduce the issue
6. Stop the PCAP
7. Save the policy trace (refresh and use FILE | SAVE and save as TEXT)
8. Zip up the entire BCAAA directory (this contains the debug and configuration files)
9. Upload
   a. Sysinfo
   b. Event log
   c. Snapshots (all)
   d. Packet Capture
   e. Zip file containing the BCAAA directory and policy trace (upload via https://upload.bluecoat.com)
10. Post the details and IP address information to the case.

BCAAA Debug

The BCAAA debug is enabled via a modification of the bcaaa.ini file located in the BCAAA installation directory (default: C:\Program Files\Blue Coat Systems\BCAAA).The debug logs are saved to the BCAAA installation

directory in the same place the bcaaa.ini file is located and are named “BCAAA-nnn.log” with “nnn” representing the PID for the BCAAA process that created the log. Each process generates a separate log so there may be several log files created at the end of the debugging session.

How to start the BCAAA debug

1. Open bcaaa.ini
2. Append the following to the end of the file

   ```
   [Debug]
   DebugLevel=0xFFFFFFFF
   ```

3. Save the bcaaa.ini
4. Restart the BCAAA service
5. Debug logs are written to the BCAAA installation directory

How to stop the BCAAA debug

1. Remark out the 2 lines added to the bcaaa.ini with a semi-colon (;)

   ```
   ;[Debug]
   ;DebugLevel=0xFFFFFFFF
   ```

2. Restart the BCAAA service

```
; ------------------------------------------------------------------------

[SSL]
; Control SSL: 0 = permitted, 1 = required, 2 = forbidden.  Default=0
UseSSL=0

; Specify the subject (CN) in the certificate.  This will be looked up
; in the certificate store, if creating, this will be the subject of
; the self-signed certificate.  Default is the hostname of the
; machine on which the agent is running.
CertificateSubject=viper.homelab.ut

; Set to 1 if an automatically generated certificate should be saved in
; the certificate store.  Default = 0
SaveGeneratedCertificate=1

; Set to 1 to specify that the ProxySG must provide a valid certificate
; in order to connect.  Default = 0
VerifySG=0

[Debug]
DebugLevel=0xFFFFFFFF
```

Enabling Windows SSO Debug

1. Open the sso.ini file found in the BCAAA install directory (default is C:\Program Files\Blue Coat Systems\BCAAA)

2. Add the following under the [DCQSetup] heading
   a. DCQDebug=1

Example:

```
;
; Domain Controller Querying must be enabled through this
; setting.  If it is not enabled, the ProxySG will not be
; able to use the Domain Controller Querying setting for
; Windows SSO.
;
[DCQSetup]
; Disabled by default
DCQEnabled=1
DCQDebug=1
```

3. Restart the BCAAA service

Disabling the Windows SSO Debug

1. Remark out the “DCQDebug=1” entry from the sso.ini file using a semi-colon (;)
2. Restart the BCAAA service

Gathering the BCAAA and Windows SSO Debug Logs

Zip up the entire BCAAA installation directory (C:\Program Files\Blue Coat Systems\BCAAA by default). This will contain:

1. bcaaa.ini
2. bcaaa debug logs
3. sso.ini
4. sso debug logs

HTTP Issues

The following information is required for HTTP issues (anything that uses HTTP such as URL requests, FTP over HTTP, Reverse Proxy, etc.).

1. Sysinfo
2. Event Log
3. Packet Capture
4. Policy Trace (limited to a single workstation IP)
5. HTTP debug
6. Details of the URL and any log-on details or steps to reproduce the problem (step-by-step).

Collecting Data for HTTP Issues

1. Start the policy trace
2. Start the HTTP debug (instructions below)
3. Start a PCAP on the SG
4. Reproduce the issue
5. Stop the PCAP
6. Save the HTTP debug (refresh and use FILE | SAVE and save as TEXT)
7. Save the policy trace (refresh and use FILE | SAVE and save as TEXT)
8. Upload via the MC
    - Sysinfo
    - Event log

- Snapshots (all)
- Packet Capture
- Zip file containing the policy trace and HTTP debug log (upload via https://upload.bluecoat.com)

9. Post the details and IP address information to the case.

HTTP Debug

- https://x.x.x.x:8082/HTTP/Debug
- Clear log
- Click “Set Debug Mask”
- Check all options
- Click SUBMIT
- Display HTTP Debug Info

HTTPS Issues

This section assumes that HTTPS is being intercepted (HTTPS service is enabled and an SSL intercept policy layer is installed). It’s important to keep in mind that HTTPS traffic is encrypted. While packet captures are helpful to a point they do not allow any visibility into the data itself. In order to see into the data we need to use SSL and HTTP debug logs.

The following information is required for HTTPS issues:

1. Sysinfo
2. Event Log
3. Packet Capture
4. Snapshots (all)
5. Policy Trace (both the default and one limited to a single IP)
6. SSL Debug (SSL Proxy and CFssl)
7. HTTP debug
8. Details of the URL and any log-on details or steps to reproduce the problem (step-by-step).

Collecting Data for HTTPS Issues

1. Enable default policy trace
   - Configuration > Policy > Policy Options > Trace all policy execution
2. Start a second policy trace (limited to single IP)
3. Start a packet capture on the SG
4. Start the SSL and HTTP debug logs (instructions below)
5. Reproduce the issue
6. Stop the packet capture
7. Stop and save the policy traces and debug logs (refresh and use FILE | SAVE and save as TEXT)
8. Zip up the policy trace and debug logs
9. Upload via MC
   - Sysinfo
   - Event log
   - Snapshots (all)
   - Packet capture
   - Zip file containing policy trace and debug logs (upload via https://upload.bluecoat.com)
10. Post the details and IP address information to the case.

SSL proxy debug

- https://x.x.x.x:8082/SSLproxy/DEBUG
- Clear log
- Set debug mask
- Add all available mask values

  SSL debug mask should look like this:

```
Current mask value is:
     SSLPROXYWARN +
     SSLPROXYERROR +
     SSLPROXYNOTICE +
     SSLPROXYINFO
```

- Display ssl proxy debug info
- Save the debug log
  - Refresh the browser (otherwise only part of the log will be saved)
  - Use **File|Save** and save as **text**

CFssl debug

- https://x.x.x.x:8082/cfssl/debug
- Clear log
- Set debug mask
- Add all available mask values

  CFSSL debug mask should look like this:

```
Current mask value is:
     CFSSLWARN +
     CFSSLERROR +
     CFSSLNOTICE +
     CFSSLINFO
```

- Display ssl proxy debug info
- Save the debug log
  - Refresh the browser (otherwise only part of the log will be saved)
  - Use **File|Save** and save as **text**

HTTP Debug

- https://x.x.x.x:8082/HTTP/Debug
- Clear log
- Click “Set Debug Mask”
- Check all options
- Click SUBMIT
- Display HTTP Debug Info

FTP Issues

The following information is required for FTP issues:

1. Sysinfo
2. Event Log
3. Snapshots (all)
4. Packet capture
5. Policy Trace
6. FTP debug
7. FTP client version and settings
8. Details such as IP address of the workstation and URL of the FTP site
9. Authentication information (used for duplication and identification of user in the PCAP)

Collecting Data for FTP Issues

1. Start the policy trace
2. Start a PCAP on the SG
3. Reproduce the issue
4. Stop the PCAP
5. Save the policy trace (refresh and use FILE | SAVE and save as TEXT)
6. Upload via the MC
    - Sysinfo
    - Event log
    - Snapshots (all)
    - Packet Capture
    - Zip file containing the policy trace and FTP debug log (upload via https://upload.bluecoat.com)
7. Post the details of the issue, FTP client version and settings, FTP URL, authentication information, and client IP address to the case.

Instant Messaging Issues

The following information is required for instant messaging issues…

1. Sysinfo
2. Event Log
3. Packet captures from the client and the SG
4. Policy Trace (limited to a single workstation IP)
5. Messenger client type, version, and network settings.
6. Steps to reproduce the problem (detailed step-by-step).
7. Details and IP information of involved devices.

Collecting Data for IM Issues

1. Start a policy trace
2. Start a PCAP on the client
3. Start a PCAP on the SG
4. Reproduce the issue
5. Stop the PCAP's
6. Save the policy trace (refresh and use FILE | SAVE and save as TEXT)
7. Zip the policy trace

8. Upload via the MC
    - Sysinfo
    - Event log
    - Snapshots (all)
    - PCAP from the SG
    - Zip file containing the policy trace and client PCAP (upload via https://upload.bluecoat.com)
9. Post details and IP information to the case.

Streaming Issues

The following information is required for streaming issues…

1. Sysinfo
2. Event Log
3. Packet captures from the client and the SG
4. Policy Trace (limited to a single workstation IP)
5. Access logs (streaming)
6. Client type, version, and network settings.
7. Steps to reproduce the problem (detailed step-by-step).
8. Details and IP information of involved devices.

Collecting Data for Streaming Issues

1. Enable Access Logging
    - Configuration > Access Logging
    - Check “Enable Access Logging
    - Apply
2. Start policy trace
3. Start packet capture on the client
4. Start the packet capture on the SG
5. Reproduce the issue
6. Stop the PCAP
7. Save the policy trace (refresh and use FILE | SAVE and save as TEXT)
8. Zip up the client PCAP and policy trace
9. Upload via the MC
    - Sysinfo
    - Event log
    - Snapshots (all)
    - PCAP from the SG
    - Access logs (streaming)
    - Zip file containing the client PCAP and policy trace (upload via https://upload.bluecoat.com)
10. Post details and IP information to the case.

Director Issues

Taking a Packet Capture on Director

Use standard Linux tcpdump CLI commands to take a packet capture from Director. By default tcpdump only captures the first 68 bytes. In order to retain the header information a filter must be set using the –s (snaplen) option before starting the packet capture.

From the Director CLI (https://<directorIPaddr>:8082):

Log in
Enable
Conf t

Getting a packet capture:

1. (config) # tcpdump filter -s200
    a. This sets the number of bytes to capture per packet, 0 captures full packet (-s0)
2. (config) # tcpdump start
3. duplicate the issue
4. (config) # tcpdump stop
5. Upload the PCAP from Director to FTP or HTTP server (file name: “sgmetcpdump” or “directortcpdump”)
    a. (config) # tcpdump upload ftp://<hostname>/<path>

    NOTE: Either of these two options can be used....
    http://<hostname[:port]>/<path>
    ftp://<hostname>/<path>

    If <path> ends with a directory name, it must end with /
    (ex): tcpdump upload ftp://192.168.1.251/mark/

6. Upload the packet capture to the case by using https://upload.bluecoat.com

Getting a Debug Dump from Director

1. Immediately after reproducing the issue go to the director CLI (https://<directorIPaddr>:8082)
2. Log in
3. Enable
4. Conf t

(config)#debug dump generate

Generating debugging dump...
Dump file successfully written to
ciqinfo-Director-2007.06.01-155844.tgz

5. Upload the dump to a local FTP server

(config) # shell
sh-2.05b# cd /local/userfiles
sh-2.05b# ls

cIQconfig_050202dump?ciqinfo-Director-2007.06.01-155844.tgz

sh-2.05b# mv dump?ciqinfo-Director-2007.06.01-155844.tgz Debug_dump.tgz
sh-2.05b#ftp

