SecureSphere Deployment Note

Networking and High Availability

Imperva SecureSphere appliances support a broad array of deployment options, enabling seamless integration into any data center environment. SecureSphere can be configured as a transparent bridge or a non-inline network monitor (sniffer). In addition, the SecureSphere Web Application Firewall supports reverse proxy and transparent proxy deployment. Because of this flexibility, customers can roll out comprehensive application-level security without changing their data center infrastructure. There is no need to reconfigure IP addresses, routing schemes, or applications—allowing SecureSphere to easily drop into any network.

The SecureSphere appliances protect critical business applications and database servers. Therefore, high availability is an essential customer requirement. To meet this requirement, Imperva offers a range of options that ensure business continuity and application availability.

This deployment note describes several networking scenarios and the corresponding high availability configurations for each scenario, including:

- **Transparent Bridge Configuration**
  - Active-Passive Failover in a Redundant Architecture
  - Active-Active Failover in a Redundant Architecture
  - Fail-open Architecture
  - Active-Passive and Active-Active Failover with IMPVHA Protocol
  - Link Aggregation
- **Network Monitor (Sniffer) Configuration**
  - Non-Inline Deployment
  - Non-Inline with Redundant Gateways
- **Transparent and Reverse Proxy Configurations (Web Application Firewall only)**
  - Load Balancer Integration
  - Active-Passive Failover

This note also describes the criteria customers can use to determine the best network and high availability configuration for their environment.

Transparent Bridge Configuration

Active-Passive Failover in a Redundant Architecture

In this scenario, two SecureSphere gateways are deployed in an existing highly available architecture. Since each SecureSphere gateway is configured as a layer 2 bridge, any failure to SecureSphere appears to the network simply as if a switch port has failed. Connected devices would recognize that the SecureSphere gateway was not reachable and would automatically redirect traffic around it.

Data inspection and analysis is performed through a powerful Transparent Inspection engine, so SecureSphere does not need to terminate or rewrite HTTP requests. TCP connections are negotiated directly between the client and the back-end server. Therefore, a failover event does not disrupt TCP connections or affect user sessions.

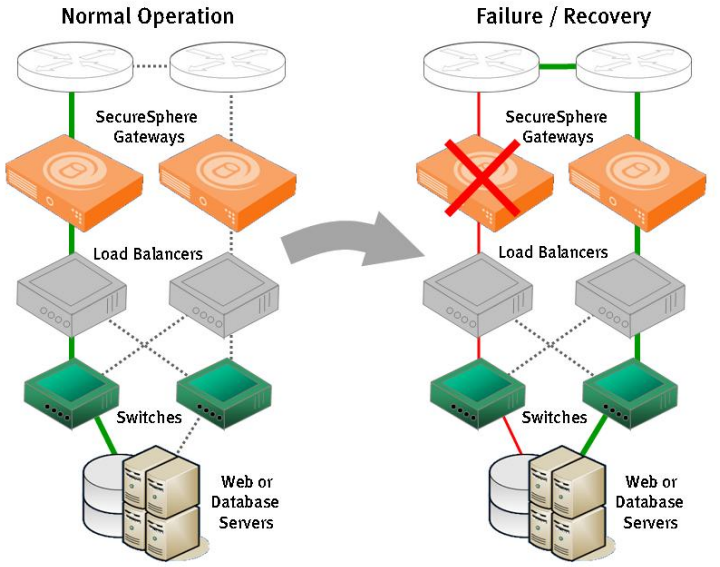


Diagram of Active-Passive Failover in a Redundant Architecture

Active-Active Failover in a Redundant Architecture

In this deployment scenario, redundant SecureSphere gateways are again deployed in an existing highly available architecture. The only difference is that both gateways transmit traffic simultaneously.

Since SecureSphere is configured as a layer 2 bridge, any failure to SecureSphere appears to the network simply as if a switch port has failed. Connected devices would recognize that the SecureSphere gateway was not reachable and would automatically redirect traffic around it.

As a bridge, SecureSphere transparently inspects traffic without terminating TCP connections. So a failover event does not affect user sessions or disrupt TCP connections between the web or database server and the client. Since one SecureSphere gateway has failed, total network capacity will be reduced until the failure is corrected.

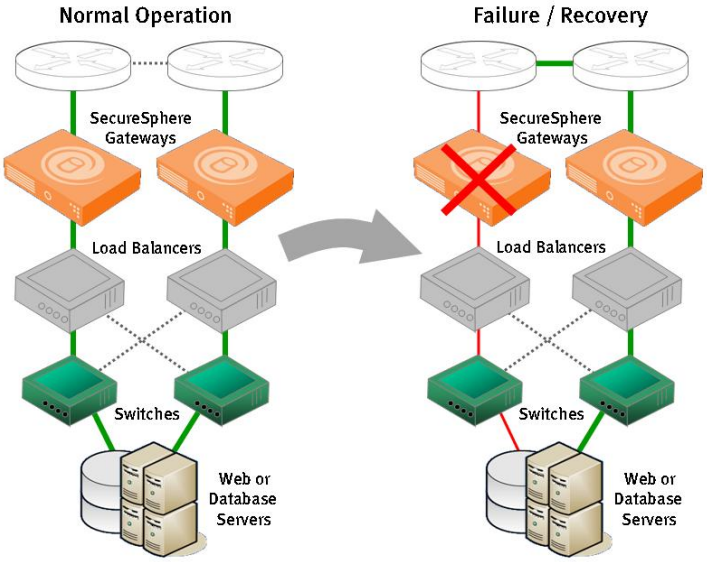


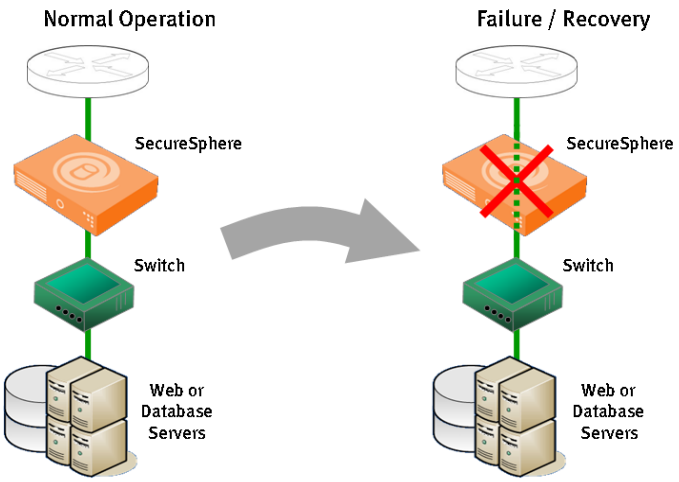
Diagram of Active-Active Failover in a Redundant Architecture

Fail-open Architecture

Fail-open bridge configuration preserves uptime without the cost or management effort of building a redundant architecture. In this scenario, SecureSphere is deployed inline in front of the protected application servers.

In the event of a software, hardware, or power failure, SecureSphere's specialized network interface card will detect the failure and physically complete the connection through the SecureSphere gateway. The NIC card will fail open in milliseconds, minimizing network downtime.

However, application servers will not be monitored or protected from attacks until the SecureSphere gateway resumes operations.



Fail-Open Architecture Diagram

Active-Passive and Active-Active Failover with IMPVHA Protocol

Imperva developed a proprietary redundancy protocol for environments that do not have a redundant network architecture and Spanning Tree Protocol (STP) cannot be implemented. For some customers, STP convergence times may be unacceptably long or STP may conflict with existing protocols, such as Rapid Spanning Tree Protocol. For these situations, the Imperva High Availability (IMPVHA) protocol is the ideal solution.

