Technology Brief

Firewall Load Balancing

High-Availability.Com Limited
Grenville House,
Unit 1,
Haig Court,
Knutsford,
Cheshire,
WA16 8XZ,
United Kingdom.

http://www.High-Availability.Com

Normal hours       +44 (0)1565 754459
Outside hours      +44 (0)1565 754453
# Table of Contents

1 Executive Summary ................................................................................................. 5
2 The Basics .................................................................................................................. 6
  2.1 What is load balancing? ......................................................................................... 6
      2.1.1 Load Sharing .............................................................................................. 6
      2.1.2 Load Balancing ......................................................................................... 6
  2.2 Why load balance? .............................................................................................. 6
      2.2.1 Sound Technical Reasons for Load Balancing Firewalls ......................... 6
      2.2.2 Idealistic, non-Technical Reasons for Load Balancing Firewalls ............ 6
  2.3 Applications to be load balanced ....................................................................... 7
3 Technology ................................................................................................................ 8
  3.1 The Principle Methods of Implementing Firewall Solutions ............................ 8
      3.1.1 Stand alone (not load balanced) ................................................................. 8
      3.1.2 Independent Servers .................................................................................. 9
      3.1.3 Hot Standby .............................................................................................. 10
      3.1.4 Forwarding Node .................................................................................... 10
      3.1.5 Ethernet Trunking ................................................................................... 11
      3.1.6 Active/Active Separate Identities ............................................................. 12
      3.1.7 Active/Active Common Identity ............................................................... 14
      3.1.8 Static Load Balancing ............................................................................ 14
      3.1.9 Mediated Solution .................................................................................... 15
  3.2 Performance .......................................................................................................... 16
      3.2.1 Failover times ......................................................................................... 16
      3.2.2 State Table Synchronisation ................................................................. 17
      3.2.3 Connection based mediation - in firewall ............................................ 17
4 Papers Findings ......................................................................................................... 18
  4.1 Super High Performance - Greater than 280Mb/s ......................................... 19
  4.2 High Performance - 160 to 280Mb/s ............................................................... 20
  4.3 Good Performance - 50 to 160Mb/s ................................................................. 21
  4.4 Standard Performance - up to 50Mb/s ............................................................. 22
List of Figures

Figure 1 - Stand Alone Firewall ................................................................. 8
Figure 2 - Independent Servers ............................................................... 9
Figure 3 - Hot Standby ............................................................................ 10
Figure 4 - Forwarding Node ................................................................... 11
Figure 5 - Ethernet Trunking ................................................................. 12
Figure 6 - 3.1.6 - Active/Active Separate Identities ................................. 13
Figure 7 - Active/Active Common Identity ............................................. 14
Figure 8 - Static Load Balancing ............................................................ 15
Figure 9 - Mediated Solution .................................................................. 16
Figure 10 - Mediated Trunked ................................................................. 19
Figure 11 - Static Trunked ....................................................................... 20
Figure 12 - Trunked Hot Standby ......................................................... 21
Figure 13 - Hot Standby .......................................................................... 22
1 Executive Summary

This paper provides the reader with a comprehensive technical understanding of the complex issues surrounding the principles and practice of firewall load balancing and deployments. There is quite a lot of misconception around the technical solutions and advantages to these solutions, this paper attempts to uncover the myths in an objective and balanced view. Whilst prepared by High-Availability.Com the company’s products are not always shown as the most appropriate for all circumstances.

The fundamental message is to understand the customers need in terms of reliability and performance. If we assume that reliability is considered to be an issue, because you are reading a paper published by High-Availability.Com then we can move directly to equating the customer’s performance requirements with the available solutions. This paper details the available solutions and the following table represents a summary of the solution viable for each performance band.

