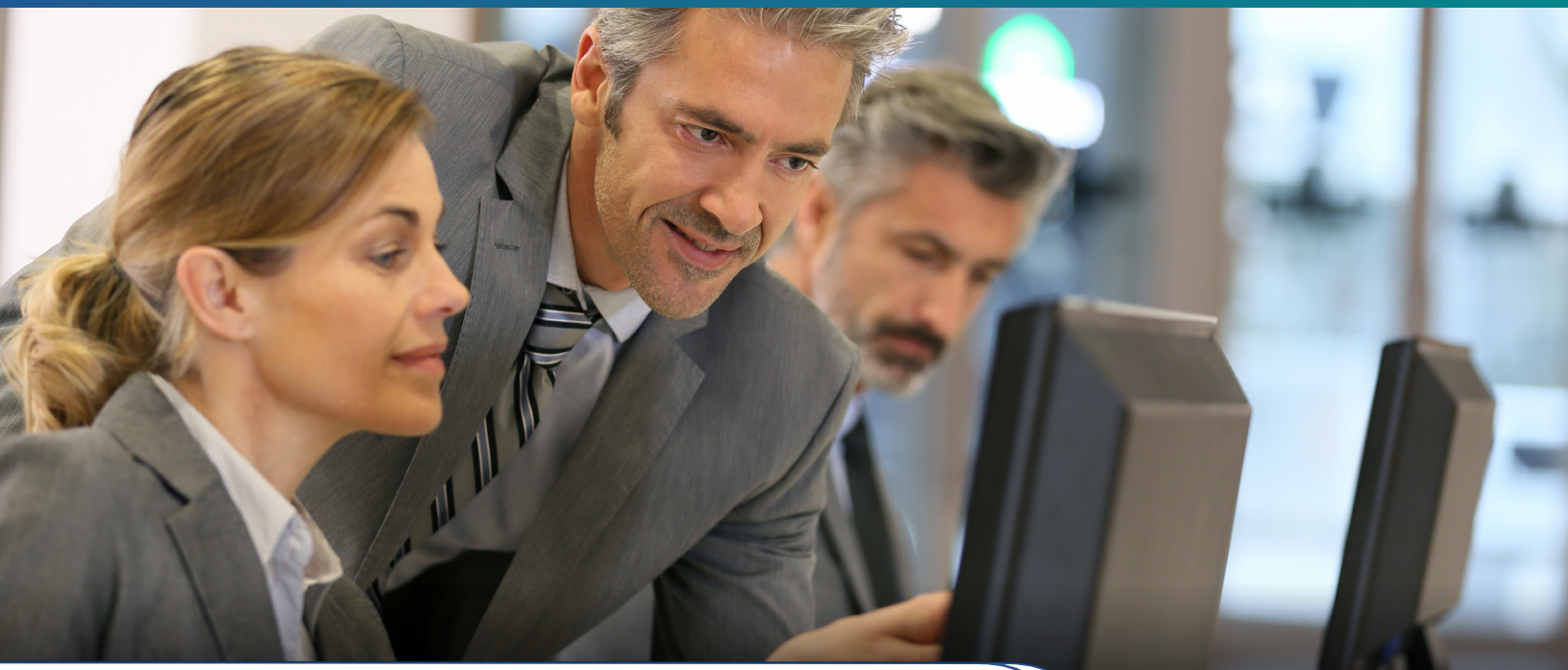

WHITE PAPER

Plan Your Firewall Migration to Increase Security Resilience

Best Practices for Maximizing Uptime and Achieving High Availability

If you will be upgrading or migrating to a next generation firewall, take the opportunity to also review your overall security architecture. You spend significant time and money to implement, maintain, and upgrade your security infrastructure. Make sure your security tool architecture is designed to maximize value and efficiency. Limit the risk of downtime to your network. Keep your applications strong. All these benefits start with the simple addition of a bypass switch. For more advanced architectures, add a network packet broker.

This paper examines how you can achieve these goals and implement a resilient security fabric—one that delivers a self-healing, highly-available security architecture to complement your next-generation firewall (NGFW).