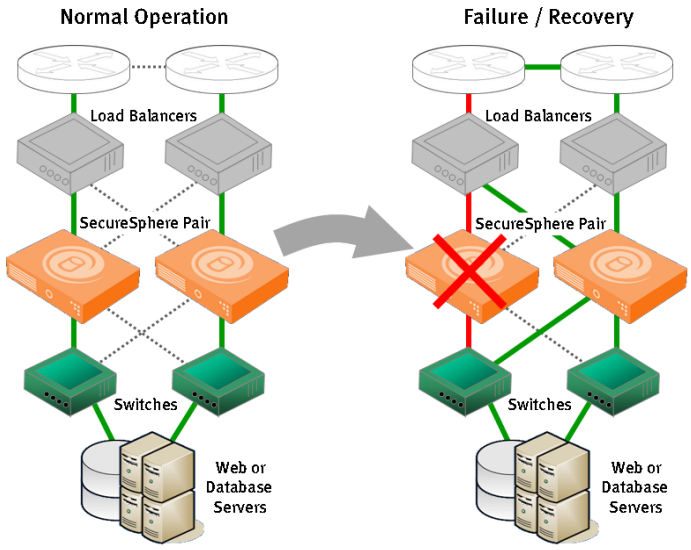


Diagram of Active-Active Failover using IMPVHA

With IMPVHA, two SecureSphere gateways can be configured as layer 2 bridges in either active-passive or active-active mode. The configuration and failover mechanism is similar to VRRP, except that when a failover occurs, the backup device informs connected devices to redirect traffic via ARP requests rather than assuming the primary device's IP address. When an IMPVHA pair is deployed, the backup gateway will send periodic loopcheck broadcast messages. If no response is received within the configurable failover time (default is 0.5 seconds), the backup gateway will become active.

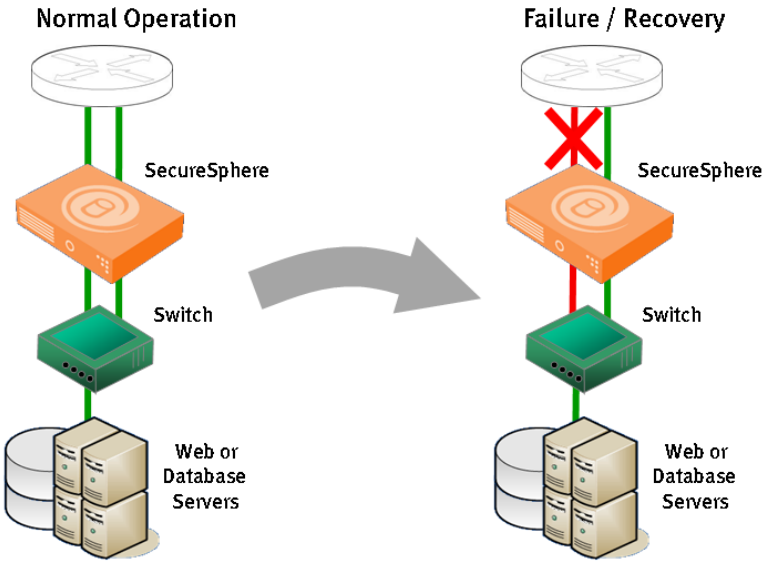
Since a SecureSphere gateway supports two bridges through its four network interface cards, it is possible to configure one bridge as the IMPVHA primary for one network and the second bridge as a backup for another network. In this configuration, two SecureSphere gateways can support an active-active failover configuration.

Link Aggregation

One or more SecureSphere gateways can support link aggregation. For example, two interfaces on a SecureSphere gateway can be connected to two interfaces on a network load balancer. Traffic can pass through both connections. For example, uplink traffic can travel through the first interface card while downlink traffic goes through the second interface card.

In bridging mode, each SecureSphere gateway includes four network interfaces for application security. So it is possible to aggregate traffic through two connections. If the load balancer has 100Mbps Fast Ethernet interfaces, then aggregating links can also increase total throughput. Even if the traffic is split between the two segments, SecureSphere can accurately inspect all traffic and block attacks.

If an Ethernet cable is disconnected or a network interface fails, then traffic will continue to be forwarded through the active link on the SecureSphere gateway.