ftp> open ftp.example.com
ftp> bin
ftp> put Debug_dump.tgz

Hardware

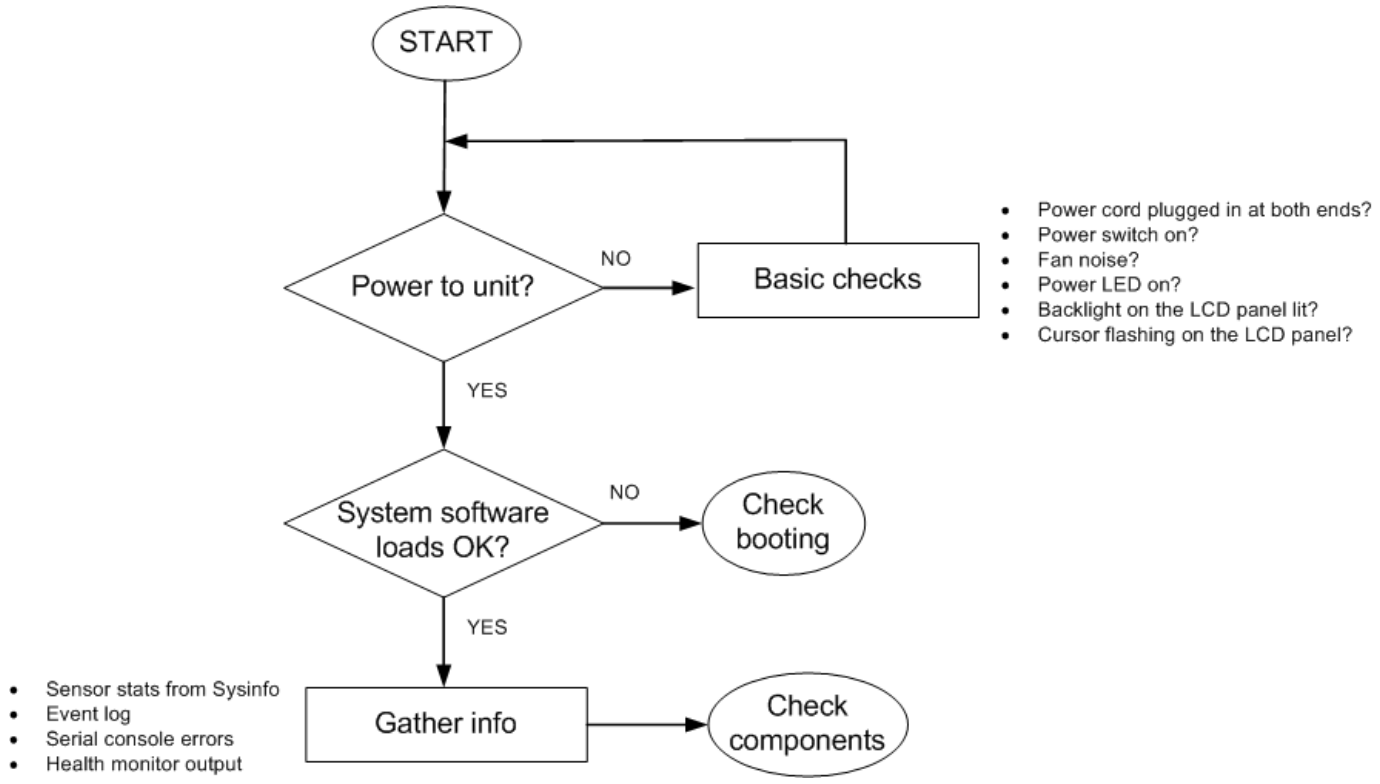
Field Replaceable Items

1. Disk drives
2. Option cards
3. Power supply (SG8100)
4. CPU fan
5. Blowers (SG510 and SG810)

Non Field Replaceable Items

1. RAM
2. CPU
3. Motherboard

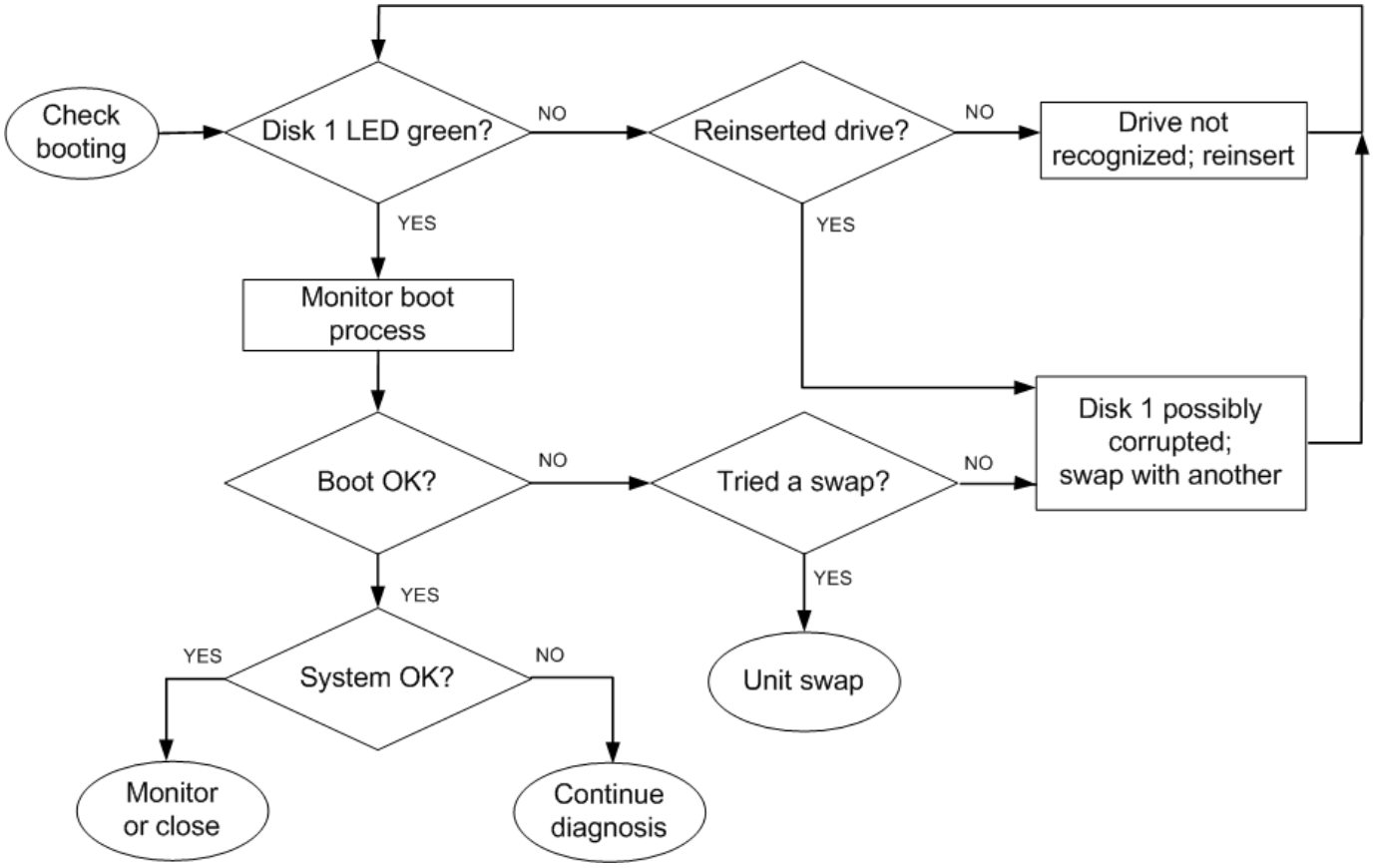
Initial Visual Inspection



The following information is required for initial inspection

1. Sysinfo
2. Event Log
3. Serial console output/errors

Diagnosing Boot Sequence



The following information is required for diagnosing the boot sequence

1. Serial Console output
2. Troubleshooting steps taken
3. Sysinfo (if bootable)
4. Event Log (if bootable)

Disk Drive, Power Supply, and Fan issues

The following information is required for disk drive, power supply and fan issues

1. Sysinfo
2. Event Log

RMA

Blue Coat provides RMA Advanced Hardware Exchanges to those customers who have a valid entitlement under product warranty or service contract. Below are the steps to take to initiate a RMA.

1. Open a technical support case via BlueTouch Online or contact Technical Support.
2. A technical support engineer will work with you to troubleshoot the issue and verify if a hardware repair or replacement is required.
3. If a hardware replacement is required, the technical support engineer will initiate the RMA by obtaining the following customer information:
    - Company Name
    - Shipping Address
    - Contact Name
    - Contact Phone Number
    - Contact email address
    - Problem Description
    - Product Model Number
    - Product Serial Number
4. When the RMA has shipped, the customer will receive a shipment notification which will include instructions regarding the defective hardware return.
5. If the defective hardware is not returned in a timely manner, the customer will be contacted. Customers may also contact Blue Coat for return instructions, rma@bluecoat.com.

Advance Hardware Replacement

RMA Requests received and deemed necessary by Technical Support before the RMA cut off time will have replacement hardware shipped same day. Requests received or verified by Blue Coat Technical Support after the RMA cut off time ship the following day. Actual delivery time will vary dependant upon shipping origin and destination. Out-of-box warranty shipments may require additional time to ship.

RMA Cut-Off Times

(Daylight Savings Time observance may affect RMA cut-off times where applicable)

Support Center	Regular Business Hours	RMA Cut Off Time
North America	Mon-Fri, 06:00 to 18:00, Pacific Time Zone	Mon-Fri 12:00, Sat 10:00, Sun *10:00, Pacific Time Zone
Europe	Mon-Fri, 08:00 to 17:00, GMT	Mon-Fri 11:00, Sat 09:00, Sun *09:00, GMT
Asia	Mon-Fri, 08:00 to 17:00, Malaysia Time Zone	Mon-Fri 12:00, Sat 09:00, Sun *09:00, Malaysia Time Zone

*RMA's deemed necessary by Technical Support will ship at the request of the customer on Sunday prior to the cut off times. Two service types will be considered for shipment. Next Flight Out (NFO) Service is subject to commercial airlift schedules and restrictions. Certain origins & destinations may not have NFO service available for shipment. Orders unable to ship on Sunday will be processed the following business day. If the customer is located within 100 miles in North America or 50KM internationally, local courier services will be considered. Customer must be on site to accept delivery for Sunday deliveries.

Aditional RMA Information can be found at
http://www.bluecoat.com/support/supportpolicies/rmainformation#process

Monitoring

There are several methods that can be used to monitor the ProxySG appliance.

1. Event logging
2. SNMP
3. Health monitoring

For more information review the following sections in the ***"Configuration Management Guide"***

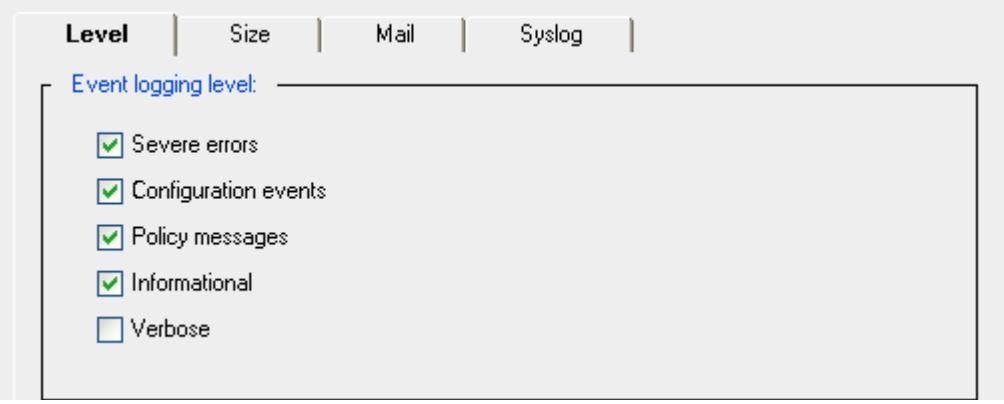
1. ***SGOS 4.x: Chapter 21: Maintaining the ProxySG***
2. ***SGOS 5.x: Volume 9: Managing the Blue Coat ProxySG Appliance, Chapter 2: Monitoring the ProxySG***

Event Logging

The SG can be configured to log system events as they occur. *Event logging* allows you to specify the types of system events logged, the size of the event log, and to configure Syslog monitoring. The appliance can also notify you by e-mail if an event is logged.

Setting Event Log Level

1. Select **Maintenance > Event Logging > Level**.



2. Select the events you want to log.

   When you select an event level, all levels above the selection are included. For example, if you select **Verbose**, all event levels are included.

3. Click **Apply**.

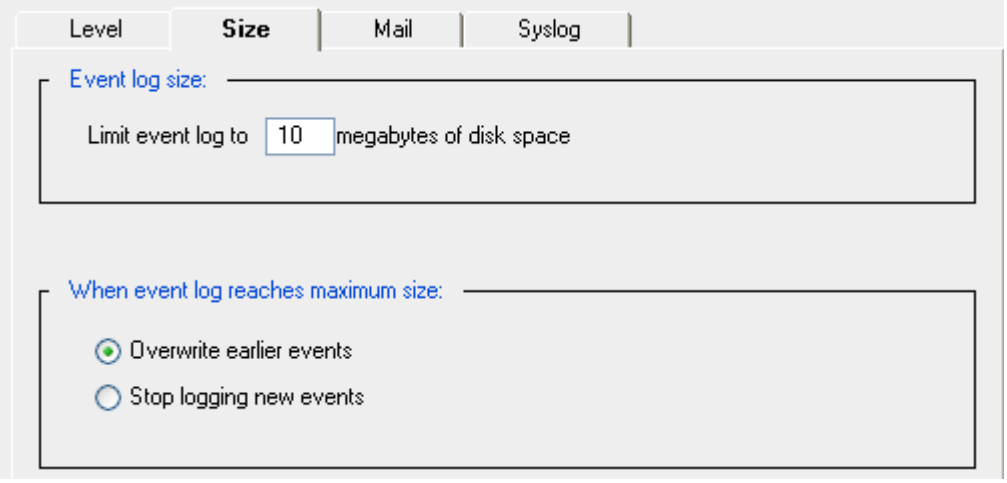
Event Logging Level Options	
`severe`	Writes only severe error messages to the event log.
`configuration`	Writes severe and configuration change error messages to the event log.

`policy`	Writes severe, configuration change, and policy event error messages to the event log.
`informational`	Writes severe, configuration change, policy event, and information error messages to the event log.
`verbose`	Writes all error messages to the event log.

Setting Event Log Size

You can limit the size of the appliances event log and specify what the appliance should do if the log size limit is reached.

1. Select **Maintenance > Event Logging > Size**.



2. In the **Event log size** field, enter the maximum size of the event log in megabytes.
3. Select either **Overwrite earlier events** or **Stop logging new events** to specify the desired behavior when the event log reaches maximum size.
4. Click **Apply**.

Email Alerts

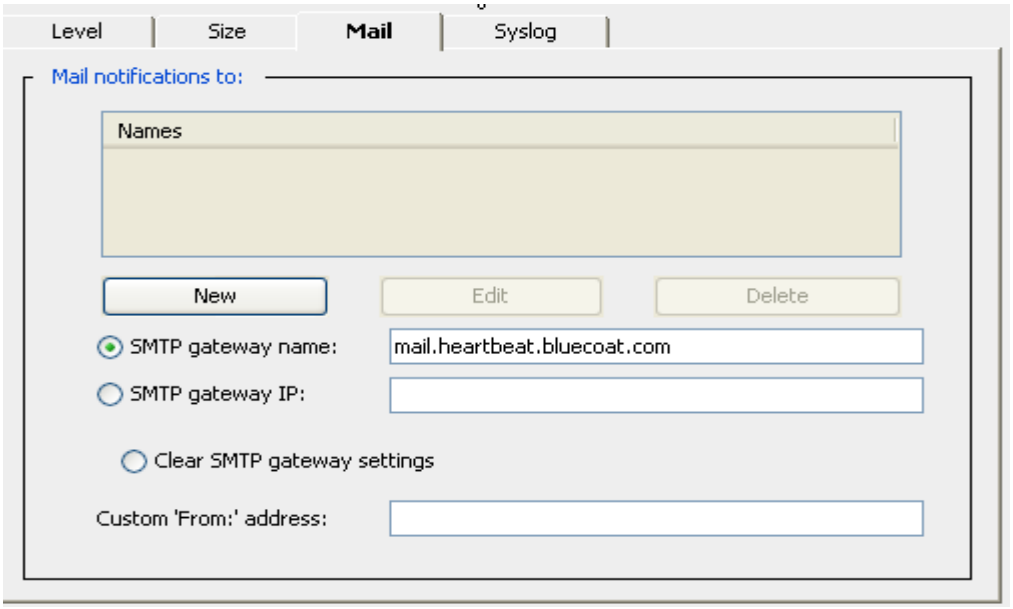
The ProxySG can send event notifications to Internet email addresses using SMTP. This setting applies to all events that can be configured to send mail such as health check warnings, CPU, memory pressure, disk errors, etc.

Note: The ProxySG must know the host name or IP address of your SMTP mail gateway to mail event messages to the e-mail address(es) you have entered. If you do not have access to an SMTP gateway, you can use the Blue Coat default SMTP gateway to send event messages directly to Blue Coat.

The Blue Coat SMTP gateway only sends mail to Blue Coat. It will not forward mail to other domains.