<table>
<thead>
<tr>
<th>Bandwidth</th>
<th>RSF-1</th>
<th>NetMon</th>
<th>Mediation Device</th>
<th>Trunking</th>
</tr>
</thead>
<tbody>
<tr>
<td>up to 50 Mb/s</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50-160 Mb/s</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>160-280 Mb/s</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>280 Mb/s+</td>
<td>optional</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Trunking is a feature available with most operating systems, sometimes with the addition of an additional package. Trunking is described in 802.3ad allows Ethernet segments to be aggregated together. Use of Ethernet trunking does rely upon a trunked device being connected directly to another host or switch which also supports trunking. Trunking does not provide failover capability and can not be used if all connections do not attach to the same switch but a similar result can be achieved using NetMon and trunking in tandem.

Consideration should be given to the future needs of an organisation when recommending a solution but the investment in most solutions will not be lost if the customer finds that he must upgrade equipment.
2 The Basics

2.1 What is load balancing?

There are a number of terms used to describe the spreading of load among servers. Two key terms are used that are subtly different:

2.1.1 Load Sharing

Load is shared between multiple servers by some mechanism which may be static or fairly dynamic but the result is not predictable, in that load may be shared unequally between the servers.

2.1.2 Load Balancing

Dynamic sharing of load between servers, possibly on a per session basis. Almost always using 'sticky' paths, where traffic will continue to flow via a particular route for the duration of a session. This provides a much better chance of load being evenly balanced between nodes but does require any active process CPU cycles, to perform the balancing.

There is little question that load balanced solutions will be more likely to provide a more even spread of load between servers. However, understanding if this is useful, i.e. actually adds value, is a little more pertinent, and should be assessed by understanding if the solution is technically more robust and more performant. There is also a case to be made for scalability; what fits now should be able to grow bigger without radical change - ideally.

This paper will show there are a number of 'good' designs depending on the budget and performance requirements of an organisation. Some solutions offer improvements that have no genuine technical merit but do offer a 'feel good' factor.

2.2 Why load balance?

There are a number of reasons that a company may wish to load balance traffic across firewalls. However, they largely fall into two distinct categories:

1. **Sound technical reasons**
2. **Idealistic, non-technical reasons**

The first are genuine concerns that should be addressed where funds and environment allow whereas the second provides a 'feel good' factor which can be important in winning business but has no technical merits.

2.2.1 Sound Technical Reasons for Load Balancing Firewalls

- Traffic volume exceeds wire-speed
- Traffic volume exceeds capacity of a single machine
- Reducing failover/recovery times
- Improving the reliability of connections
- Reducing transit delay by spreading the load

These reasons can be condensed into two fundamental issues: bottlenecks and resilience.

2.2.2 Idealistic, non-Technical Reasons for Load Balancing Firewalls

This list of reasons for a company wishing to load balance firewall traffic, has no genuine technical merit and/or detracts from achieving sound technical solutions.

- Spreading the load evenly
- Making best use of all company equipment
- Easing network management
Easing network management is a worthy aim but introducing a more complex solution, as load balanced firewalls are, does not do this in a transparent manner.

Implementing a simple solution which is no less reliable or performant than a complex solution is normally preferable. Where the simple solution also costs less and is easier to implement and manage then there is a clear case for 'Keep It Simple' (K.I.S.). However, there are times when a more complex solution offers genuine benefits in reliability and performance, where there is a need (real or perceived) and funding available then there is a clear case for providing this more complex solution.

Complexity is not just about the ease of implementation, it is also important to understand the underlying mechanisms, indeed a solution may be simpler while the implementation is more complicated. The overall assessment of complexity is fairly subjective but should include implementation costs, standards reliance, other affected systems and the number of CPU cycles required to perform operations.

2.3 Applications to be load balanced

This paper is focused at firewall solutions but it is useful to have a slightly wider understanding of the issues involved, this brief section will introduce the wider issues.

In principle an application that does not rely on a single data source which can (or should) only be accessed by one application / server at a time is suitable for load balancing. Ask yourself these simple questions when trying to make the assessment;

1. Is there a single data repository where any machine or application requires an exclusive lock on that data?
2. Is the application a stateless application (see HAC White Paper on Statefull / Stateless Applications)?

Here are some examples of applications which can successfully be used with load balancing;

1. Firewalls (most notably Check Point’s FireWall-1)
2. Web Servers
3 Technology

3.1 The Principle Methods of Implementing Firewall Solutions

This section shows most popular methods of implementing firewall solutions. Diagrams are used to aid the text. Check Point’s FireWall-1 and Alteon WebSwitch AC-3’s are used as reference equipment but can be substituted for other vendor equipment. For the firewall it is assumed that another vendor solution will have session synchronisation, like Check Point’s State Table Synchronisation, setup between firewalls, where there is a bold black arrow shown between the firewalls. Where the equipment is shown faintly, this indicates that it is running in standby mode.

The scope of this document does not include general network design and such matters as alternative Internet Service Providers are not addressed in this paper, although do have elegant solutions for such matters. Please contact us further to discuss this level of detail.

The top cloud in each diagram represents the outside world, usually via ISP. At the base of the diagram are two routers and an Ethernet segment, these routers are often not installed, instead the clients on the inside of the network use the firewalls as their routers. The routers at the top of the diagram are often provided by the ISP and can not be configured by the customer/user.

The solutions are presented in cost order, cheapest first and most expensive last. This is approximately equivalent to value order as well but there are a couple of anomalies, most notably that of the Shared Identity Solution, which is less effective than a Hot Standby solution.

3.1.1 Stand alone (not load balanced)

This is the most common solution for small businesses that have implemented a firewall. Simple and cost effective.
As there is only a single path for all traffic configuration is simple and quick, with all internal users having router/firewall as their default gateway. The most striking feature of this design is the multiple points of failure, so this design needs to be enhanced.

Included for completeness

| Perf | VFM |

### 3.1.2 Independent Servers

This *solution* is achieved by installing a parallel configuration of equipment. Simple to install and cost effective, more complicated to actually get working usefully. Both firewalls are capable of passing traffic but rely on internal users deciding which firewall to use, external users and replies to NAT addresses can be effectively controlled by using different NAT addresses on each firewall.

![Figure 2 - Independent Servers](image)

There is no fail over, in the event of a fault, without manual intervention and sessions will be lost. The re-configuration to deal with faults could be performed either with all the clients or by an administrator at the firewalls. Again this solution will work but is less than a professional approach to providing quality service to users.

Included for completeness

| Perf | VFM |
### 3.1.3 Hot Standby

The classical deployment for firewalls. Simple and cost effective to implement, minimal CPU overhead and transit delays but restricted to wire-speed and can not realistically be scaled up beyond the capacity of wire-speed and machine throughput limits.

One IP address per subnet, normally a VIP, is automatically configured by a suitable software clustering solution, like RSF-1. The routers and clients forward packets to this VIP, which may be on a machine in the cluster. In the event of a failure the clustering software will recognise the failure and may decide to move the VIP to another machine. Connections through the firewall and VPN tunnels are failed over transparently to the standby server which becomes the primary server.

This configuration provides up to wire-speed throughput capability, minimal CPU overhead and an easy to implement and maintain solution. As a result it is by far the most popular configuration. However, for customers needing to cater for higher than wire-speed levels of traffic then this solution is not suitable as shown. The disadvantage of this system is that only one firewall, despite how many are clustered together, is active at one time and this limits the scalability.

One point that is often considered is the standby machine. It would appear that this would be better employed if it were actively being used, this is in principle true but relies upon one of the alternative solutions here and in most cases. This point should be reviewed by the reader after finishing this document, however, which will show that whilst in principle it a good idea, in practice a more performant and reliable system is achieved using hot standby than a number of other solutions.

### 3.1.4 Forwarding Node

This fairly new model is a twist on standard redirection and standard mediated devices. Transit delays are increased and traffic is increased because the majority of traffic will pass through one switch
twice. The maximum bandwidth of this solution is wire speed or half of the Ethernet switch backplane, whichever is lower.

Figure 4 - Forwarding Node

All nodes are configured in a common cluster and one is 'elected' as the 'pivot' node, which has both the internal and external VIPs, so all traffic is sent to this node. If the node fails another node will be 'elected' as the pivot node and will take on the VIPs. The pivot node can process traffic in the normal way, but most traffic will be forwarded to other nodes in the cluster for them to process.

One serious drawback with this solution is that the current solution (ClusterXL from Check Point) does not provide multiple independent heartbeat paths. In fact the solution uses just the one type of heartbeat (multicast) typically on a private LAN. This is a new single point of failure, which could result in little or no traffic being passed should a fault of some kind develop on the private LAN or one of the nodes.

This configuration typically provides up to half wire-speed throughput capability and an average CPU over head and an easy to implement and maintain solution. Unfortunately it does not contribute positively to high-availability because of it's single point of failure design. The solution can not be recommended for use in any instance.

One point that is often considered is the standby machine. It would appear that this would be better employed if it were actively being used, this is in principle true but relies upon one of the alternative solutions here and in most cases. This point should be reviewed by the reader after finishing this document, however, which will show that whilst in principle it a good idea, in practice a more performant and reliable system is achieved using hot standby than a number of other solutions.

3.1.5 Ethernet Trunking

Where the current wire-speed is less than the volume of traffic required then an alternative to the solutions above must be provided. Ethernet trunking can be used to divide, or as in this case, bind
multiple Ethernet links together. This effectively increases the wire-speed. The 'uplinks' from switches and routers must be of at least the same capacity as the trunked links.

![Figure 5 - Ethernet Trunking](image)

This solution is identical to the 'Hot Standby' solution, with the exception that low level drivers are sharing the load across multiple network connections. This sharing (trunking) does have some restrictions, key is that the connections must all connect to the same switch, so this does not improve reliability in the event of a switch failure for example.

The multiple links are joined together using a low level Ethernet standard (802.3ad), which allows the links to be viewed as one externally. So for example there is only one MAC address for both interface.

The bottleneck should no longer be the network but is more likely to be with the architecture of the server and the CPU capability of the machine. Until recently FireWall-1 could only work with a single CPU, although more could be installed, the firewall module was not threaded, this has now been resolved for later versions of FireWall-1.

### 3.1.6 Active/Active Separate Identities

Multiple firewalls configured with state table synchronisation and clustering enabled. Each firewall is configured with a VIP per subnet and clients are divided into different groups. Each group will use a different firewall so that the number of clients per firewall is approximately even. In the event of a firewall failing another firewall will take over the VIP and traffic will continue to flow.
3.1.6.1 Service Providers

Service Providers, in this sense rather than the ISP type, provide a server of some sort that external users use. Usually web based but may include mail or specialised applications. The traffic begins it’s journey through the firewall, outside of the control domain of the customers we are dealing with, usually coming in from the Internet.

This solution is unable to balance in bound traffic, although DNS-RR can help this solution, it is neither effective nor scalable.

3.1.6.2 General Users

General Users are all within the network, looking out. The traffic all originates internally and is within the control domain of the customer, who can direct which firewall will be used for each user, or group of users. The administration for this solution is a little tiresome and there are no active control mechanisms to monitor traffic flows. The solution does scale reasonably well, given the previously stated limitations.

Because different IP addresses are used and the solution is spread onto different machines the wire-speed limitation previously stated is not a problem and there is no discernable increase in the overheads to maintain state table synchronisation.

This solution is cost effective and for general users provides an acceptable compromise between the un-scalable solutions previously mentioned and the higher cost solutions to follow. However, it should be noted that it is a very poor solution for service providers and should only be used where the organisation is unable to fund a more appropriate solution.
3.1.7 Active/Active Common Identity

This solution uses multiple clustered firewalls with a VIP for each subnet, in a similar way to the Hot Standby solution described above. However, all firewalls have the VIP and can pass the traffic. To achieve this the firewall will use a common MAC address or this IP address. Most switch vendors, but not all, allow this and all traffic for the VIP is sent to all firewalls. Some switches get very confused with this configuration and it has been known to cause significant problems in live environments.

