Alcatel·Lucent

TECHNOLOGY INFORMATION GUIDE

Alcatel-Lucent VPN Firewall Brick™ Security Appliance Failover and State Sharing

Alcatel-Lucent Internet Security Products

Table of contents

Introduction

The Alcatel-Lucent VPN Firewall is a high-speed packet-processing engine that provides firewall and virtual private network (VPN) services using a centrally managed, no-touch appliance model. The appliance, named the Alcatel-Lucent VPN Firewall Brick Security Appliance, is protected against failure with the use of an active/standby architecture. In this architecture, two Alcatel-Lucent VPN Firewall Bricks are collocated and connected in parallel, with the corresponding port from each Alcatel-Lucent VPN Firewall Brick connected to the same physical network segment. These Alcatel-Lucent VPN Firewall Bricks then operate as a single Brick: if the currently active Alcatel-Lucent VPN Firewall Brick fails, the standby becomes active and begins processing packets. State information is shared between the two Alcatel-Lucent VPN Firewall Bricks to avoid any single point of failure.

To ensure the maximum degree of network security and availability, Alcatel-Lucent VPN Firewall Bricks can be configured as redundant “failover” pairs.

Product description and architecture

In the failover configuration, the active Alcatel-Lucent VPN Firewall Brick processes traffic just as it would if it were a standalone firewall. Meanwhile, the standby Alcatel-Lucent VPN Firewall Brick — a second Brick connected to the same LAN segments as the active Brick — monitors “heartbeat” signals transmitted by the active Brick up to ten times a second on each of its ports. If all heartbeats cease, the standby Brick takes over the active role. Only a few hundred milliseconds’ delay accompanies the transition of the standby Alcatel-Lucent VPN Firewall Brick to active status, allowing traffic to continue passing into and out of the network in an uninterrupted fashion.

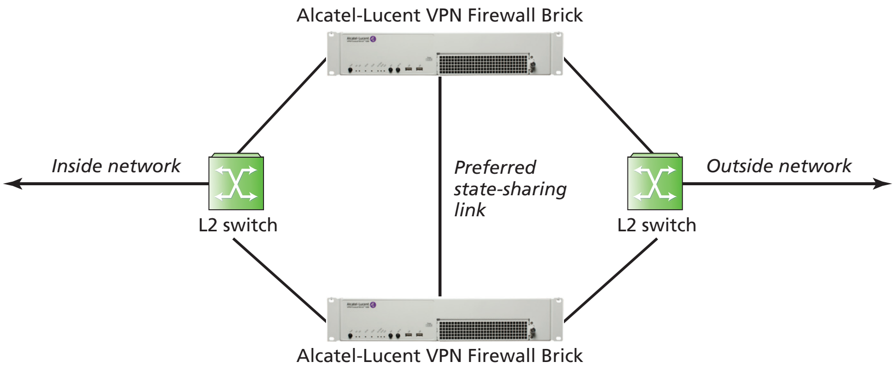
In addition, the active Alcatel-Lucent VPN Firewall Brick continuously sends state information to the standby Brick on one of its ports. This “state-sharing” functionality allows transient information stored in the RAM of the active Alcatel-Lucent VPN Firewall Brick to be shared with the standby Brick, allowing traffic to be correctly processed even if a failure occurs in the middle of a conversation between two or more endpoints.

Redundancy

Redundant Alcatel-Lucent VPN Firewall Bricks must be connected to the network in a particular manner. Each physical port — numbered 0, 1, 2, and so on — on a given Alcatel-Lucent VPN Firewall Brick must be connected to the same broadcast segment as the corresponding port on its redundant Brick. Alcatel-Lucent recommends that this be accomplished by connecting both Alcatel-Lucent VPN Firewall Bricks to as many physically discrete switches (or hubs) as needed to support the desired number of physical segments.

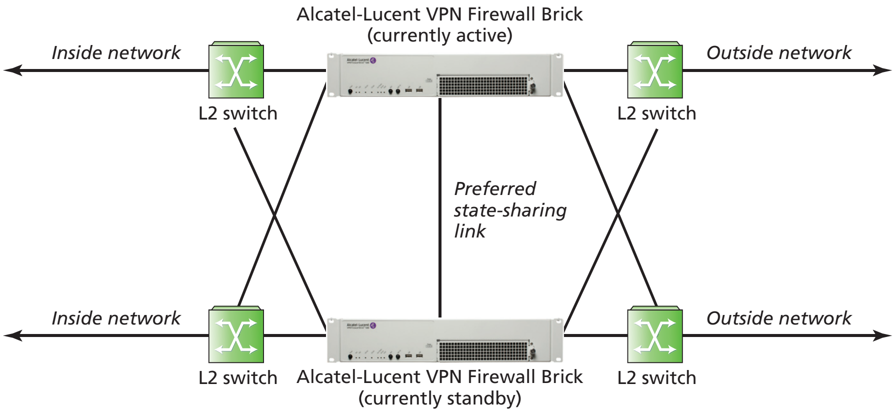
This topology is illustrated in Figure 1. At least two logical connections should exist between the Alcatel-Lucent VPN Firewall Bricks to avoid a single point of failure. Alcatel-Lucent strongly recommends a direct link, such as a crossover cable, between the two.