Enabling Event Notifications:

1. Select **Maintenance > Event Logging > Mail**.



2. Click **New** to add a new e-mail address; click **OK** in the Add list item dialog that appears.
3. In the **SMTP gateway name** field, enter the host name of your mail server; or in the **SMTP gateway IP** field, enter the IP address of your mail server. The ProxySG is configured to use only one of these two fields.
4. (Optional) If you want to clear one of the above settings, select the radio button of the setting you want to clear. You can clear only one setting at a time.
5. (Optional) You can specify a custom address for email notifications in the **Custom `From' address** field. For example, headoffice.sg1@bluecoat.com.
   If set, all email notifications use the specified address (headoffice.sg1@bluecoat.com) as the sender's address.

   By default, the field is empty and email notifications use the *Appliance Name* configured on the ProxySG as the sender's address. For information on configuring the appliance name, refer to *Volume 1: Getting Started*.

6. Click **Apply**.

Syslog

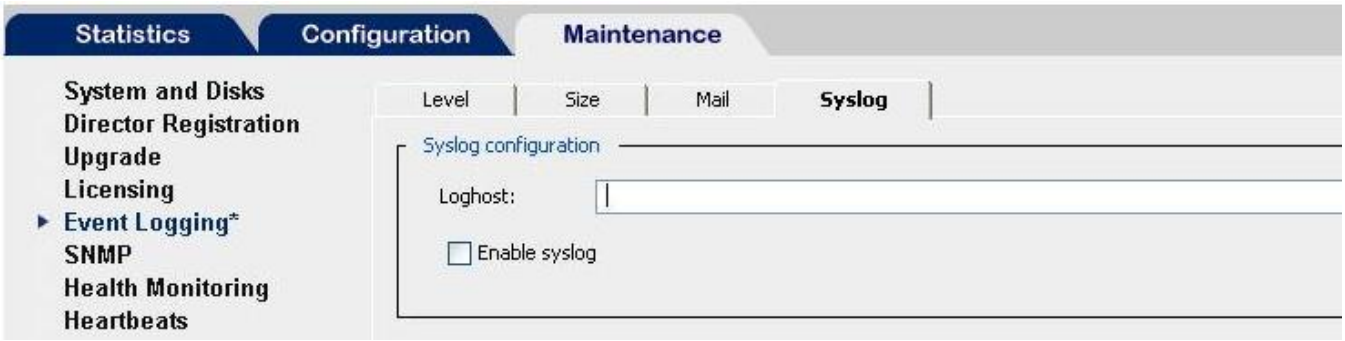
You must have a syslog daemon operating in your network to use syslog monitoring.

Syslog format: `Date Time Hostname Event.`

Many customers using syslog have multiple devices sending messages to a single syslog daemon. This allows viewing a single chronological event log of all of the devices assigned to the syslog daemon. An event on one network device might trigger an event on other network devices, which, on occasion, can point out faulty equipment.

Enabling Syslog Monitoring

1. Select **Maintenance > Event Logging > Syslog**.
2. In the **Loghost** field, enter the domain name or IP address of your log host server.
3. Select **Enable Syslog**.
4. Click **Apply**.



Health Monitoring

Health Monitoring allows you to set notification thresholds on various internal metrics that track the health of a monitored system or device. Each metric has a *value* and a *state*. The *value* is obtained by periodically measuring the monitored system or device. In some cases, the value is a percentage or a temperature measurement; in other cases, it is a status like "Disk Present" or "Awaiting Approval". The *state* indicates the condition of the monitored system or device:

- OK - The monitored system or device is behaving within normal operating parameters.
- WARNING - The monitored system or device is outside typical operating parameters and may require attention.
- CRITICAL - The monitored system or device is failing, or is far outside normal parameters, and requires immediate attention.

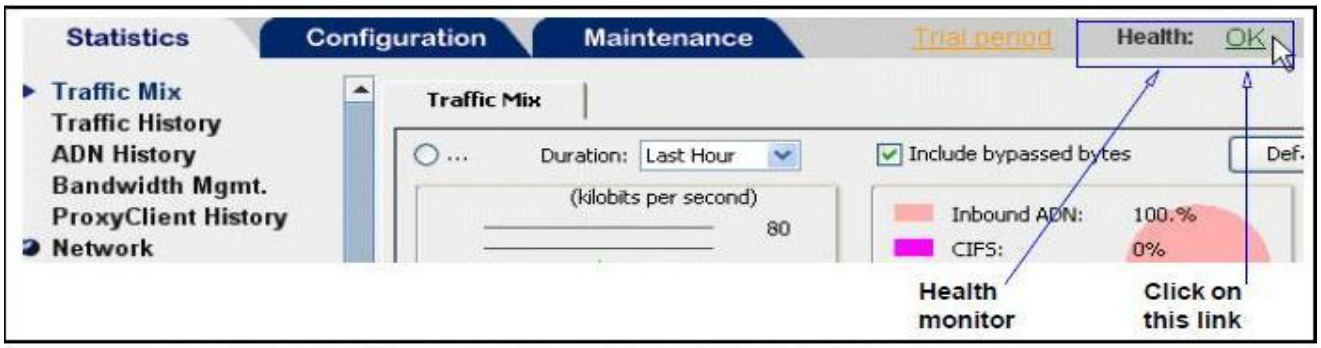


Figure 2–1 Health Monitor as displayed on the Management Console

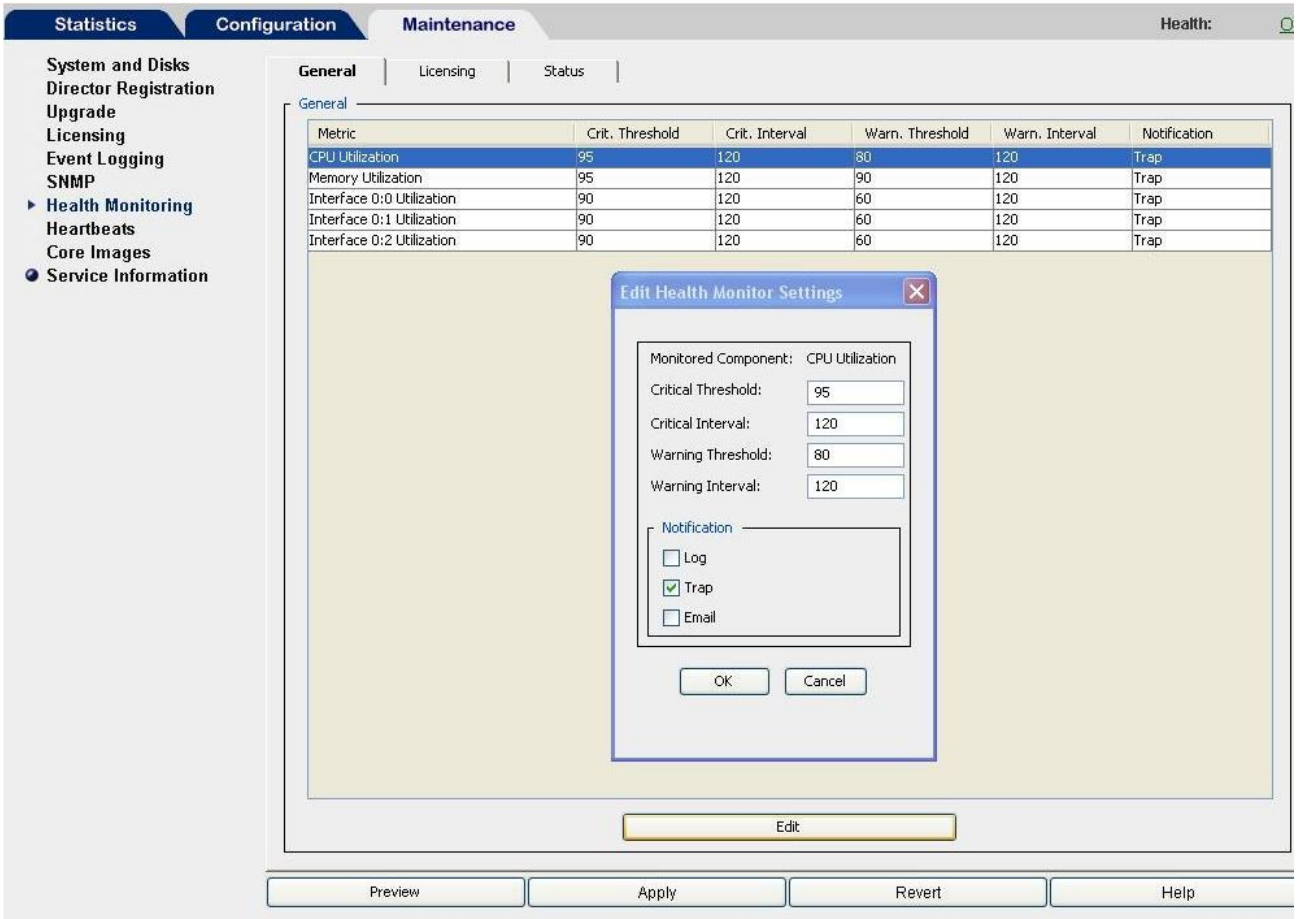
A change in health status does not always indicate a problem that requires corrective action; it indicates that a monitored metric has deviated from the normal operating parameters. The health monitor aids in focusing attention to the possible cause(s) for the change in health status.

The ProxySG monitors the status of the following metrics:

- Hardware — Disk, Voltage, Temperature, Fan speed, Power supply
- System Resources — CPU, Memory, and Network usage
- ADN Status
- License Expiration and Utilization
- Health Check Status — health status of external services used by the appliance

Changing Threshold and Notification Properties:

1. Select **Maintenance > Health Monitoring**.
2. Select the tab for the metric you wish to modify.
    a. To change the system resource metrics, select **General**.
    b. To change the hardware, ADN status and health check status metrics, select **Status**.
    c. To change the licensing metrics, select **Licensing**.
3. Click **Edit** to modify the threshold and notification settings. The **Edit Health Monitor Setting** dialog displays. Hardware, health check, and ADN thresholds cannot be modified.



Modify the notification settings.

- Log adds an entry to the Event log (and/or SYSLOG if configured).
- Trap sends an SNMP trap to all configured management stations.
- Email sends an email to the addresses listed in the Event log properties.

SNMP

The ProxySG provides the capability to configure SNMP for single network management systems (NMS), a multiple user NMS, and for notification only.

Configuring SNMP

Full configuration information is found in the Configuration Management Guide and the Help files on in the SNMP section on the SG itself.

1. Maintenance > SNMP
2. Click “Help” on each tab for information on configuring SNMP

Information can also be found in the following sections of the **“Configuration Management Guide”**

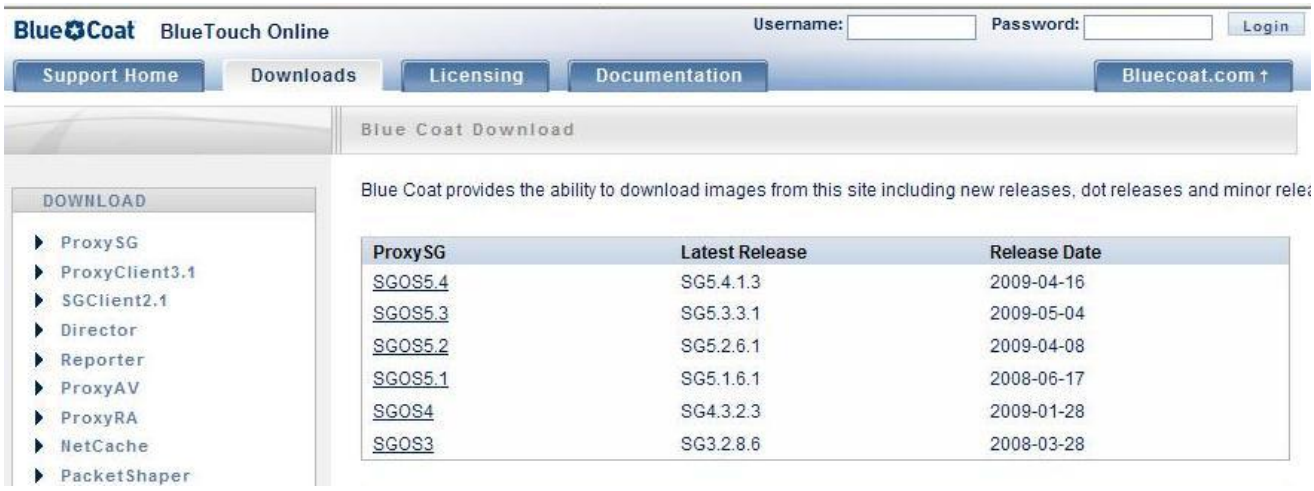
1. **SGOS 4.x: Chapter 21: Maintaining the ProxySG, Configuring SNMP**
2. **SGOS 5.x: *Volume 9: Managing the Blue Coat ProxySG Appliance***
   Chapter 2: Monitoring the ProxySG
   Section D: Configuring SNMP

Obtaining MIB Files

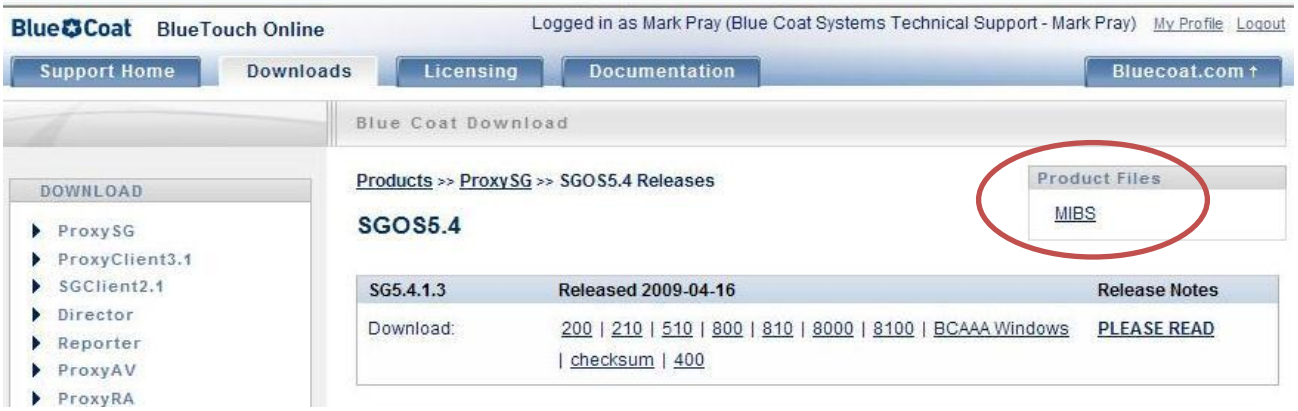
The ProxySG uses both public MIBs and Blue Coat proprietary MIBs. You can download the MIB files from the Blue Coat Web site.