Nearly 90% of companies have suffered a security incident, with enterprises paying an average of $551,000 to resolve and smbs $38,000.

— Kaspersky Lab

Reduce the Risk of Downtime

Take a close look at your overall architecture and identify all of the potential points for failure or performance issues. With serial inline deployment, traffic is passed from one security appliance to the other, meaning a failure in any one of the devices can stop traffic flow and cause a network outage. For most organizations,

KEYSIGHT TECHNOLOGIES

the cost of downtime is substantial and can be used to calculate the return on investment of any project proposed to reduce it.

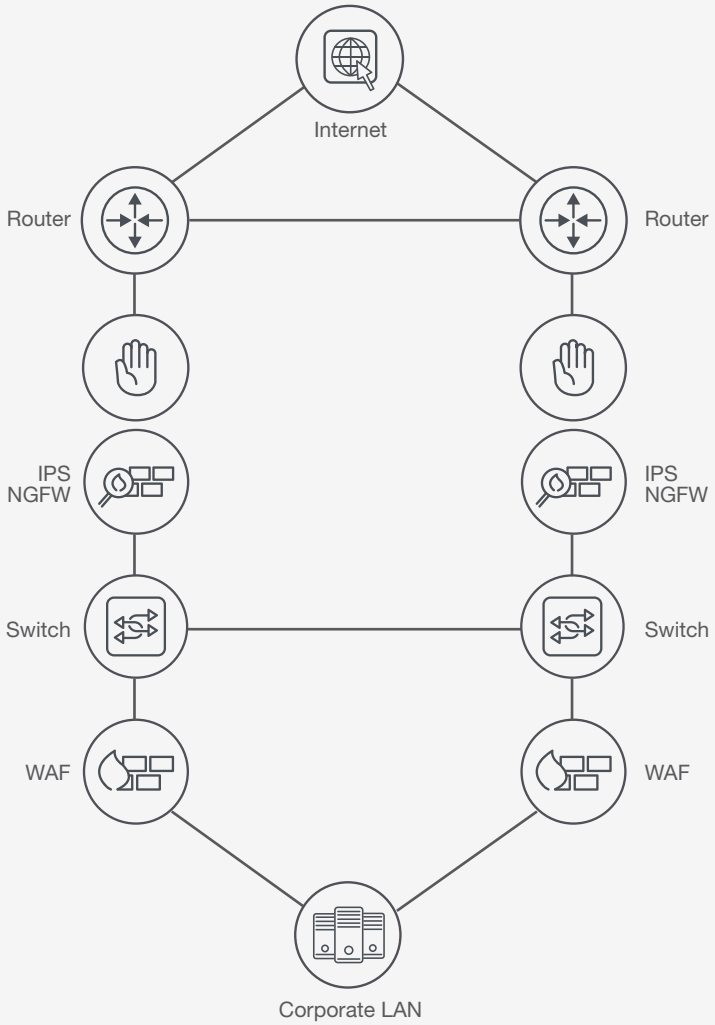

Figure 1. Inline security architecture (before).

Cost of lost enterprise business is rising, averaging $1.57 Million per security incident, and growing annually by 15%.

— Ponemon Institute

Even security architectures designed with redundancy can be highly susceptible to network outages and bottlenecks. In the architecture shown here, redundant routers and switches provide failover protection of those devices, but any failure in the inline security devices, such as an intrusion protection system (IPS), NGFW, or web application firewall (WAF) can cause traffic on either path to stop flowing or become overloaded, and a single failure on each path can cause a complete network outage. This serial inline architecture also forces traffic in each path to pass through each

security device in the path, which can severely slow its performance and impact network availability. This design also causes downtime during software and hardware upgrades.