![Figure 7 - Active/Active Common Identity](image)

The maximum theoretical performance of the firewalls is wire-speed and could be increased by using Ethernet trunking but there is an added cost of computing who should 'own' each session. This session start-up phase needs to be negotiated and will introduce a delay and will increase the CPU cycles needed by the firewall. This will increase the cost of the platform for every additional firewall installed.

The solution is great on paper but very poor in the field or when examined with an objective informed technical eye.

| Perf | VFM |

3.1.8 Static Load Balancing

This solution is an extension of the Hot Standby solution, shown above, increases the maximum performance by using all firewalls in an active configuration. The maximum performance is wire-speed but can be further increased by using Ethernet trunking. However, the load on the firewalls is spread as one firewall is only processing the in-bound or out-bound traffic, this reduces the CPU load and will therefore increase the performance. A VIP per subnet is configured, with the VIPs implemented onto different machines, such that in-bound traffic flows through a different firewall than the out-bound traffic.
To make this solution work well there are a few design issues that need to be considered, the most important is ensuring that where possible the external round trip time is greater than the state table synchronisation interval. In practice this is not very complicated but caching devices need to be installed inside the firewalls for example. The reason for ensuring that the external round trip is greater than the state table synchronisation is to ensure that session and NAT information can be transferred to the other firewall(s), if this is not done then replies will not be recognised and may be dropped or rejected.

There is no particular concern over using this solution in a service provider situation, as replies to requests that originated externally will be allowed through by default and, where applicable, NAT’ed using static rules.

While the solution is able to provide a good degree of scalability using Ethernet trunking it is not as scalable as the mediated solution that follows and does rely on a design which ensures that external round trip times are less than the state table synchronisation. The solution cannot, without compromise, be properly implemented with more than two active firewalls, but could be implemented with a third in a standby mode.

### 3.1.9 Mediated Solution

This is the ultimate in performance and reliability (and cost 😞). This solution is most commonly implemented by large xSPs and other organisations offering services which have very high volume data requirements. Clustering is not required, but does add some value, although some kind of interface failover solution, like NetMon, should be implemented on the firewalls. State table synchronisation should still be used.

A VIP per subnet is configured, on the mediation device, which can often also act as a router, depending on the vendor used. The mediation device actively balances the traffic through the firewalls and keeps sessions on the same firewall.
There is no design limit to the performance of this solution other than the performance capabilities of the mediation device, which is typically greater than 1Gb/s. Many vendors offer elegant management techniques for adding and removing firewalls from the system. This is undoubtedly the best technical solution for a very high volume solution. The value for money equation should be assessed in terms of the performance required. Buying a Formula 1 car to do the shopping in may satisfy the technician doing the shopping but the finance people may not be easily pleased.

### 3.2 Performance

#### 3.2.1 Failover times

Fail over times are appropriate in two scenarios: clustered solutions and mediated solution, all other solutions do not have the ability to failover. As the volume of traffic increases, so does the load on all components. For clustered solutions, with the clustering software installed on the firewall, this becomes a risk to reliability where the resource utilisation of the firewall becomes stretched. With the mediated solution, the resources available are normally greatly in excess of any possible load, this provides a good safety margin. As the mediated solution also has a good view of transit and genuine connectivity, this solution has additional benefits.

Load and resource availability should be carefully monitored periodically to ensure that each solution has sufficient spare capacity to continue to operate safely. Because of the complex rule sets and
variable nature of the setup of each installation it is impossible to provide truly meaningful figures on sizing and performance. The firewall vendor should be approached for more accurate information on this subject.

A safe time to set for failover in the event of a failure is a function of the load on the active firewall(s). If the load is such that the clustering software does not have enough CPU cycle to respond in good time then a false failover may occur. Solutions that increase the load of the firewall by introducing session based negotiation and other load balancing techniques 'inside' the firewall all make the safe time for failover longer. The static load balanced solution above introduces the least likelihood of a false failover at a given load, with the exception of the mediated solution, which is even better.