To download the MIBs:

1. Go to https://bto.bluecoat.com/download
2. Click the SGOS version desired (the running version).



3. In a small window in the upper right of the page there is a section called “Product Files”. Click “MIBs” and a file download dialog will display.



4. Click **Save** to navigate to the location to save the zip file of MIBs.

Note: To load the Blue Coat MIBs on an SNMP network manager, be sure to load the dependent MIBs, as well. Most commercial SNMP-based products load these MIBs when the software starts.

Appendix

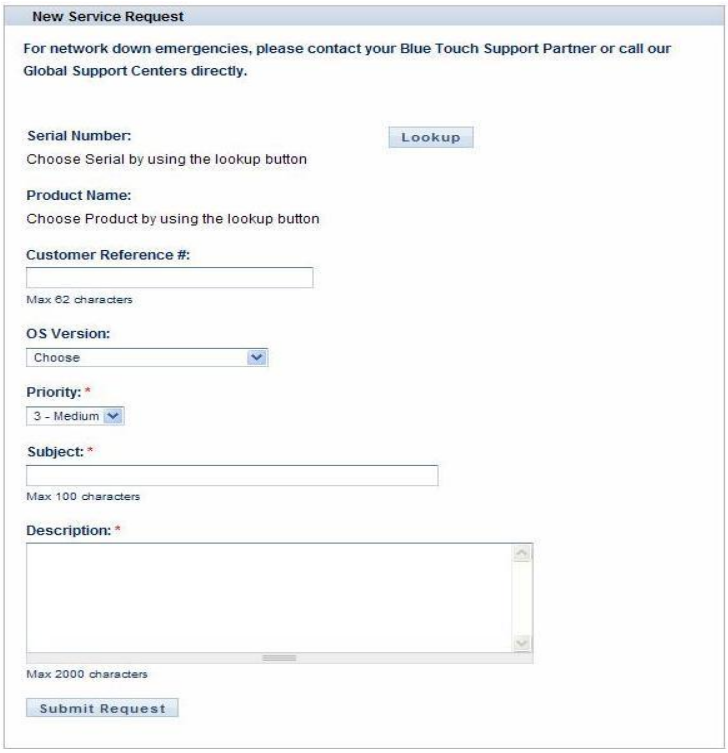
Appendix A: Opening Service Requests

Blue Touch Online

Opening SR's via Blue Touch Online:

1. Access: https://bto.bluecoat.com/support
2. Login using your Blue Coat login or click "Request Login" to obtain a login.
3. Under "Service Management" click "Open New SR"

4. Complete the "New Service Request" form
    a. OS Version
        1. Choose the version closest to what you are running. If the exact version is not available in the drop down list please add the exact version in the description field.
    b. Subject
        1. This is a short concise abstract descritption of the problem
    c. Description
        1. Enter a detailed description of the issue following the guidelines set forth in the section: Troubleshooting Methodology: Clear understanding of the issue.



5. Submit the request
    a. A confirmation email will be sent to the email address on file.

Telephone

For network down or other emergencies, please contact your Blue Touch Support Partner or call our Global Support Centers directly at the numbers below. The online portal (Blue Touch Online) is intended for P3 and P4 issues only.

Americas:

Local Call: +1 408 220 2200, option #3, or

Toll-Free: +1 866 362 2628, option #1

Europe, Middle East and Africa:

UK Call: +44 (0)1252 554 700

Asia-Pacific:

Asia-Pacific: +6 03-2687-7501

Japan: +81 335808390

Appendix B: Manually Retrieving Files from the ProxySG

If you are unable to upload service information using the Management Console (GUI), the following steps will allow you to pull the information locally, for uploading through an alternate channel.

1. SysInfo
   a. In the browser enter: https://x.x.x.x:8082/sysinfo
   b. Use your browser's FILE | SAVE and save as TEXT

2. Event Log
   a. In the browser enter: https://x.x.x.x:8082/Eventlog/fetch=0xFFFFFFFF
   b. Use your browser's FILE | SAVE and save as TEXT

3. Packet Capture
   a. In the browser enter: https://x.x.x.x:8082/PCAP/statistics
   b. Click the download link
   c. Save the .cap file locally

4. Snapshots
   a. In the browser enter: https://x.x.x.x:8082/Diagnostics/Snapshot/
   b. Click “download all” beside each snapshot
   c. Save the .gz file locally

5. Context/Core Image
   a. In the browser enter: https://x.x.x.x:8082/CM/Core_image
   b. Click the hyperlinks to download the core files.

Examples:

```
Most recent core image was produced on Mon, Aug 06 2007 22:06:08 UTC
The most recent core image has not been retrieved.
ProxySG Appliance: Version 4.2.4.1.29063
Core image version: 3.5
Hardware exception code: 0x0
Software exception code: 0x6001A
Page fault linear address: 0x0
Page fault error code: 0x0
Core image components:
0: size = 198,266,880; 1,049,013,705 bytes compressed to 198,183,505
1: size = 28,913,664; uncompressed size 82,702,784  /CM/Core_image/Context.cgz
2: size = 169,282,427; uncompressed size 966,323,476  /CM/Core_image/Memory.cgz
```

Later hardware platforms like the 210, 510, 810, and 8100’s will have a table view like this:

System cores:

Time	Version	Hardware Exception	Software Exception	Page Fault Address	Process		
Tuesday June 26 2007 12:19:26	4.2.3.21.28657	0x0	0x6001a	0x0	Process "CLI_Worker_2" in "cli.dll" at .text+0xb67fb	Details; Minicontext (37888); Context (24651152); Full (295704952);	Delete

Wednesday May 30 2007 16:36:29	4.2.3.21.28657	0x0	0x60019	0x0	Process "CAG_Maintenance" in "con_agent.dll" at .text+0x2a49e	Details; Minicontext (37888);	Delete

If this is the case simply click on the appropriate link for “Minicontext”, “Context”, or “Full” and the file will download.

Upload all of the retrieved information directly to the case using: https://upload.bluecoat.com/

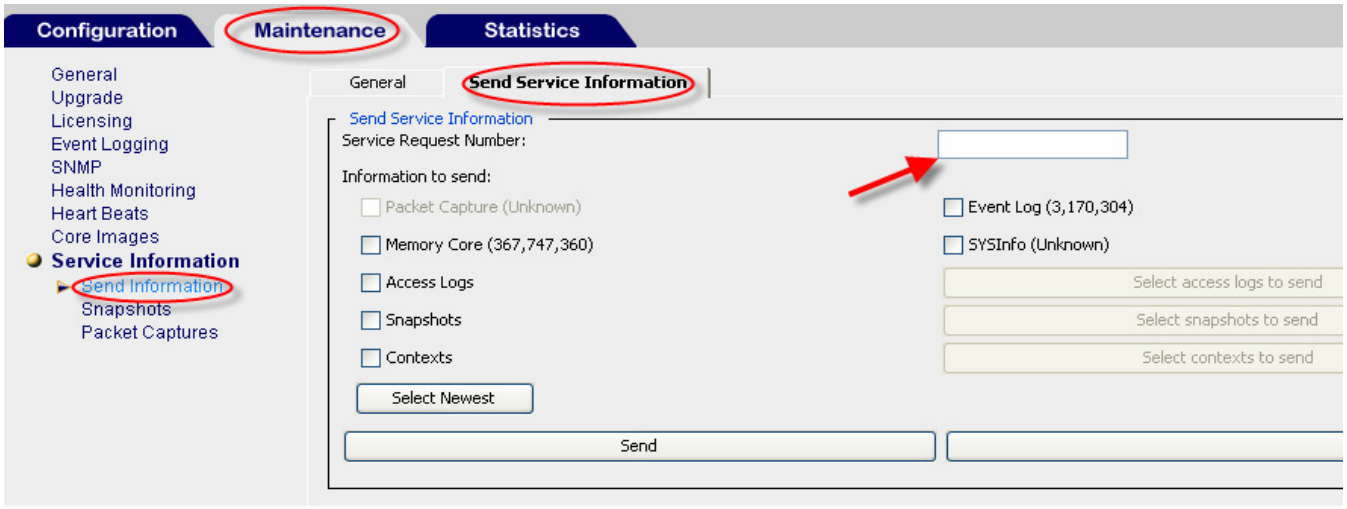
Enter the SR number (Service Request number) in the appropriate field. The SR number does *not* contain the letters "S" "R", and cannot have a trailing space after the SR number. Cut/Paste often adds a trailing space which should be removed if present.

Appendix C: Uploading Files to Bluecoat

There are different options for uploading files to technical support listed here in order of preference.

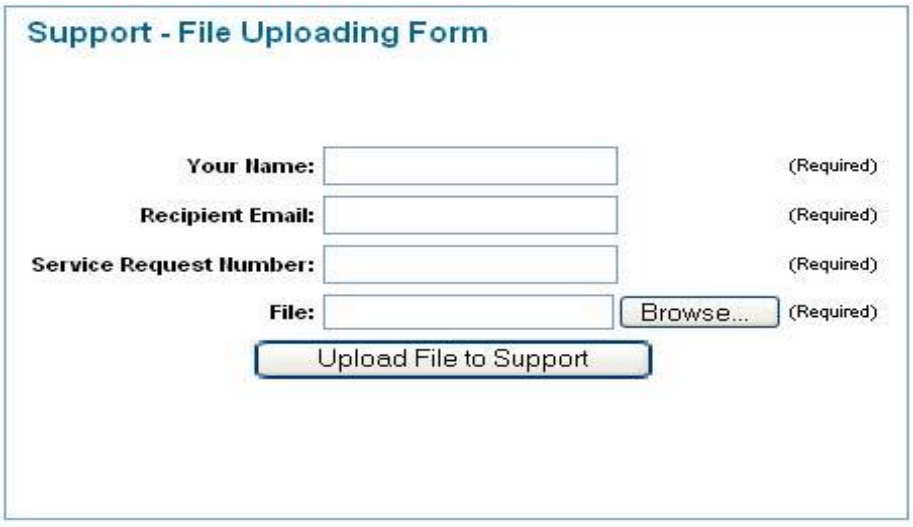
Management Console GUI (MC)

1. Maintenance > Service Information > Send information > Send service information
2. Enter the service request number (include the dash (-))
3. Press the button "Select Newest" –OR- check individual boxes for desired files
4. See how to do this using the CLI below.



upload.bluecoat.com

1. Enter your name, email, SR number, and browse to the file
2. Click “Upload File to Support”
   The file will be uploaded to a folder with your SR number as the name which is accessible to Blue Coat engineers.



ftp.bluecoat.com

1. Use only if the MC or https://upload.bluecoat.com are not available
    a. Change the directory to \incoming\support_dir (note that directory reading is not allowed)
    b. Make a new directory (mkdir) named the same as SR# (or use another pertinent name)
    c. Change the directory to the one that was created in the previous step
    d. "Put" the file into this directory (be sure the FTP client is in binary transfer mode)
    e. Forward the name of the new directory to the Blue Coat technical support engineer

Uploading Files Using the CLI

From the CLI:

1. en
2. (type enable password)
3. config t
4. diagnostics
5. service-info
6. view available
7. send <SR number> <file names as listed in “view available” delimited by a space)

You can use “view status” to check the status of the upload.

Example:

192.168.1.220 - Blue Coat SG200 Series>en
Enable Password:
192.168.1.220 - Blue Coat SG200 Series#config t
192.168.1.220 - Blue Coat SG200 Series#(config)diagnostics
192.168.1.220 - Blue Coat SG200 Series#(config diagnostics)service-info
192.168.1.220 - Blue Coat SG200 Series#(config service-info)view available
Service information that can be sent to Blue Coat

Name	Approx Size (bytes)
Event_log	2,465,792
Policy_trace	1,834,370
System_information	Unknown
Snapshot_sysinfo	Unknown
Snapshot_sysinfo_stats	Unknown
Access_log_main	189,708
Access_log_ssl	980,892

192.168.1.220 - Blue Coat SG200 Series#(config service-info)

192.168.1.220 - Blue Coat SG200 Series#(diagnostics service-info) send 2-41459134 Event_log System_information Snapshot_sysinfo Snapshot_sysinfo_stats

NOTE: Ignore the “unknown” states and send those files anyway.

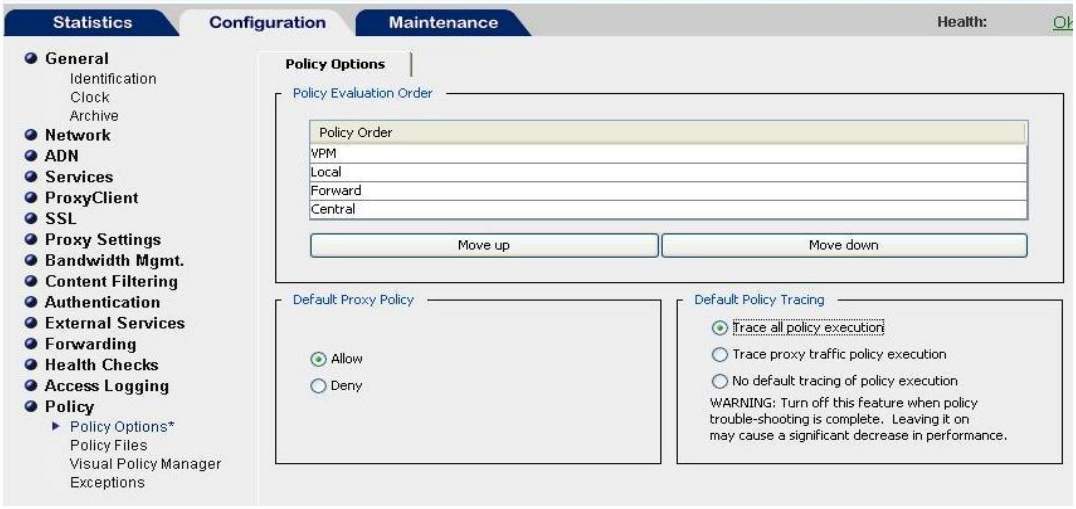
Appendix D: Policy Trace

A policy trace will track and log what policy rules are executed and which are not for any given request. This can be very helpful for tracking down URL, authentication, or any other issue that might be policy related. The SG has a default policy trace setting which captures all policy execution from every device passing through it, but it is also possible to limit policy tracing to just a few devices or even just one device. In most cases it is not helpful to trace policy for every box on the network and when a policy trace is requested it is assumed that the trace will be limited to just one device.