A simple alternative that reduces the risk of planned and unplanned downtime is to deploy a simple high-speed bypass switch in front of every firewall and other security appliance—a switch with the ability to continually monitor all inline devices and make sure they are ready to receive traffic. If any device goes down unexpectedly, the bypass steers traffic around it until the device is returned to a ready state. This eliminates the risk of a single device failure causing a network outage. The bypass ensures network traffic can still be inspected by all other functioning security appliances and keeps the overall network up and running. The best bypass switches operate at line-rate speed and have no impact on network availability.

Enterprises deploy an average of 32 different security solutions.

— ZK Research

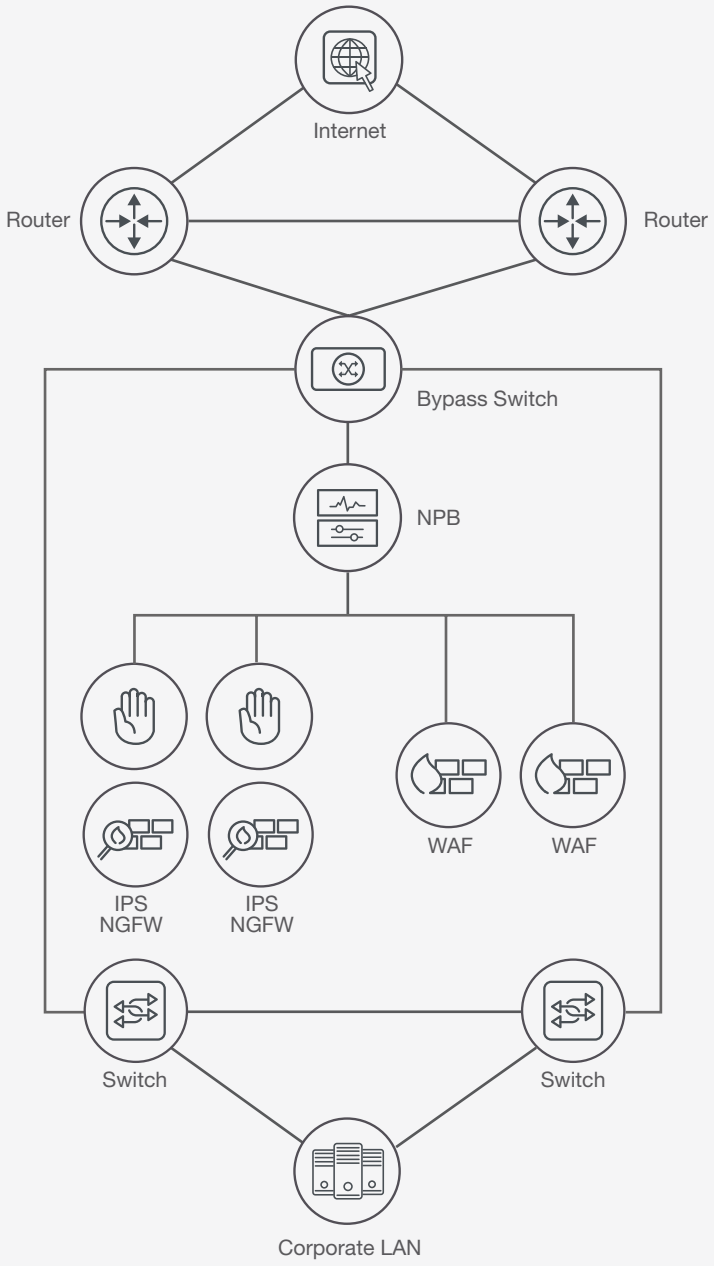

Figure 2. Security fabric architecture.

In addition, once a bypass switch is installed, planned maintenance such as configuration changes, deployment of new appliances, or device upgrades can be performed without impact to the network, as the bypass will route traffic around the offline device. Since 70-90% of all downtime is associated with maintenance, this simple change can dramatically increase application uptime.

While extremely useful for reducing downtime, the bypass makes a trade-off between availability and security inspection, since traffic is simply routed around any security device that is unable to respond. Fortunately, there is an even better, more resilient security solution.

80% of organizations believe lack of tool integration impacts time to resolution.