Figure 1. Basic topology for connecting redundant Alcatel-Lucent VPN Firewall Bricks


Alcatel-Lucent VPN Firewall Brick
Inside network
Preferred state-sharing link
Outside network
L2 switch
L2 switch
Alcatel-Lucent VPN Firewall Brick

It is often useful to address full redundancy across the entire network. In this case, all devices and links must be made redundant, as shown in Figure 2.

Figure 2. Fully redundant configuration with no single failure point


Alcatel-Lucent VPN Firewall Brick (currently active)
Inside network
L2 switch
Outside network
L2 switch
Preferred state-sharing link
Inside network
Outside network
L2 switch
Alcatel-Lucent VPN Firewall Brick (currently standby)
L2 switch

How failover works

On the Alcatel-Lucent Security Management Server (SMS), a check box on the Brick Editor Option tab must be selected to enable failover functionality. In addition, a preferred link for state sharing may be chosen. From the user's point of view, these are the only differences in the configuration of a failover pair of Alcatel-Lucent VPN Firewall Bricks from the configuration of a standalone Brick.

Both the active and standby Alcatel-Lucent VPN Firewall Bricks are bootstrapped from the same Universal Serial Bus (USB) drive. The configuration loaded from the USB drive is similar in most respects to the configuration of a standalone Alcatel-Lucent VPN Firewall Brick, and with good reason. During most of its operational life, the active Alcatel-Lucent VPN Firewall Brick works as if it were a standalone Brick. Because the two physical Alcatel-Lucent VPN Firewall Bricks share the same identity — that is, the same name and IP address — only one logical Brick exists.

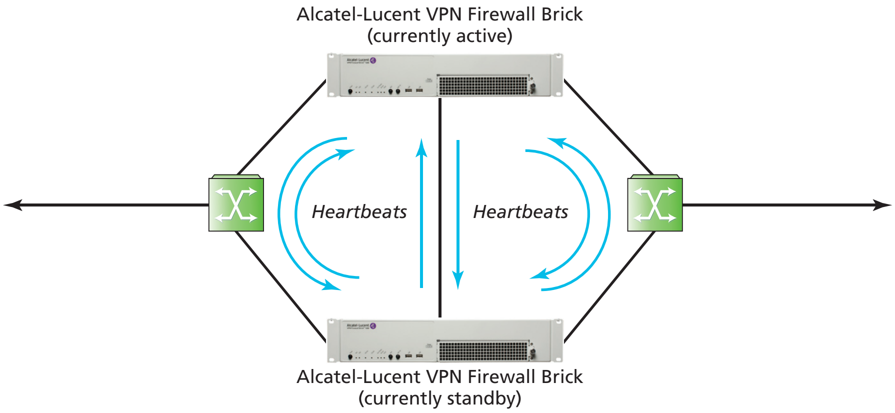
Heartbeat

Both the active and standby Alcatel-Lucent VPN Firewall Bricks regularly issue “heartbeat” signals, as shown in Figure 3. The active and standby Alcatel-Lucent VPN Firewall Bricks generate a heartbeat up to ten times a second on each link, using an adaptive algorithm to slow this heartbeat when permissible. Note that the heartbeats are Layer 2 packets and the configuration therefore requires Layer 2 connectivity between the two Alcatel-Lucent VPN Firewall Bricks. Among other information, heartbeat messages contain the Alcatel-Lucent VPN Firewall Brick identifier, its current role (active or standby), and a health and status indicator.

Heartbeats serve several functions:

- The heartbeat announces the presence of an active Alcatel-Lucent VPN Firewall Brick. If incoming heartbeats cease, the standby Alcatel-Lucent VPN Firewall Brick becomes active.
- Heartbeats allow the Alcatel-Lucent VPN Firewall Bricks to determine the relative health of each of their Ethernet links. Without the heartbeats or some other configured flow, the Alcatel-Lucent VPN Firewall Bricks would have to rely on simple link integrity to assess the health of their respective ports.
- Because Alcatel-Lucent VPN Firewall Brick security policies are based on connections to specific ports, heartbeats must also verify that corresponding ports on each Brick are connected to the same LANs.
- Heartbeats carry authentication and anti-replay information to prevent flood attacks based on forged or previously recorded heartbeats.