NOTE: SSL issues require 2 policy traces. The default and a separate policy trace limited to just one IP address as the default trace will contain the SSL intercept layer information.

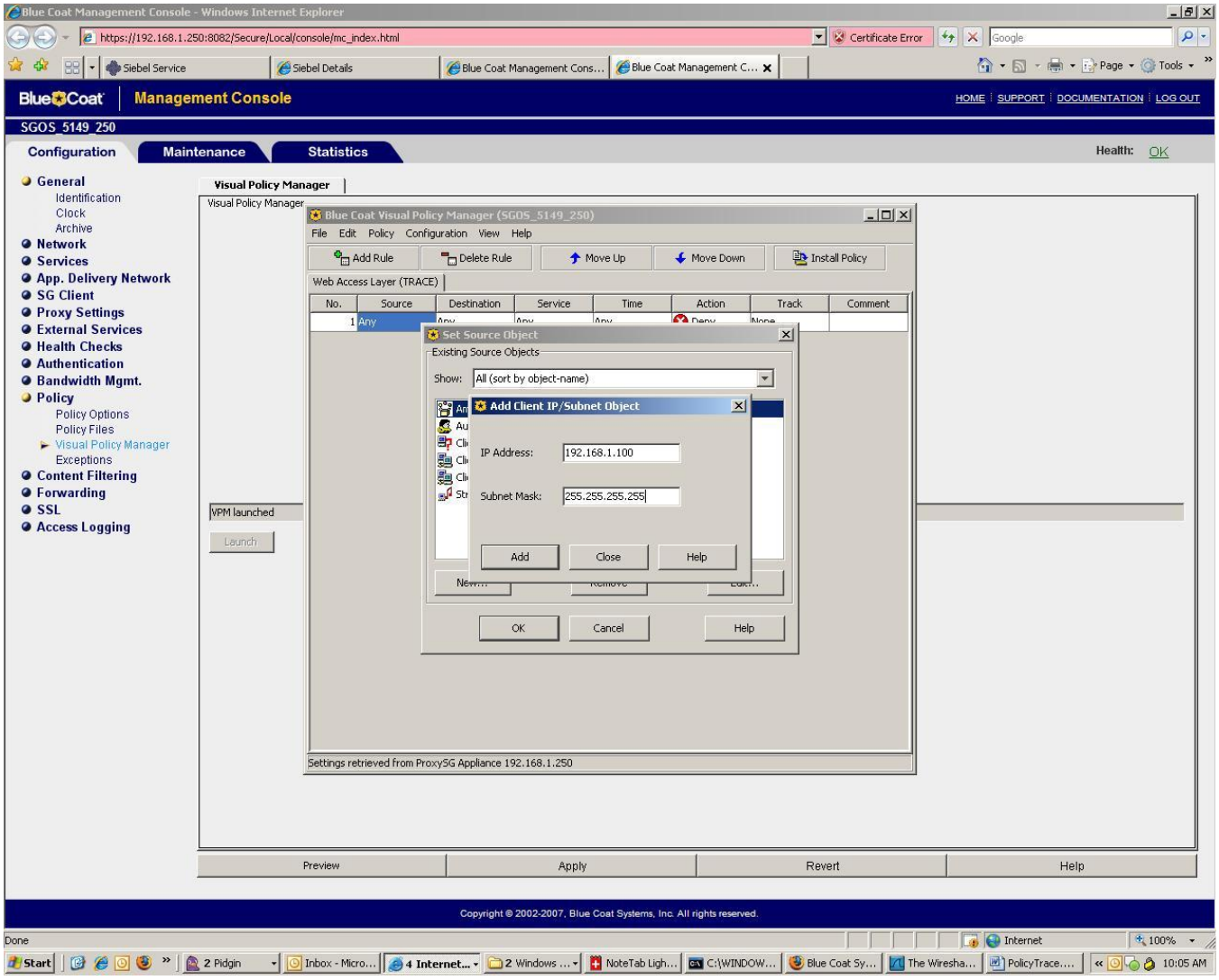
Default Policy Trace

Configuration > Policy > Policy Options
Choose “Trace All Policy Execution”
Apply

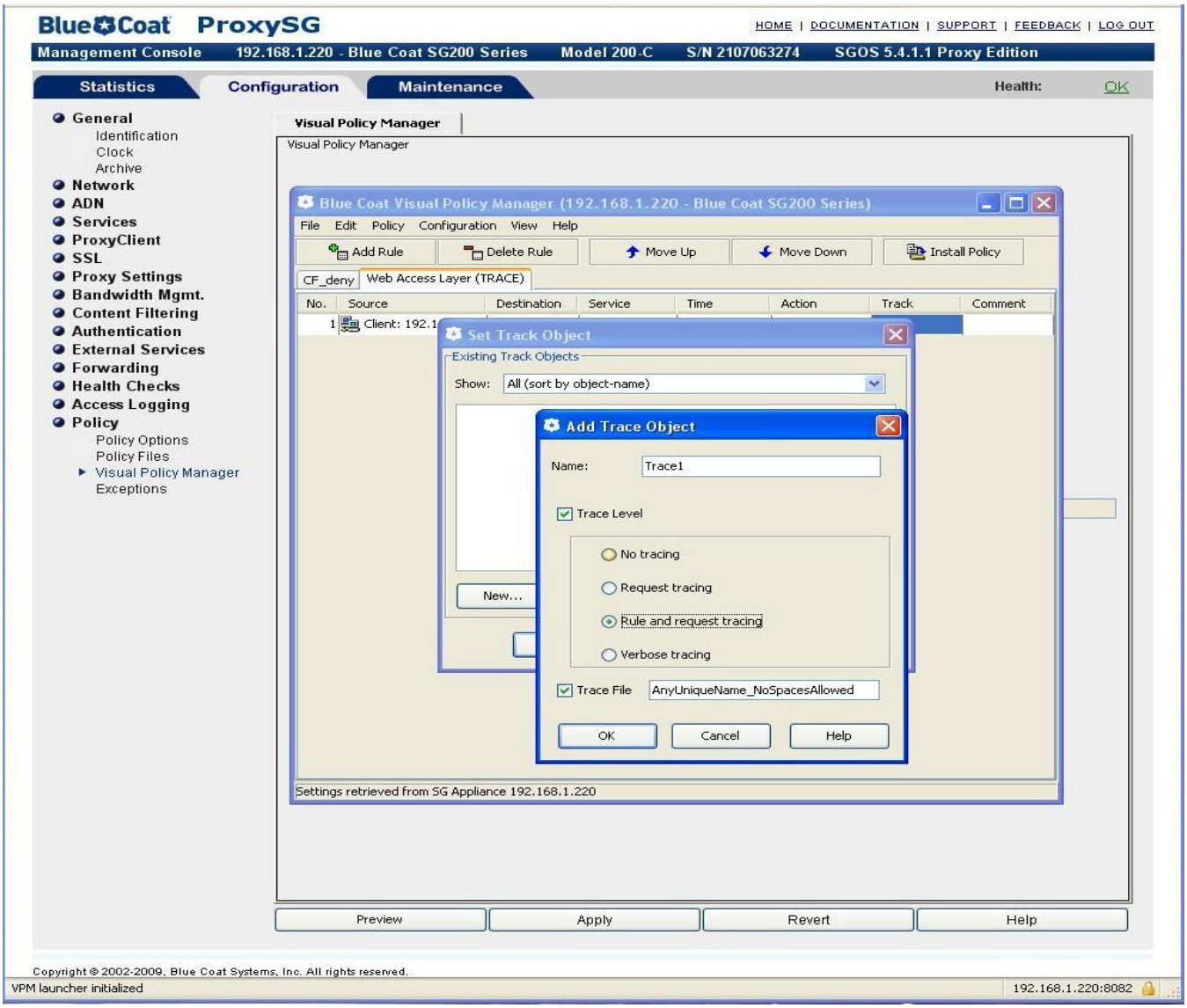


Tracing requests from one Client IP address

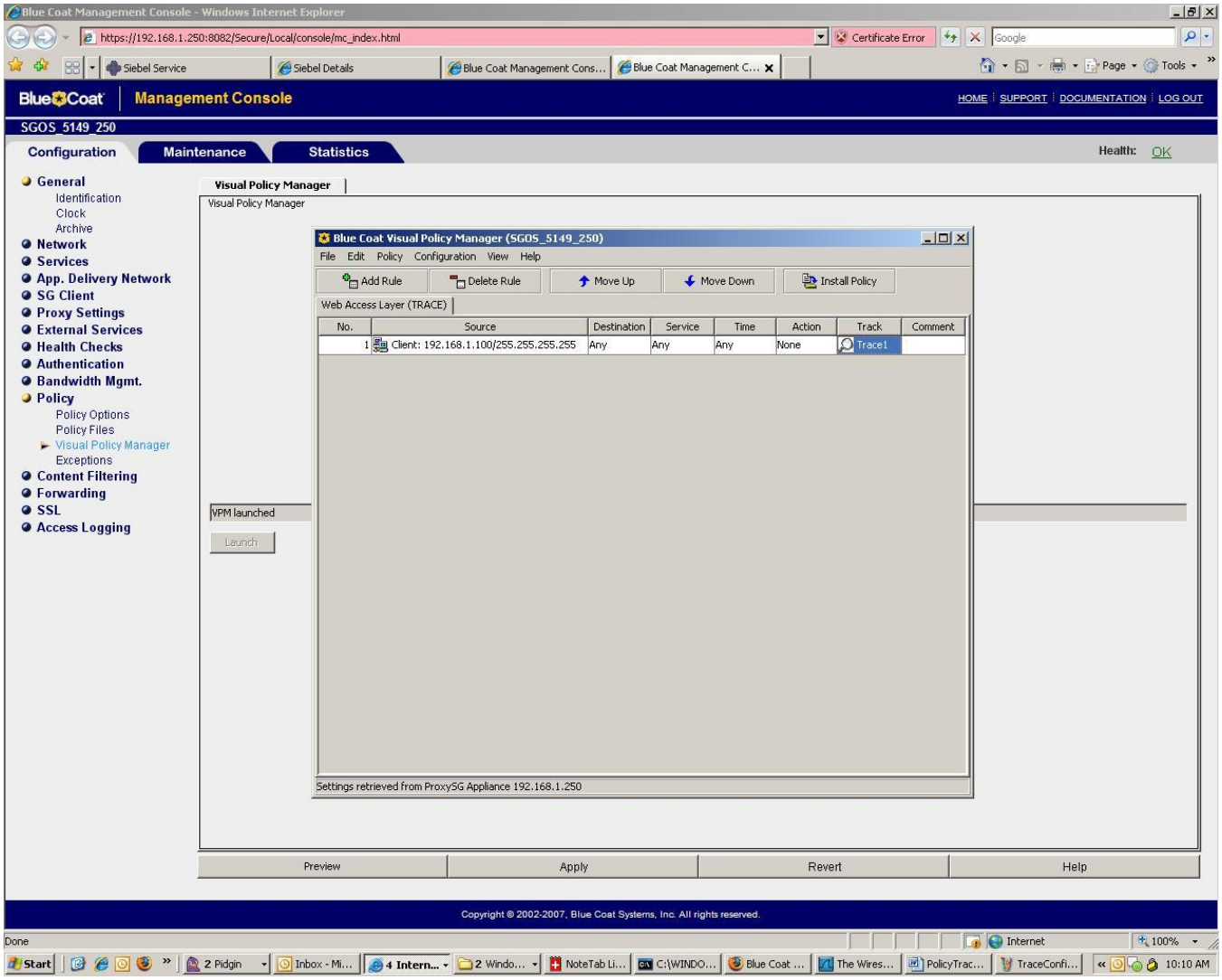
1. Go To: https://x.x.x.x:8082/policy
    a. Click: Delete all policy traces
2. Open VPM (visual policy manager)
    a. Configuration > Policy > Visual Policy Manager > Launch
3. Add new Web Access policy tab
    a. Policy > Add Web Access Layer
4. Set “SOURCE” to the test client IP address
    a. Right click in the source field
    b. SET
    c. NEW
    d. Client IP address/subnet
        i. Enter IP address of the workstation used to test
        ii. Enter full subnet mask (255.255.255.255)
    e. Click ADD > CLOSE >OK



5. Set “ACTION”
    a. Right click in the action field
    b. DELETE (this will set it to “none”)
6. Set “TRACK”
    a. Right click in the TRACK field
    b. SET
    c. NEW
    d. TRACE
        i. Rule and request tracing
        ii. Check “Trace File”
        iii. Name it (“MUST NOT” contain a space or the policy will not be traced)
    e. Click OK > OK
7. Install Policy


Blue Coat ProxySG
HOME | DOCUMENTATION | SUPPORT | FEEDBACK | LOG OUT
Management Console 192.168.1.220 - Blue Coat SG200 Series Model 200-C S/N 2107063274 SGOS 5.4.1.1 Proxy Edition
Statistics Configuration Maintenance Health: OK
General
Identification
Clock
Archive
Network
ADN
Services
ProxyClient
SSL
Proxy Settings
Bandwidth Mgmt.
Content Filtering
Authentication
External Services
Forwarding
Health Checks
Access Logging
Policy
Policy Options
Policy Files
Visual Policy Manager
Exceptions
Visual Policy Manager
Visual Policy Manager
Blue Coat Visual Policy Manager (192.168.1.220 - Blue Coat SG200 Series)
File Edit Policy Configuration View Help
Add Rule
Delete Rule
Move Up
Move Down
Install Policy
CF_deny
Web Access Layer (TRACE)
No.
Source
Destination
Service
Time
Action
Track
Comment
Set Track Object
Existing Track Objects
Show:
All (sort by object-name)
New...
Add Trace Object
Name:
Trace1
Trace Level
No tracing
Request tracing
Rule and request tracing
Verbose tracing
Trace File
AnyUniqueName_NoSpacesAllowed
OK
Cancel
Help
Settings retrieved from SG Appliance 192.168.1.220
Preview
Apply
Revert
Help
Copyright © 2002-2009, Blue Coat Systems, Inc. All rights reserved.
VPM launcher initialized
192.168.1.220:8082

Your trace should look similar to this when complete:



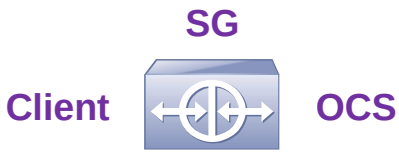
Saving the policy trace

1. https://x.x.x.x:8082/policy
2. Trace will display with the name you gave it previously.
3. Click the trace to open it.
4. Save using FILE | SAVE and save as TEXT.