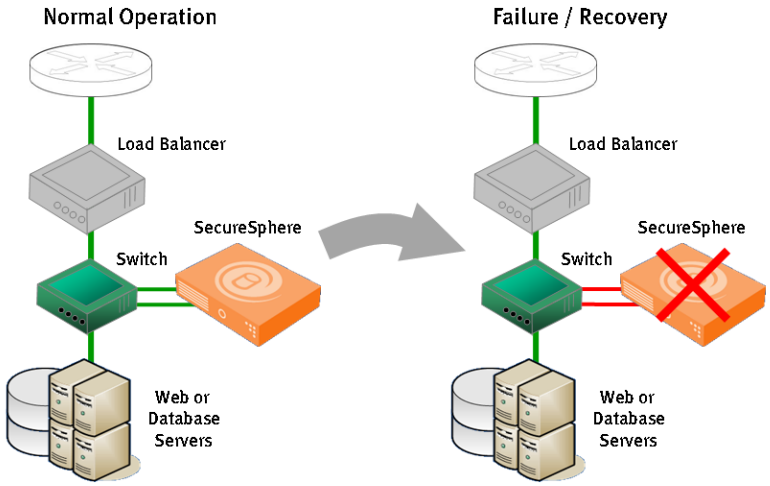


Link Aggregation Diagram

Network Monitor Configuration

Non-inline Deployment

Configuring SecureSphere as a network monitor enables organizations to protect critical servers without introducing a new point of failure. It is a lower price alternative to deploying to or more redundant SecureSphere gateways. To deploy SecureSphere as a network monitor, connect it to an open SPAN port or a network TAP to observe traffic. A second connection to an active port on the switch allows SecureSphere to block malicious connections by sending TCP resets to both the server and the client involved in the session. In the event of a SecureSphere gateway failure, network traffic is unaffected. However, traffic will not be monitored or protected until the SecureSphere gateway becomes operational again.

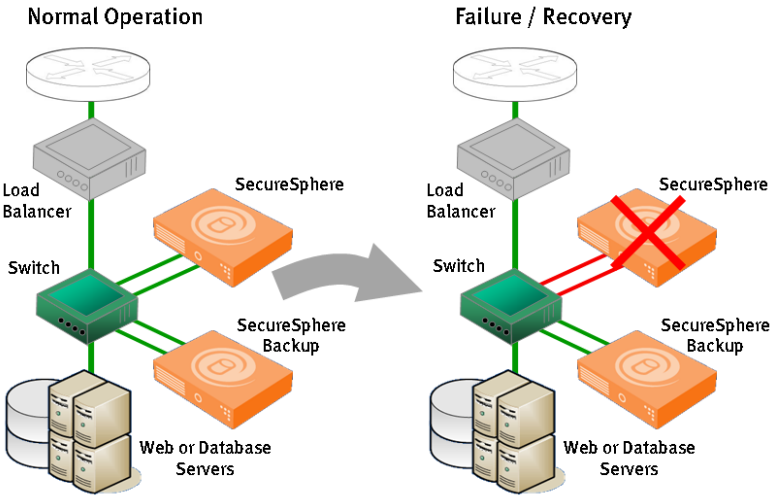


Non-Inline Deployment Diagram

Non-inline with Redundant Gateways

For some organizations, it may be imperative to monitor and audit all Web or database traffic without disruption. These organizations can deploy multiple SecureSphere gateways in non-inline mode. If one of the gateways fail, the other gateway will continue to monitor and record traffic.

In this configuration, each gateway should be managed by a separate MX Management Server or by using the integrated software management option.



Non-Inline Deployment Diagram with Redundant SecureSphere Gateways

Transparent and Reverse Proxy Configurations *(Web Application Firewall only)*

SecureSphere is often deployed as a direct replacement for legacy reverse proxy appliances. In most cases, customers choose to configure SecureSphere as a bridge because it fits into the existing architecture and reduces the operational burden associated with Web proxies. However, in some cases, customers deploy SecureSphere as in proxy mode to meet architectural requirements or for content modification.

The SecureSphere Web Application Firewall supports both reverse proxy and transparent proxy configurations. Both proxy configurations offer content modification, including cookie signing and URL rewriting. Transparent proxy mode enables transparent deployment without network or DNS changes.

Load Balancer Integration

In proxy mode, one or more SecureSphere gateways are deployed as either a reverse proxy or a transparent proxy. A load balancer balances the traffic between the gateways and the gateways forward the traffic to the Web servers. It's possible to configure load balancer to work in active-active or active-passive modes.