Figure 3. Heartbeat messages transmitted between active and standby Alcatel-Lucent VPN Firewall Bricks


Alcatel-Lucent VPN Firewall Brick
(currently active)
Heartbeats
Heartbeats
Alcatel-Lucent VPN Firewall Brick
(currently standby)

When failovers occur

An Alcatel-Lucent VPN Firewall Brick that is configured for failover boots immediately into standby mode, under the assumption that there is already an active Brick functioning in the network that should not be interfered with.

The standby-to-active transition event occurs under one of several conditions:

- The standby ceases to receive "active" heartbeats from a previously active Alcatel-Lucent VPN Firewall Brick.
- The standby receives "standby" heartbeats from a previously active Alcatel-Lucent VPN Firewall Brick.
- The Alcatel-Lucent VPN Firewall Brick boots and receives no heartbeats on any interface.

Following a switch from standby to active, the now-active Alcatel-Lucent VPN Firewall Brick begins transmitting "active" heartbeats.

The active-to-standby transition event occurs under one the following conditions:

1. The active receives "standby" heartbeats with a greater health and status indicator from a standby Alcatel-Lucent VPN Firewall Brick (if the yield parameter is set to a value greater than zero).
2. The active receives "active" heartbeats of a higher priority (potentially resulting from correction of a prior network failure or outage).
3. An administrator has issued a manual failover command.

Current measurements indicate that the entire detection and failover process can occur in as little as 400 ms — well below thresholds for Application and Network-layer timeouts. The failover event is therefore undetected by most classes of users.

Alcatel-Lucent recommends the following to ensure that the Alcatel-Lucent VPN Firewall Brick failover process does not cause calls in-progress to be dropped:

- Use the right Alcatel-Lucent VPN Firewall Brick model that can handle network traffic without being overloaded.
- Use the same Alcatel-Lucent VPN Firewall Brick model for the redundant pair.
- The quality of the links between the two Alcatel-Lucent VPN Firewall Bricks should provide a frame-loss rate better that one in a million frames and transmission latency of less than 1 ms.
- Use a dedicated failover link between the two Alcatel-Lucent VPN Firewall Bricks for state sharing.
- Use a Gigabit Ethernet interface for the dedicated failover link when available.
- Network congestion and overload conditions should not impact the quality of the failover link.

IP tracking feature

The Alcatel-Lucent VPN Firewall Brick failover mechanism supports the "IP tracking" configuration option, which helps the Brick to decide to fail over if it loses connectivity between the active Brick and some network components (for example, a router behind the failover switch). If the active Alcatel-Lucent VPN Firewall Brick discovers, using the IP tracking feature, that the links to other network elements are not working, failover to the standby Brick is initiated.

State sharing

State sharing is a technique by which the active Alcatel-Lucent VPN Firewall Brick proactively and continuously notifies the standby Brick about transient session and keying information, under the assumption that it can fail at any time. If it does fail, the now-active Alcatel-Lucent VPN Firewall Brick can continue to function because it has almost the same information that the previously active Brick had immediately before failure.

Determining which link to use

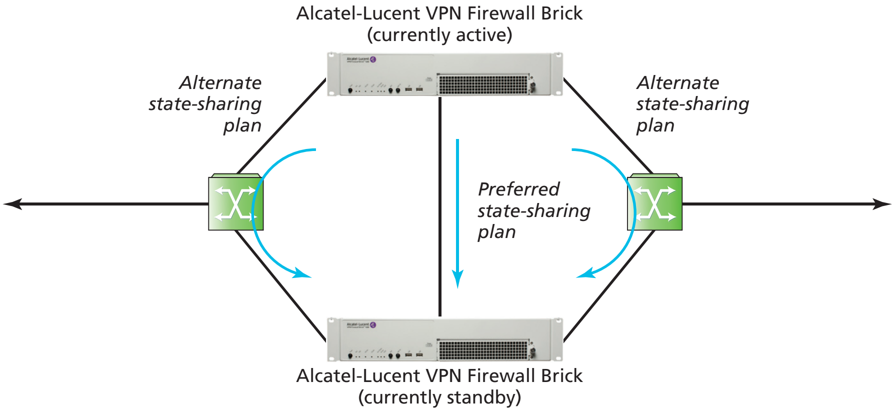
State information is transferred across only one link at a time. While the state-sharing link may also carry data traffic, if any unused ports exist, Alcatel-Lucent strongly recommends connecting the two Alcatel-Lucent VPN Firewall Bricks with a crossover cable to establish a dedicated path for state-sharing information. The connection does not introduce a single point of failure because the two Alcatel-Lucent VPN Firewall Bricks self-heal if this link breaks: they find an alternate path if one is available.

The Alcatel-Lucent VPN Firewall Brick chooses a network link over which to transfer state information based on several factors, in the following order (see Figure 4):

1. If the administrator has specified a particular link for state transfers and that link is active, it is the Alcatel-Lucent VPN Firewall Brick's first choice.
2. The least heavily loaded active Gigabit Ethernet link, over which heartbeats are being exchanged, is the Alcatel-Lucent VPN Firewall Brick's second choice.
3. The active full-duplex Ethernet link with the highest number of available bits is the Alcatel-Lucent VPN Firewall Brick's third choice.
4. The active half-duplex Ethernet link with the highest number of available bits is the Alcatel-Lucent VPN Firewall Brick's last choice.

Measurements of "available" bits are based on proactive monitoring data collected every 30 s, excluding traffic generated by the state-sharing activities themselves.

Figure 4. Preferred and alternate state-sharing paths



Sharing of state information

Because the quantity of data resident on the active Alcatel-Lucent VPN Firewall Brick is potentially very large and continuously in flux and inter-Brick bandwidth is finite, state information is shared in priority order: the most critical information is shared as highest-priority, and less-critical information is shared at lower priorities. Certain critical events require the recipient's acknowledgement.

All critical and most other transient information is shared between both Alcatel-Lucent VPN Firewall Bricks. In addition, operating-system updates and configuration modifications are shared, allowing changes to be applied to both Alcatel-Lucent VPN Firewall Bricks without concern about coordination between the two.

Some information, including use counts and Address Resolution Protocol (ARP) entries, is never shared. Some information about security events and conditions is of such critical importance to network operation that it must be transmitted immediately. Other types of events are held and periodically sent in batch updates. Finally, some long-lived events are resent periodically for validation.

State sharing for VPN tunnels

To ensure VPN tunnels are maintained during a Brick failover, the tunnel-state information shared between active and standby Alcatel-Lucent VPN Firewall Bricks includes:

- All Security Association (SA) information: keys, Security Parameter Index (SPI), sequence number, addresses, and so on)
- For Internet Key Exchange version 2 (IKEv2), all state information about the negotiation, including child SAs

Security

Different types of state-sharing messages require different levels of security. All messages are authenticated to protect against an intruder sending an invalid state-sharing message. Messages that contain keys, in particular, are encrypted with the maximum level of encryption supported by the Alcatel-Lucent VPN Firewall Brick. Replay protection is provided on all messages to protect against a message-replay attack.

Alcatel-Lucent SMS notifications

The Alcatel-Lucent SMS delivers advanced, carrier-grade IP services management without costly additional modules or recurring license fees. The Alcatel-Lucent SMS provides distinct indications when an Alcatel-Lucent VPN Firewall Brick is configured as part of a failover pair, and the states of the active and standby are reported on the Alcatel-Lucent SMS GUI. The GUI can also show that both Alcatel-Lucent VPN Firewall Bricks are up and healthy and report if the standby is unavailable for any reason.

In addition, failover events are logged in the Alcatel-Lucent SMS event log. When a failover event occurs, an alarm can be triggered, alerting the administrator to determine the root cause of the failure.

Product features and benefits

FEATURE	BENEFIT
Configuration as redundant failover pairs	Provides the maximum degree of network security and availability
Minimal delay during transition from standby to active	Allows uninterrupted passage of traffic, with failover events undetected by most classes of users
IP tracking configuration option	Helps initiate failover if connectivity is lost between the active Brick and a network component
Sharing of operating-system updates and configuration modifications	Allows changes to be applied uniformly to both Alcatel-Lucent VPN Firewall Bricks
Authentication, encryption and replay protection for all state-sharing messages	Provides appropriate protection for messages that require different security levels
Triggering of alarms when failover events occur	Alerts administrators to determine the root cause of failures

Conclusion

The Alcatel-Lucent VPN Firewall Brick can operate in an environment where high availability is a requirement. When an Alcatel-Lucent VPN Firewall Brick pair is used to protect multiple networks, the combination of heartbeats, failover, Alcatel-Lucent SMS notification, and state sharing provides a transparent mechanism by which failures are detected and eliminated from the data path. This process helps to ensure a network that is of the highest availability.

For more information about the Alcatel-Lucent VPN Firewall products, see:
http://enterprise.alcatel-lucent.com/?product=VPNFirewallBrick&page=overview

Acronyms

ARP	Address Resolution Protocol
GUI	graphical user interface
IKE	Internet Key Exchange
IP	Internet Protocol
LAN	local area network
RAM	Random Access Memory
SA	Security Association
SMS	Security Management Server
SPI	Security Parameter Index
USB	Universal Serial Bus
VPN	virtual private network

Alcatel·Lucent