Appendix E: Packet Capture

Overview

When taking a packet capture it's important to remember that the SG is in the middle of the connection.



In order to see all the information "both sides" of the connection must be captured (client and server side). Configuring a filter for the client IP, for example, would only capture half of the traffic we need to see and therefore render the packet capture useless. Capturing with a filter for both the client IP and server IP can be effective depending on the circumstance; however, in most cases it is optimal to take an "unfiltered" packet capture. This helps ensure we don't miss anything.

Limitations

The packet capture utility in the SG has a few limitations that are vital to take into account when capturing data.

1. The SG has a 100MB buffer. By default, once the buffer is full it will stop capturing data. In a busy environment the buffer may fill very quickly (as little as 6 seconds in some cases). In these cases it is necessary to either filter on specific traffic to capture or reduce the amount of traffic being captured (off hours duplication, etc.). When using filters we may miss the data we need to see. It is preferable to keep duplications as simple as possible and use unfiltered packet captures.

2. It is not possible to capture properly using a filter for ***WCCP GRE*** traffic. When using WCCP redirection with GRE an ***unfiltered*** packet capture is ***required***.

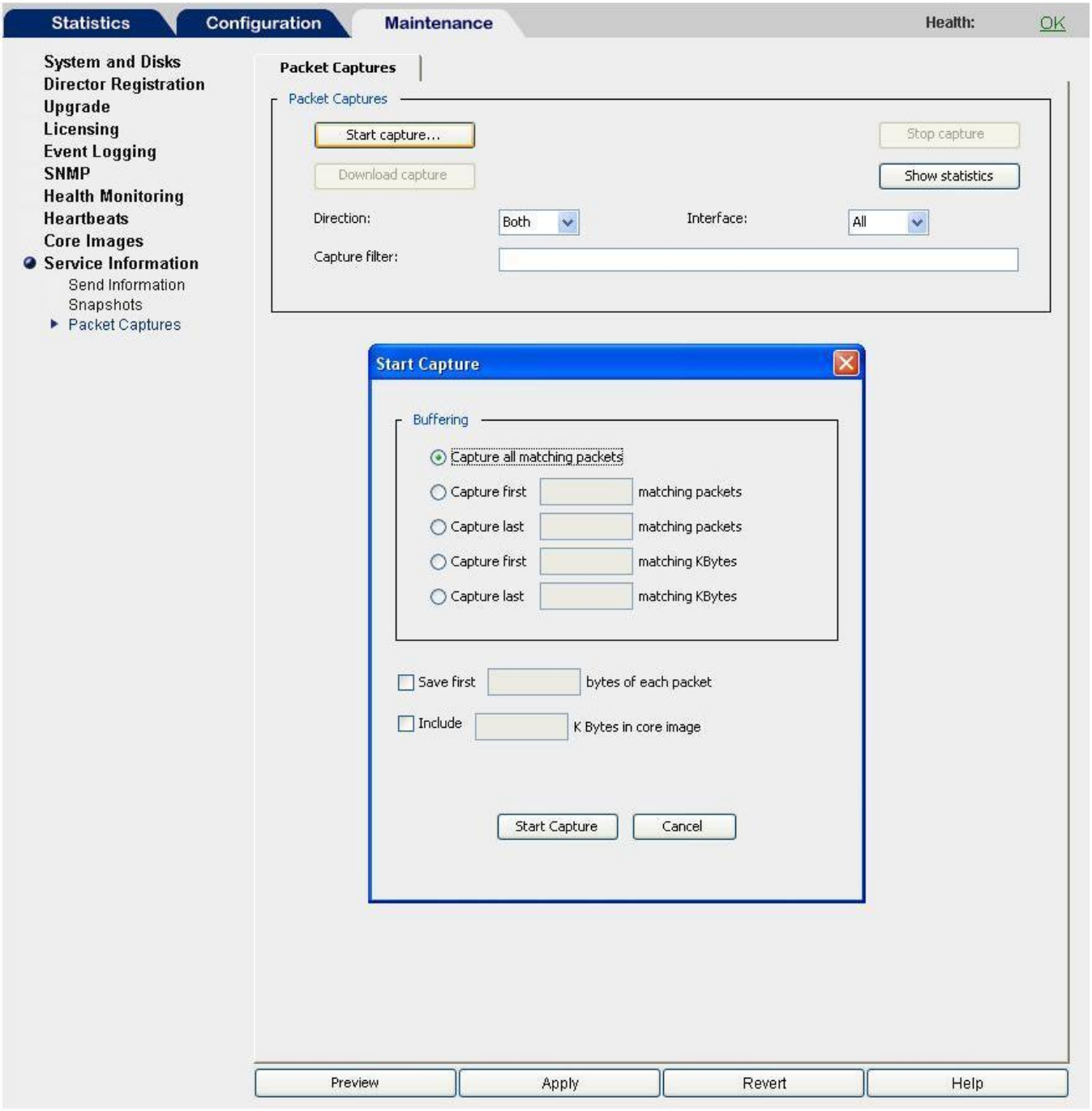
3. The SG will not save more than one packet capture at a time. Once a packet capture is taken it must be either uploaded to the case or downloaded to the PC (saved) before any further packet captures are taken. Any additional packet captures will overwrite the capture before it as will downloading any running packet capture.

Methods

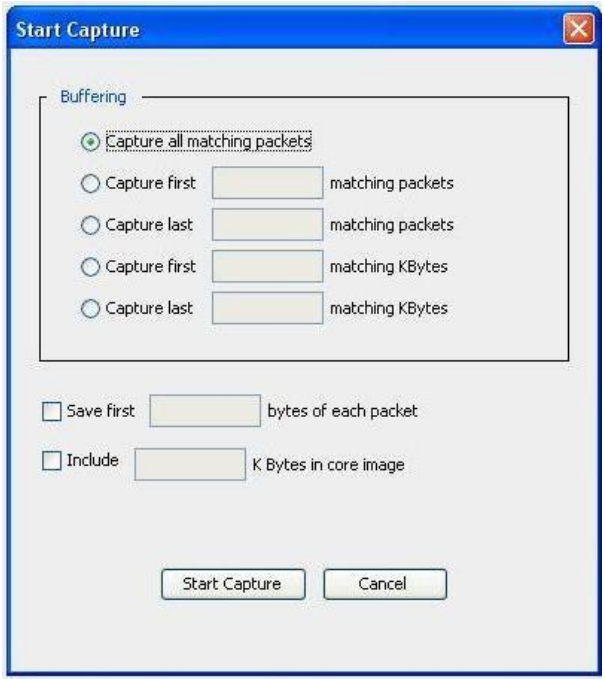
Management Console

This is the preferred method of taking a packet capture as it allows filtering and setting capture preferences.

1. Maintenance > Service Information > Packet Captures
2. Leave the defaults (no filter) and click "Start"
3. Select an optimal configuration for the problem being captured (see "Start capture window")
4. Run a "simple" duplication of the problem.
5. Click "Stop"
6. The packet capture can then be downloaded to the PC for upload via https://upload.bluecoat.com or uploaded directly to the case via use of the "packet capture" check box in "maintenance > service information > send information > send service information.


Statistics
Configuration
Maintenance
Health: OK
System and Disks
Director Registration
Upgrade
Licensing
Event Logging
SNMP
Health Monitoring
Heartbeats
Core Images
Service Information
Send Information
Snapshots
Packet Captures
Packet Captures
Packet Captures
Start capture...
Stop capture
Download capture
Show statistics
Direction:
Both
Interface:
All
Capture filter:
Start Capture
Buffering
Capture all matching packets
Capture first
matching packets
Capture last
matching packets
Capture first
matching KBytes
Capture last
matching KBytes
Save first
bytes of each packet
Include
K Bytes in core image
Start Capture
Cancel
Preview
Apply
Revert
Help

Start Capture Window



- Capture all matching packets
  - Captures all packets matching the “capture filter”.
- Capture first……matching packets
  - Packet capture will stop after reaching *n* number of packets.
- Capture last……matching packets
  - Once stopped the packet capture will save the last *n* packets captured. For example, if 100,000 is specified the SG will save the “last” 100,000 packets captured.
- Capture first……matching KBytes
  - Same function as previously mentioned, but based on size rather than number of packets.
- Capture last……matching KBytes
  - Same function as previously mentioned, but based on size rather than number of packets.
- Save first…..bytes of each packet
  - Truncates each frame by the number of bytes specified rather than capturing the entire packet. This can be used to reduce capture size while maximizing the sample of packets captured. Used to capture packet header information when the payload (data) of the packet is inconsequential to the issue. More packets will be captured in a packet trace.
- Include…..K Bytes in core image
  - Used to insert packet trace data into a full core.

Browser URL

- https://x.x.x.x:8082/PCAP/statistics
- Limitation: Filters cannot be used. Ability to stop, start, and download the packet capture only.

Example view of the PCAP URL:

Packet Capture Statistics

Current state: Stopped
Filtering: Off

Packet capture information:
Packets captured : 0
Bytes captured : 0
Packets written : 0
Bytes written : 0
Coreimage ram used : 0 B
Packets filtered through : 0

Start packet capture

Stop packet capture

Download packet capture file

Filters

The PCAP utility on the SG uses TCP dump style filter syntax for capturing data (as does Director and Wireshark).

PCAP Filter Expressions	
Filter Expression	**Packets Captured**
ip host 10.25.36.47	Captures packets from a specific host with IP address 10.25.36.47.
not ip host 10.25.36.47	Captures packets from all IP addresses except 10.25.36.47.
ip host 10.25.36.47 and ip host 10.25.36.48	Captures packets sent between two IP addresses: 10.25.36.47 and 10.25.36.48. Packets sent from one of these addresses to other IP addresses are not filtered.
ether host 00:e0:81:01:f8:fc	Captures packets to or from MAC address 00:e0:81:01:f8:fc:.
port 80	Captures packets to or from port 80.
ip sr www.bluecoat.com and ether broadcast	Captures packets that have IP source of www.bluecoat.com and ethernet broadcast destination

More filter information:

1. http://wiki.wireshark.org/CaptureFilters
2. http://www.ethereal.com/docs/eug_html_chunked/ChCaPCAPtureFilterSection.html
3. http://www.cs.ucr.edu/~marios/ethereal-tcpdump.pdf

Appendix F: Cores

Overview

A core is the process that occurs when the system writes, or "dumps" its memory to the hard drive. It may be referred to as a dump, core, context, core dump, image, core image, full dump, full core, or memory core. Blue Coat will normally use the following terms…

1. Full Core (full memory core)
2. Context (partial memory core)
3. Minicontext (Short text output logged in the sysinfo at the time a core is written containing running processes and restart codes as well as other functions helpful to support.)

While cores are not necessary or even helpful in troubleshooting all issues, they are required in order for Blue Coat to resolve *certain* issues such as system crashes (also referred to as "restarts"). Cores can also provide information and insight into issues such as proxy hangs, high CPU, and high memory usage.

Basic Configuration

1. Set the core type (example is for "full core")
    a. Click Maintenance > Core Images
    b. Select "full"
    c. Select how many cores you wish to store (default is 2)
    d. Click APPLY
2. Set the proxy restart mode
    a. SGOS 5.x
        i. Click Maintenance > System and Disks > Tasks
        ii. Click "Hardware & Software"
    b. SGOS 4.x
        i. Click Maintenance > General
        ii. Click "Hardware & Software"
    c. Click APPLY.

Note: The SG will write a core regardless of the "restart mode". However, best practice is to have the SG do a "hardware & software" restart unless instructed otherwise.

The default setting is for "**Context Only**" as this provides sufficient information in many cases and is by far the fastest type of core to write resulting in the least amount of down time. A context can be written with almost no more down time than it takes to perform a normal reboot, but a full memory core can take as much as 5-20 minutes to write…depending on your hardware and amount of memory. During the time the proxy is writing a full memory core the box is offline and unavailable until it finishes and restarts (reboot).

Core Generation

Cores are generated in one of two ways.

1. Automatically
2. Manually (also referred to as “forced”)

When the proxy restarts (crashes) due to some error, by default it will write a core and minicontext automatically. It is also possible to manually force the proxy to write a core.

Forcing a Core

Useful information can be obtained from a core when the proxy is **hung**, **slow**, or **behaving unexpectedly** (i.e. high CPU or high Memory usage). For such cases the admin can force a core to be written to disk using one of the following 2 methods:

Command Line Interface (CLI): **restart abrupt**
Serial Session: **ctrl+x ctrl+h**

DO THIS ONLY ONCE!! - it may seem like nothing is happening, but it is dumping the core. If **ctrl-x ctrl-h** is entered a second time it will overwrite the first core and the dump will be useless.

****IMPORTANT****

Forcing a core is only useful if it’s accomplished while the proxy is in a *problem state* such as when it is “hung”, experiencing slowness, or behaving unexpectedly. If the ProxySG is actually crashing, or automatically restarting then a forced core “after the fact” will not provide any useful information. Forcing a core on a system that is currently running normally will not provide any useful information. If you are unsure about when a core should be forced, please consult with support first.

Core Location/Retrieval

Normally it is sufficient to simply go to *“Maintenance > Service Information > Send information > Send service information”*, check the appropriate boxes, and click “Send” to upload the core. However, there are times when it may be necessary to download the files manually. When manual retrieval is necessary the following URL may be used to download the core files.

https://<x.x.x.x>:8082/CM/Core_image

See the example output of this page below:

```
Most recent core image was produced on Mon, Aug 06 2007 22:06:08 UTC
The most recent core image has not been retrieved.
ProxySG Appliance: Version 4.2.4.1.29063
Core image version: 3.5
Hardware exception code: 0x0
Software exception code: 0x6001A
Page fault linear address: 0x0
Page fault error code: 0x0
Core image components:
0: size = 198,266,880; 1,049,013,705 bytes compressed to 198,183,505
1: size = 28,913,664; uncompressed size 82,702,784  /CM/Core image/Context.cgz
2: size = 169,282,427; uncompressed size 966,323,476  /CM/Core image/Memory.cgz
```

NOTE:
The hyperlinks in the above example are the links to the latest cores. In the event a full core was produced it may be necessary to download both the Context.cgz and Memory.cgz. Please review the “Definition of Terms” to learn more.

You may have more links further down the page. These links will be for previous crashes and will allow downloading of the stored cores for those crashes. See the example below.

```
Minicontext region version: 1.0
Element size 1024, number of elements 64, index 3

Minicontext produced Mon, Aug 06 2007 22:06:08 UTC, HW code 0x0, SW code 0x6001A
Minicontext produced Fri, Jun 29 2007 15:20:15 UTC, HW code 0x0, SW code 0x6001A

Minicontext produced on Mon, Aug 06 2007 22:06:08 UTC
Minicontext version: 1.3
ProxySG Appliance: Version 4.2.4.1.29063
Hardware exception code: 0x0
Software exception code: 0x6001A
Page fault linear address: 0x0
Process "CLI_Worker_0" in "cli.dll" at .text+0xB7BBB
Register context:


  Link     CR3       EIP    EFLAGS    EAX       ECX       EDX     EBX
00000000 00C94000 0059DBBB 00200286 D8C897B0 0006001A FFFFFFFF D8C897B0
   ESP      EBP       ESI      EDI      ES       CS       SS       DS
D8C89690 D8C896BC D8C896D0 D8C897F4 00000000 00000000 00000000 00000000
   FS       GS
00000000 00000000


Call Stack:

Module "cli.dll" at .text+0x10A4AC
Module "cli.dll" at .text+0x10A7E6

Minicontext produced on Fri, Jun 29 2007 15:20:15 UTC
Minicontext version: 1.3
ProxySG Appliance: Version 4.2.3.26.28839
Hardware exception code: 0x0
Software exception code: 0x6001A
Page fault linear address: 0x0
Process "CLI_Worker_0" in "cli.dll" at .text+0xB67FB
Download context core 75,694,080 bytes          <--- Download link for this core image
```

Hardware platforms such as the 210, 510, 810, and 8100's have a table view.

System cores:

Time	Version	Hardware Exception	Software Exception	Page Fault Address	Process		
Tuesday June 26 2007 12:19:26	4.2.3.21.28657	0x0	0x6001a	0x0	Process "CLI_Worker_2" in "cli.dll" at .text+0xb67fb	Details; Minicontext (37888); Context (24651152); Full (295704952);	Delete
Wednesday May 30 2007 16:36:29	4.2.3.21.28657	0x0	0x60019	0x0	Process "CAG_Maintenance" in "con_agent.dll" at .text+0x2a49e	Details; Minicontext (37888);	Delete

If this is the case simply click on the appropriate link for "Minicontext", "Context", or "Full" and the file will download. (The file name will be "Context.cgz", "Context.cwz", or "Context.cwz.gz").

Files to Upload

(Maintenance > Service Information > Send Information > Send service information)

1. Context
    a. Sysinfo, Event log, Snapshots (all)
    b. Context
2. Full Core (older platforms)
    a. Sysinfo, Event log, Snapshots (all)
    b. Context
    c. Memory Core
    d. Packet Capture (if applicable)
3. Full Core (newer platforms)
    a. Sysinfo, Event log, Snapshots (all)
    b. Full Core
    c. Packet Capture (if applicable)

Note Concerning Uploads:
When the SG is configured to write a full core the newer platforms such as the 210s, 510s, 810s, and 8100s will write a single file called "full" which contains both the context and memory core. The older platforms such as the 200s, 400s, 800s, 8000s will write a context and separate memory core file (2 files). In the case of the older models both the context and memory core must be uploaded as together they comprise the "full" core.

Full Core with Packet Capture Included

1. Set core type
    a. Click Maintenance > Core Images
    b. Click the radio button to set the core image to "Full"
    c. Click APPLY to store these settings.
2. Set the proxy restart mode
    a. SGOS 5.x
        i. Click Maintenance > System and Disks > Tasks
        ii. Click "Hardware & Software"
    b. SGOS 4.x
        i. Click Maintenance > General
        ii. Click "Hardware & Software"
    c. Click APPLY to store these settings.
3. Setup a packet capture
    a. Click Maintenance > Service Information > Packet Captures
    b. SGOS 4
        i. Check "include" and set this to 1024 (will store 1M of capture data in the core file.)
        ii. Select “Capture last” and set this field to 200000
        iii. PRESS APPLY to store these settings
        iv. Click “Start capture”
    c. SGOS 5
        i. Click “Start capture”
        ii. Check “include” and set this to 1024
        iii. Check “capture last….matching packets” and set this to 200000
        iv. Click “Start capture”
    d. Let run until restart happens and full core is written

Note: A full core may take as much as 5-20 min, depending on hardware and the amount of memory.

Quick Reference

1. Set the proxy restart mode
    a. SGOS 4: Maintenance > General
    b. SGOS 5: Maintenance > System and Disks > Tasks
2. Set core type
    a. Maintenance > Core Image
3. Allow system to automatically restart
4. Download context and memory core from: https://x.x.x.x:8082/CM/Core_image
5. upload.bluecoat.com – include sysinfo, event log, snapshots (all)

If the system settings already match sections 1 & 2 and restart has already occurred

1. Download core from: https://x.x.x.x:8082/CM/Core_image
2. upload.bluecoat.com - include sysinfo, event log, snapshots (all)

Options for forcing a core image

1. Command Line Interface (CLI): **restart abrupt**
2. Serial Session: **ctrl+x ctrl+h**

Definition of Terms

Full Core	Written only by the newer platforms such as the 210s, 510s, 810s, and 8100s. Contains the data structures that are missing in the context and is made up of the context and memory core in one easy file. Requires 10-20 minutes to complete. Most comprehensive core available.
Memory Core	Written by older platforms such as the 200s, 400s, 800s, 8000s. Contains data that is missing in the context. A memory core must be matched up with the right context (both would be needed). As mentioned before we only configure for “full” or “context”. In this case the “full” core is made up of a “context” and “memory” core.
Context	A partial dump of the system memory. Contains the data structures minus the data.
Minicontext	Short text output logged in the sysinfo at the time a core is written containing running processes and restart codes as well as other functions helpful to support. Normally you won’t be asked to provide this as it is contained in the sysinfo, but there are occasions when you may be requested to obtain this manually from https://x.x.x.x:8082/CM/Core_Image
Restart	System crash. Normally referred to as a restart because when the system experiences a critical error it will automatically write a core image and “restart”.
CLI	Command Line Interface. Accessed via SSH to <proxyIPaddr> and port 22. Often a program such as “Putty” is used. Also accessible via a hyper-terminal or other terminal emulation such as TeraTermPro which makes use of the COM port for a serial connection to the SG. Simply connect the serial cable, open the COM port, and press enter 3 times to activate the CLI console.

Appendix G: How To…

Archive and Restore the ProxySG Configuration

It is always a good idea to backup the current configuration before making changes, especially major changes, to the ProxySG. The ProxySG configuration is stored in a single text file and can be backed up and restored with ease.

Backing up the Configuration

1. (optional) Request a copy of your license from Blue Coat in advance (1-2 days)
    a. You can license your box via the management console after the restore is complete.
        i. Maintenance>License>Install
            1. click “retrieve”
    b. However, just in case this fails for any reason it would be a good idea to have your license on hand so that you can install using the local file.
        i. mailto: support.services@bluecoat.com
            1. Contact Name
            2. Company Name
            3. SG serial number and operating system version.
2. Backup the “configuration-passwords-key” (see: “Export- Import SSL Keys”)
3. Backup non-default SSL keys (see: “Export- Import SSL Keys”)
4. Backup the system config
    a. Configuration > General > Archive > View Current Configuration
    b. Select “Configuration – expanded”
        i. If the archive will be restored to multiple systems then “post setup” is the better archive option. For more information see “Archive Types” at the end of this document.
    c. Click “View” (brings up the config in a new browser window)
    d. Save using your browsers FILE | SAVE function and save as TEXT

Restoring the Configuration

If this is a new system (no IP configuration) you must first make a connection to the SG via a serial cable and run through the initial setup wherein the IP information is configured. Then begin with step 1 below.

1. Launch the GUI management console
2. Restore the “configuration-passwords-key”. (see: “Export- Import SSL Keys”)
3. Restore other SSL keys. (see: “Export- Import SSL Keys”)
4. Download the content filtering database.
5. Restore the system configuration
    a. Configuration > General > Archive > Install Configuration from:
    b. Select “Local File”
    c. Click “Install”
    d. Browse to where you saved the backup system config file

e. Select and click “Open” and this initiates the install.
f. Wait and when it is finished it will tell you that it was successful.

Errors

Errors are reported for all types of reasons, but getting errors doesn’t necessarily mean the install wasn’t successful. Some errors may be expected. If errors are generated while restoring the archive be sure and save them (copy/paste to a text file) so that they can be examined later in the event something does not function as expected. The errors may help understand the cause.

Examples of expected errors:

1. Restoring the config before restoring the “configurations-passwords-key”.
    a. This will generate errors as the proxy tries to decrypt configured passwords and fails. However, the config will be restored successfully it just means those passwords will need to be set manually from the management console.
2. Restoring a config without first installing the content filter database.
    a. The archive may contain policy referencing content filter categories that do not yet exist. The configuration will be successfully restored, but the policy will not install until the content filter database has been downloaded.
3. Restoring network settings to an SG that already has network information configured.
    a. This will generate errors during the restore, however the configuration will be restored successfully using the existing network settings.

The key to knowing whether or not the restore was successful is to test to be sure that the proxy is functioning as expected.

NOTE:

Always check to be sure you “Default Proxy Policy” is set to what you intend (Allow/Deny).

Configuration > Policy > Policy Options

Archive Using the CLI

```
SGOS>en
Enable Password:
SGOS #config t
SGOS #(config)archive-configuration host x.x.x.x
SGOS #(config)archive-configuration protocol ftp
SGOS #(config)archive-configuration path //bluecoat/config
SGOS #(config)archive-configuration username <username>
SGOS #(config)archive-configuration password <password>
SGOS #(config)exit
SGOS #upload configuration
% Uploading ftp://x.x.x.x/bluecoat/config
  ok
SGOS #
```

FTP	protocol used to upload the configuration (ftp or tftp is available)
x.x.x.x	IP of the FTP server where you want to upload the configuration.
bluecoat/config	path off of the root directory on the ftp server to upload the configuration to
<username>	user name used to log into the ftp server
<password>	password used to log into the ftp server

Restoring the Configuration File Using the CLI

To restore a configuration file onto a Proxy SG using the command line interface the file needs to be located on an FTP server that is accessible by the proxy.

- Copy the configuration file from onto an FTP server if it is not on one already
- Using an FTP browser, locate the archived configuration to be restored and note the *URL*.
- Access the serial console of the proxy using SSH or direct serial connection
- Enter “enable” mode on the proxy
  #enable
- Enter enable password
- At the enable command prompt, enter the following command:

  SGOS#configure network "<URL noted earlier>"

  This will work if the FTP supports anonymous login.

For example

- #configure network ftp://x.x.x.x/archived-file-name.config
  If the above statement does not work try entering the URL in quotes
  #configure network “ftp://x.x.x.x/archived-file-name.config”

- If the FTP server requires username and password the username and password can be embedded into the URL. The format of the URL is: ftp://username:password@ftp-server
  where ftp-server is either the IP address or the DNS resolvable hostname of the FTP server.
  #configure network ftp://username:password@ftp-server/archived-file-name.config

Export-Import SSL Keys

The process discussed here is used for all SSL keys, but this section uses the “configuration-passwords-key” as an example as this is one of the SSL keys created on the SG by default and requires some extra explanation. It is also a good example of an SSL key that contains a dash (-) in the name which requires special handling on an SGOS 4.x ProxySG.

The “configuration-passwords-key” is used to encrypt the various passwords stored for use on the SG.

Examples of Encrypted passwords:

1. Administrator console passwords
2. Privileged-mode (enable) passwords
3. The front-panel PIN
4. Failover group secret
5. Access log FTP client passwords (primary, alternate)
6. RADIUS secrets
7. LDAP search password
8. Content Filter download passwords
9. SNMP read, write, and trap community strings
10. Etc, etc…

An SG’s archived configuration contains passwords which have all been encrypted with the existing configuration-passwords-key. Once the SG has been restored to a new state (reinitialization on a single disk system, restore to factory defaults, RMA, etc..) this key will be recreated, but it will not be the same key that was used to encrypt the existing passwords. Upon restoring the archive the SG will attempt to decrypt the passwords using its ***new*** configuration-passwords-key. Since this is not the key used to encrypt the passwords originally this process will fail (see ftp-client example below).

```
ok
10.78.1.136 - Blue Coat SG200 Series#(config log main)ftp-client
ok
10.78.1.136 - Blue Coat SG200 Series#(config log main)ftp-client
ok
10.78.1.136 - Blue Coat SG200 Series#(config log main)ftp-client
ok
10.78.1.136 - Blue Coat SG200 Series#(config log main)ftp-client
"gCxLXe+5DCTN0AprPT1R9ThiLIMPGQIMA05AKwXaEXTMd4xl
3cJNSjOu/tDD35GTH3tWjX0Uibn8dOeKLvkyZVtumKPbKzpFdZq
2hVAcvYWLiWVyw="
% Password could not be decrypted: RSA decryption failed.
A failure to apply an encrypted password indicates that you
may be attempting to apply passwords that were encrypted by
a different ProxySG. You will need to re-enter the password
on this ProxySG.
10.78.1.136 - Blue Coat SG200 Series#(config log main)ftp-client
ok
```

While the passwords can be manually reset one by one via the management console after the configuration has been restored it is possible to avoid this step by simply exporting the existing key and importing it again ***before*** restoring the configuration to the SG.

Export the SSL key

1. Enter enable mode and configuration terminal (config t)
2. ssl
3. view keyring
    a. listing of keyrings is displayed
4. view keypair des3 configuration-passwords-key
    a. enter an encryption password when prompted (remember this password…it will be used later restore the key)
5. Copy and paste the private key to a text file.