In this mode, the IP address of the Web site resolves to the SecureSphere gateway's IP address. If SSL is used, then the gateway should be configured to terminate the SSL connection. Note that in proxy mode, SecureSphere establishes a new connection to the Web server on behalf of the client.

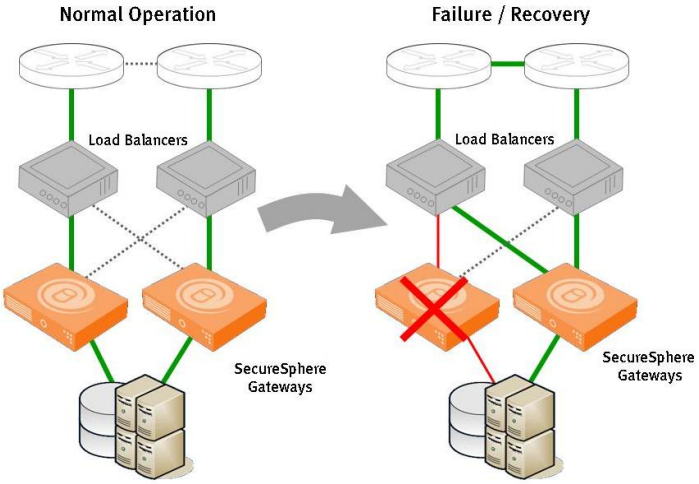


Diagram of Proxy Mode with Load Balancer Integration

Active-Passive Failover

VRRP also provides redundancy for two or more SecureSphere gateways configured as reverse or transparent proxies. In this deployment scenario, two SecureSphere gateways are deployed as proxies. The gateways are configured as a VRRP pair (Virtual Router Redundancy Protocol).

When the active SecureSphere gateway becomes unavailable, the passive gateway assumes the IP address of the failed gateway and becomes active.

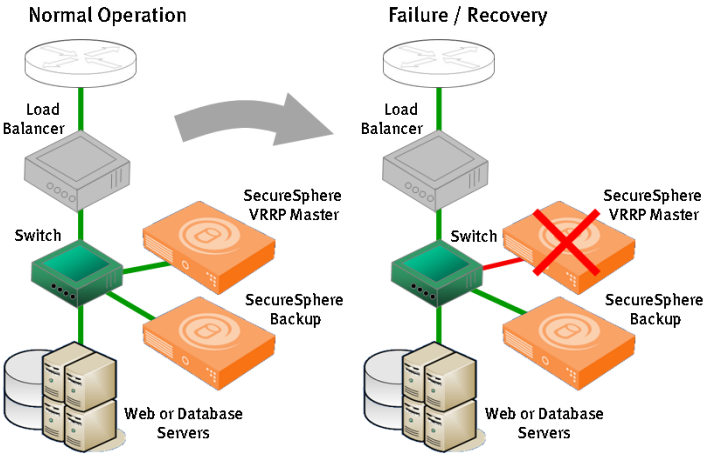


Diagram of Active-Passive Failover in Proxy Mode

Summary of Network Configuration Modes

The best-in-class SecureSphere application security appliances support a wide array of deployment options. SecureSphere customers can select the best deployment scenario based on their network, high availability and ongoing maintenance objectives.

So which configuration mode would best suit your needs? That depends on your data center architecture, your business applications, and your performance and operational requirements. For example, if you wish to encrypt cookies or rewrite URLs, you can configure SecureSphere as a proxy. If line speed performance and zero impact deployment are important, then deploy SecureSphere as a layer 2 bridge.

The table displayed below describes which network configuration mode you should choose based on your existing network infrastructure and applications and your performance and high availability requirements.

Configuration Mode	When to Use
Bridge	• When transparent deployment is required – Provides drop-in installation – Layer 2 operation is transparent to most networks and applications • For high performance environments
Proxy	• For seamless replacement of legacy application proxy deployments, cookie signing, and URL rewrite • Transparent proxy option for content modification with no network changes
Network Monitor	• For risk-free evaluation and pilot projects • To avoid adding new devices to the network – The appliance is not inline and won't impact the network • When only monitoring and reporting functions are needed

3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065
Tel: (650) 345-9000
Fax: (650) 345-9004