— ESG Survey

Enable Efficiency and Load Balancing

Implementing a network packet broker (NPB), along with the bypass switch, gives you the added ability to see inside network packets and route them selectively among all the connected devices. Keysight calls this design the Keysight security fabric™ and it allows you to route packets only to the appliances that are appropriate for that type of traffic, while maintaining complete resiliency. For example, non-HTTP/HTTPS traffic does not benefit from passing through the WAF, so that traffic can be routed around that device. Reducing the amount of traffic passed to an appliance minimizes the likelihood that it will become overwhelmed and/or fail, which increases efficiency and keeps your security infrastructure operating at maximum strength.

Reducing the workload also gives your devices room to accommodate growth in network traffic and delays the need to upgrade or scale up your infrastructure. With less traffic to process, the useful life of your devices is extended, holding off replacement costs. Many organizations have been able to completely offset the cost of implementing a bypass switch and NPB by canceling planned upgrades.

When you do decide to upgrade to a NGFW or add scale to an existing appliance, you can configure the NPB to automatically balance the workload between the original and new devices, sending the most sensitive traffic to the new, more functional device. Another major advantage of deploying Keysight security fabric is the ability to feed traffic to different inline or out-of-band devices at their respective speeds. This means that even after upgrading to a 10G, 25G, or 40G network, you can continue to use your legacy 1G security appliances, extending their useful life.

Since intelligent routing is such a critical part of a highly resilient security architecture, you should choose an NPB that operates at line rate speed with the lowest possible packet loss and provides maximum flexibility for data manipulation and load balancing, to achieve optimal efficiency.

Configure for High Availability

To reduce downtime even further and maximize resiliency, you can deploy your security fabric with high availability (HA) using redundant modular bypass switches and NPBs. If you use an NPB capable of being deployed in redundant active-active mode, you will have automatic and instantaneous recovery of any device in your security architecture.

In the maximum strength security architecture (shown above), dual bypass switches and dual NPBs enable full recovery from the failure of any inline device in the security architecture. The bypass switches deployed in active-standby mode monitor the health of all devices, including the NPBs, and reroute traffic from one to another, should an outage be detected. In the case of a failure on one branch, security is completely maintained, and users would detect no service or application outage.