    Example:

```
BCSG#config t
Enter configuration commands, one per line.  End with CTRL-Z.
BCSG#(config)ssl
BCSG#(config ssl)view keypair des3 configuration-passwords-key
  Encryption key: *****
  Confirm encryption key: *****
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,E4C61B6B317608F8

JtC9mvmAn1uWAjxCH3LzKappqQ0DV9dsl0Am/HgZl6dQU9Ovzu71cc6xTZ36KZLV
UOGdy81FSrjhler8/hDK+7PkQXfnn3zHX+34FzIngNKpXHYqlpC7Sni1liXcjJdy
ZCuyipQp2tkcd8s6WCBZBvgFuL/NX6QTpHW2PQGRxadVPo3jIWc62LLQm4HnNcke
stsNRriRSpq519JuHOyzOZvz8p/K0WfyxMJ56hUsZEvLGkSoZe+1KgENan2xEwQR
7BX4CZi7/cpe1vRlVwq285kM0iO8gxTDyid1DIrClRtWF5+Ru4iLnlRlhicILDWG
IHnrXvgFBDFbmbv95pnhs94XUGmA768CHB8t0ZKMs1u+YWREWJTz6f4UrXxwm6JX
pi/vi9vuEzxdT7OqEmQRP7tghTE7YhQ8u6sP34AsTL1W8G51trGzCxaBabToeEh3
3QcNmJzF1DuapRCRAv9JiWMiX6IEOxZp//MvJfelvRHiNAKguiAXwX4e62q1ixW+
OryNLni4/iUh2IcIM/1lx0Y0LIR6tBGkXzqhUTHIyfi8Uv6lnUzifVMu8WLmy0iD
FGLpUZS7j1w7RK3x1Efjulx3lRzFdcvK63NsvQHnVWtirx4a8MYrxvGWf2KDMw4W
uizVCrBARXpKAaL5rSGqj+7h256t8DvZ7nky4ydHV4Pk+BLz8wPsiS7DAUp37fhj
r94sxeHWqF4dxRO5xqycJrs9SQ2t5ZlUXEaTg1AP1q7yhGVVBmEXVxhSD1PjxbAM
SDS/N26izAL355Np3dP3U2xkN1SZ5wjokBAS7X1FidV4A3J3PnPweg==
-----END RSA PRIVATE KEY-----
BCSG#(config ssl)
```

Below is the portion of the key that must be copied and pasted to a text file (including the BEGIN and END RSA PRIVATE KEY lines).

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,DA3B9D4E52B80997

5RI7qZLuQrGPCZ+l2ona+5ebJFJRJFWWOas+PO+lyZhdyOM3fwZBsXoQ/0eMOUvs
F4eq/KRnyQxIiVTOFBXYGv7Yw3T2DBjUepi+mFSWT+iPgvE2OaZmmP1F1DpGmB+q
tLpZID1XI77My+jUtzhr7dgzF2NFCo+iAKJ/vIgTVsM1A47SoAB1LdhXntPSafLx
wL+/BdfOS1C7VOwUMmU+xY7xs7DccnGHE/SoAaOaMxsoWPaCYeuoVcWGixOoUOVf
htMQamw6zeO3B1EQJE8DJnBmUWROvwHKxrI3iDDaqpu62h4dq8cvggyfi3a9q9BH
mxJQf1dSYOoyUwrfC+DSLNLZIF9UpYLooTTKPc7gr+cW1OX1O+A/mQ1NAOe3F7y9
eBxcrByeq75c86+mFn1Aq55qZ9WuyBae3T8iy8yuPoLIjS88MTwhf2j4+JQSCogE
e3MIl8cgsfdTKMGe5dydQFEr6RjOqqcBevdc1WspxvDPiLMfB1dJmtaEW915PNra
MCUh1P6CEQZJEcP9mcuo17EEZXm9dWz19YNpYiJdL9seRFKQL7aRnzCl6XOOoy1a
qMsCZJ6tn8XdrFxBRpZa/+/fwqxKUc815/PL1pyJ/8QNOcBzAwqy/UHu6YNPpOfO
bxXne+jcvRLyhFnxZmUO7A4jb9bQoXJjMzhkvlZnBwwJar3QUZEEbrUsVx5Mx8TJ
1ZCq5uSPw6qW1l21oPf1LwUbybbUCYDoMfNZHyE6SYPn3tQtjTLsZ6141qZxL7PC
Yh2COBQOHni6fn6vt3ujPh7cqaqNXRKlndryX/qdbJazHT11y4O+dQ==
-----END RSA PRIVATE KEY-----
```

Import the SSL Key

SGOS 4

The configuration-passwords-key on SGOS 4 must be restored via the CLI as the ***GUI will not allow the creation of a keyring with dashes (-) in the name***. This limitation does not exist in SGOS 5.

1. Launch the CLI
2. Delete the existing configuration-passwords-key

   ```
   #(config ssl)delete keyring configuration-passwords-key
   ```

3. Create a new configuration-passwords-key

   ```
   #(config ssl)create keyring show configuration-passwords-key
   ```

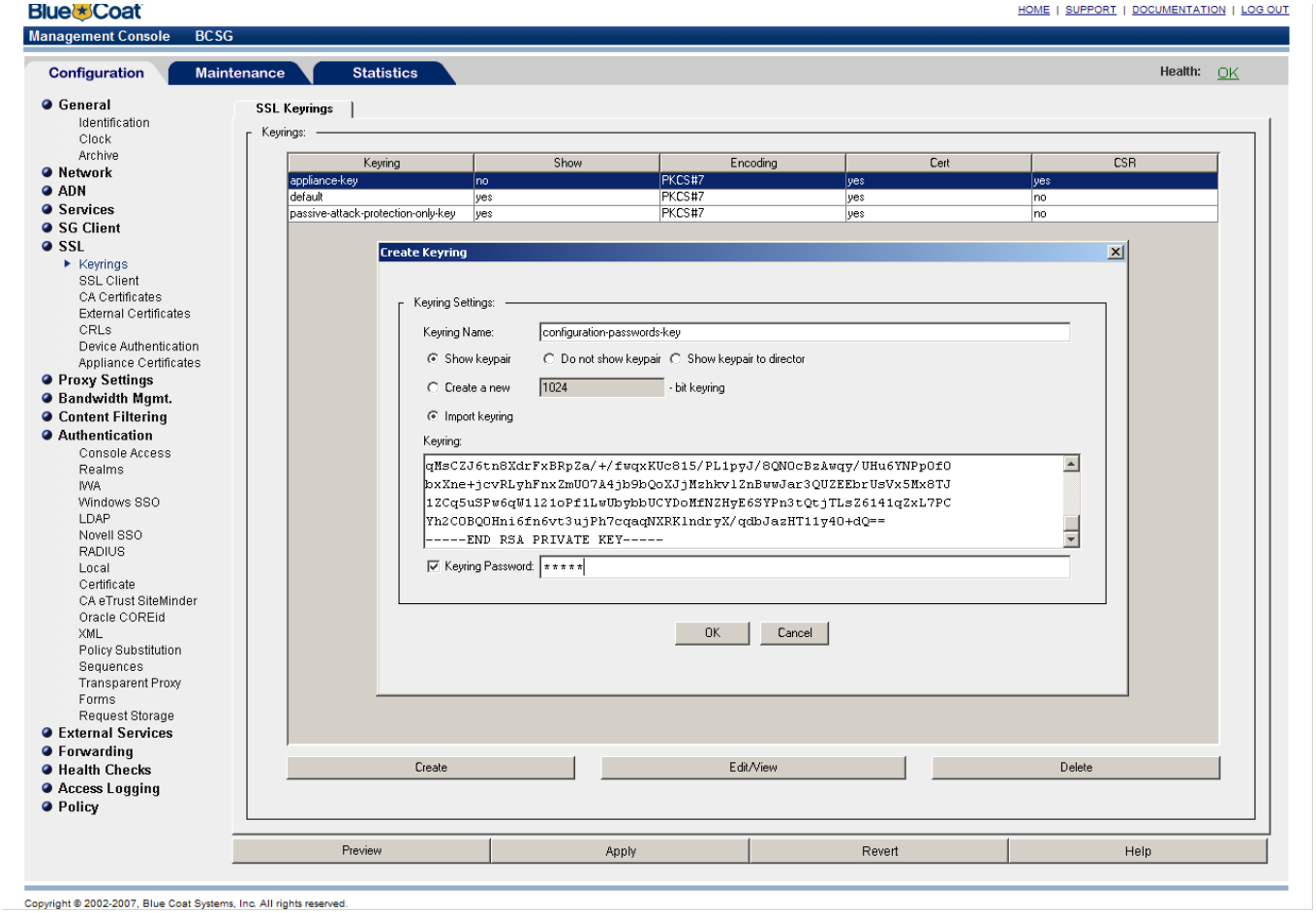
4. Import the original configuration-passwords-key
   a. This process is demonstrated in the example below. After typing “inline keyring show configuration-passwords-key eof” hit enter and then paste in the key just as it is shown below, hit enter again, and type “eof”. You will be prompted for a decryption key. This is the password used to encrypt the key with when it was exported. After entering the decryption key the keyring is successfully imported.

```
#(config ssl)inline keyring show configuration-passwords-key eof
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,7430D2F9F2DDD0E5

tSBcWWxNIYfbTGp1HXNPEtS7SSMg6+74szejiKMpAs9dtQyLdEkW6F3o1dqdiknH
9v0ObWnWaPF4FXQp/141d6wv2JFeZMAVusU+GUkUD0BScaLwf2LZ5oLkjuBV3BdI
qPNODHyUW50GqTWmiZRPgOAf+WeuvcBVCCHFzt+Ne5r0DcY3E6Gl6R+PSyMzf0ap
MZRzMYrAgHwkrbVz2v4ANQkkDp9NET3nktl2C4B2IQec0dhWzeA9agLE2lYerrxt
uyDsrGlJBXluZ0pZIMtgdYwbTdqWZU+p7jsYZF9FuqshUFLsV4PrsUqobZqz7zj1
lPurQyXppGD6s10QItyrd/fb7ebCnERvmH5wcKl91vQBTuG7gTHaNH6VocSiYFrK
Z4Vv7Q2dkmA0e27K2w+MHHbJ2Tdn2cs31plvowpsK0vcpmuZHYAQNHIJwgMKhpoH
8SH1iQqb/0ooxrbgBlQ8ocnAuwKDx8e/kalCb2T+dqeftPTAVK1MBZSldUFsIP2g
02LLqMaP4ISUrOOdcsgU/tLUaK46JRb62S8tPtyXIB1jnEBkqWZRpy9JUxllxExv
pEXYrzdf/tqxzWyFSgcpu8HbVFOzgQZjwPDNuYEYNcfSb9DXq5IT6nX5q3MKo97r
aoi7xX1M/VVsRnfwmwdKhzNDRVpSpFSyp48VmCvWPQ+cV9PwjplSiY3MoY3tdjjq
RvzN0xwoPUJ8p+IEhpjzjdWrgLDq1AVmjQnyOoF/o59YGhKm0YBkPcVyVvO/BV4x
iAMQOAxNcFna85lo3N0NJS8svoZ6Ro/Pd/GY8EcHV8t3Ttpv99qC1g==
-----END RSA PRIVATE KEY-----
eof
  Decryption key: *****
  Confirm decryption key: *****
  ok
```

SGOS 5

1. Launch the Management Console
2. Configuration>SSL>Keyrings
3. configuration-passwords-key
    a. delete the existing key (click apply)
    b. create a new one using the exported key
        i. Keyring Name: configuration-passwords-key
        ii. Select “Show keypair”
        iii. Leave the default “1024” –bit keyring
        iv. Click “Import keyring
        v. Paste configuration-passwords-key in the “Keyring:” box
        vi. Enter the password used to encrypt it in “Step 4a” above.
        vii. Click “OK”
        viii. Click “Apply”
4. The configuration-passwords-key is now successfully imported.



Reinitializing the Disk(s) on the ProxySG

There may be times when a disk reinitialization is necessary to correct certain problems.

Single Disk System

1. Backup the system configuration and SSL keys (*Appendix G*)
    a. Serial cable to the proxy and launch the CLI
        i. SSH will not work for this operation as the entire configuration will be lost including any network settings.
        ii. One option when doing this remotely would be to connect a serial cable between the SG and a local PC or server. Then remote into that PC or server and launch a terminal session to the SG (proterm, hyperterminal, etc).
    b. Enable mode
    c. Type: reinitialize
2. Run through the initial setup via CLI
    a. When the proxy finishes the reinit on the disk it will reboot and come back up as a new system devoid of any IP information. A network connection (SSH) will not be possible.
3. Restore the system configuration and SSL keys (*Appendix G*)

Multiple Disk System

It is much simpler to reinitialize a multiple disk system. This process can be done during production hours without impact to production, however, unless absolutely necessary it is best to perform a reinitialize operation during low traffic or off hours.

1. Backup the system configuration and SSL keys (*Appendix G*)
2. Reinitialize the disks one at a time
    a. Use the “slot number” for reference when reinitializing disks. Start with slot 1 and work up. Be sure to look over the “Sysinfo” file to review what the actual slot numbers are.
        i. https://<x.x.x.x>:8082/sysinfo
        ii. Under: “Hardware Information”
    b. Launch the CLI (ssh or serial)
    c. Enable mode
    d. Type:
        i. disk reinitialize 1
            1. Wait until it finishes
            2. Check the event log for disk related errors and save as “reinit-1.log”
                a. https://<x.x.x.x>:8082/eventlog/fetch=0xFFFFFFFF
                b. save the log using the browser save function
        ii. disk reinitialize 2
            1. Wait until it finishes
            2. Check the event log for disk related errors and save as “reinit-2.log”
                a. https://<x.x.x.x>:8082/eventlog/fetch=0xFFFFFFFF
                b. Save the log using the browser save function
    e. Upload the event logs: upload.bluecoat.com

The process for reinitializing is normally quick and problem free. Each disk on the SG contains a copy of the system configuration (mirrored). When a disk is reinitialized it is taken off-line. When this happens the ProxySG will automatically use the next active disk as primary and continue processing traffic. This continues until all disks have been reinitialized.

In the event a problem does occur and for some reason the configuration is lost during a reinitialize then it will be necessary to restore the system configuration from backup (*Appendix G*).