### 3.2.2 State Table Synchronisation

A firewall is implemented to stop unauthorised traffic from passing and to log the authorised and unauthorised traffic. Logging is outside the scope of this document, but a limited understanding of why and how a firewall works is useful here: by default most traffic is blocked from the Internet to the 'internal' network, but users are allowed to make outgoing connections. For the connection to work the firewall must allow the replies back through the firewall. This is achieved by tracking connections, so that the replies are expected and allowed back through the firewall.

Where there is more than one firewall there are additional considerations, as the reply may not return through the same firewall that the request left by. Therefore, firewalls need some way of keeping all of the firewalls informed about what connections are in progress. This is important for both active-active solutions and for hot standby solutions.

Different vendors may have different terminology for this state transfer but Check Point refer to it as State Table Synchronisation (STS) and Stateful Inspection.

The mediated solution greatly reduces the risk when STS is not used, as this is normally performed by the mediation devices. However, there is still a very strong case for implementing it here as well, to cater for the failure of a firewall and reduce the possibility of interrupted sessions.

Firewall-1 only supports STS on Solaris, Linux and Windows.

### 3.2.3 Connection based mediation - in firewall

Solutions that are available to perform active-active load balancing with truly dynamic load distribution can only do so by having a common IP and MAC address and negotiating each connection. Every packet for every connection will be processed by all active firewalls but a low-level kernel module will filter out those not assigned to a particular firewall. This system produces a very elegant and potentially perfectly balanced solution but at a cost. The total throughput is reduced and the transit delay is increased not to mention the reduction in reliability, see above section on performance.
4 Papers Findings

There are no absolute right and wrong ways to implement reliable firewall solutions. Some provide better performance and reliability than others and some cost more than others. The above text goes in to a degree of detail about the pros and cons of the various solutions, no absolute rules can be written regarding how to deploy in all circumstances but it is useful to have some basic guidelines and this section lays some out.

All of the solutions below assume that the firewall hardware has been correctly sized for the volume of traffic and the rule set applied. In addition it should be noted that a high number of short duration sessions will disproportionately distort the load figures, this is known as the tear-up/tear-down rate and is an advanced topic which is outside the scope of this document.
4.1 Super High Performance - Greater than 280Mb/s

With a predicted or actual traffic load through the firewalls in excess of 280Mb/s the only satisfactory solution is to implement a mediated firewall solution, with either five or more firewalls running 100Mb LANs or at least two firewalls running either 1Gb/s Ethernet or trunked Ethernet.

![Figure 10 - Mediated Trunked](image-url)
4.2 High Performance - 160 to 280Mb/s

With a predicted or actual traffic load through the firewalls in excess of 160Mb/s the mediated firewall solution should be considered but a static or trunked static balanced solution may be much more cost effective. Three or more firewalls running 100Mb LANs or at least two firewalls running either 1Gb/s Ethernet or trunked Ethernet should be used. Where a static or static trunked solution is being used the third firewall will be used as a hot standby for both systems, alternatively more resilience could be afforded by installing four firewalls and using the third and four as hot standbys for the first and second respectively.

Figure 11 - Static Trunked
4.3 Good Performance - 50 to 160Mb/s

With a predicted or actual traffic load through the firewalls in excess of 50Mb/s a number of solutions are available, those outlined above and a trunked hot standby solution. As with the Static Trunked solution additional attention needs to be paid to the aggregate Ethernet bandwidth available.

Figure 12 - Trunked Hot Standby
4.4 **Standard Performance - up to 50Mb/s**

With a predicted or actual traffic load through the firewalls not exceeding 50Mb/s, which is probably most sites, then *K.I.S.*, should be the first rule applied. A traditional hot standby solution is the most appropriate solution and provides an easy to install and maintain platform, along with a very reliable and well understood environment. This is not quite as sexy as some of the above solutions or indeed as the active-active session based load balanced solution but outperforms the latter and represents excellent *VFM*.

![Figure 13 - Hot Standby](image-url)