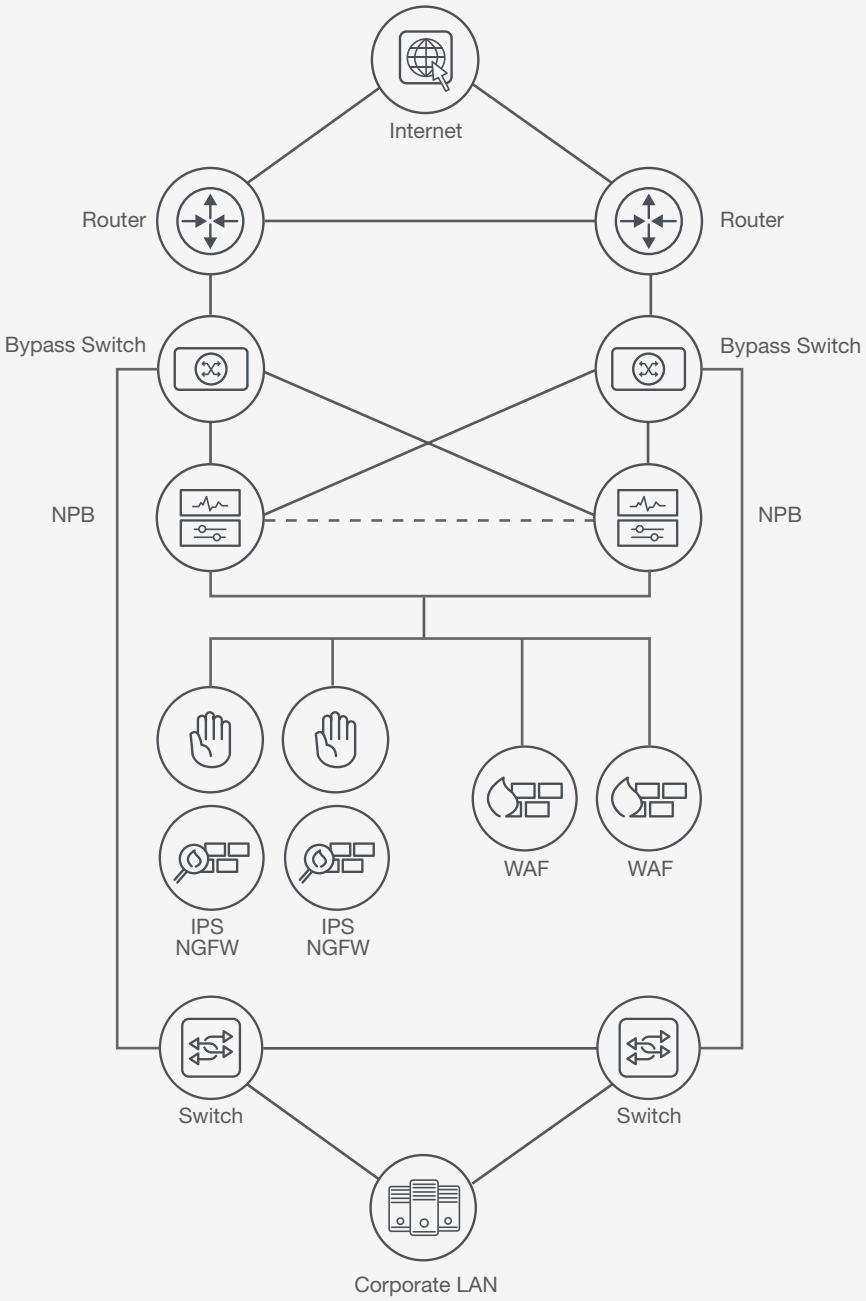

Figure 3. Security fabrixc with maximum strength HA.

The NPBs configured for HA with complete synchronization in active-active mode provide load balancing during normal conditions and are configured for full protection of all traffic if one goes down. Again, users detect no downtime, and security monitoring is completely unaffected.

Gain Visibility with Network Packet Brokers

Increasing the number of security devices in your architecture does not automatically minimize risk. Network complexity creates blind spots. NPBs provide a more comprehensive view of your environment: capturing the growing volume of traffic from virtual networks, aggregating data collected, eliminating duplication, and stripping away unnecessary detail.

While inline monitoring is clearly important, out-of-band tools are better suited to analyze network performance, identify emerging trends, and respond to compliance requests. The best NPBs provide a central point for efficient and simultaneous management of both inline and out-of-band devices. They allow you to precisely select traffic for analysis by application type, geography, device, or other parameters and produce customized reports for compliance purposes.

The likelihood of an organization suffering an outage over the next 2 years is 25%.

— Ponemon Institute

A firewall upgrade is more than an opportunity to add new security features; it gives you the chance to future-proof your architecture and build in greater adaptability.

Build a Future-Proof Architecture

Optimal customer experience and application uptime are more important than ever before. A firewall upgrade is more than an opportunity to add new security features; it gives you the chance to future-proof your architecture and build in greater adaptability. Consider the advantages of a security framework based on reliable high-speed bypass switches and powerful network packet brokers operating in active-active HA mode.

- Eliminate network downtime from unplanned security device failure and planned deployments, maintenance, and upgrades.
- Provide complete protection against failure of a one or more security tools, as wells as the bypass switch or NPB.
- Ensure maximum uptime for security infrastructure through HA configuration.
- Achieve maximum efficiency for your security appliances and reduce the load on security appliances to extend useful life and delay new purchases.
- Enable more efficient traffic analysis.
- Support growth in network traffic with minimal new investments.

With Keysight's Security Fabric, creating a self-healing, highly-available security architecture has never been easier.

Find out more about maximizing uptime and increasing resilience with Keysight's Security Fabric solutions at https://www.keysight.com/my/en/cmp/2020/network-visibility-network-test.html.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES