Resilient connection of Intrusion Prevention Systems to a critical UK banking network

SECURITY VISIBILITY CASE STUDY

Increasing and proving in-line security fail-safe for a major High Street Bank

At a glance

Customer: One of the UK's major retail and commercial banking institutions.

Solutions: Advanced Feature Network Packet Brokers.

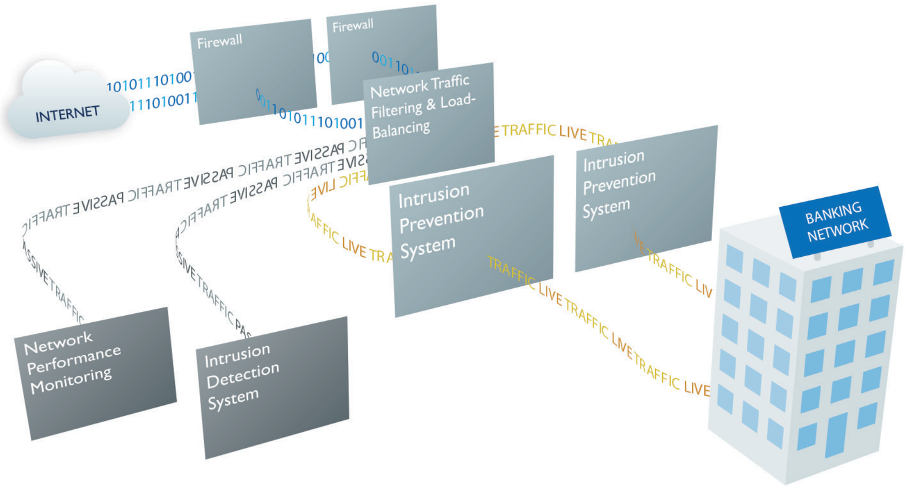
Services: Design, provision and proof testing of an in-line security protection resilience layer.

Outcome: Continued network and security uptime in the event of an in-line security failure.

The objective

To keep up with the increased demand for its internet banking applications and Government guidance/regulation (such as CBEST, CREST and PCI), our customer wanted to add further in-line security with the ability to share the load between filtering devices and ensure automatic fail-over in the event of an IPS device failure or degradation of performance.

It was also imperative that the overall security and resilience capability could easily scale with inevitable future growth.


INTERNET
Firewall
Firewall
Network Traffic Filtering & Load-Balancing
Intrusion Prevention System
Intrusion Prevention System
Network Performance Monitoring
Intrusion Detection System
BANKING NETWORK
PASSIVE TRAFFIC
LIVE TRAFFIC

Needing to see how the security protection and resilience capability would work in context to its unique environment, the bank wanted to work with a solution partner of exceptional technical ability, so chose Red Helix to help design, provision, proof-test and implement the security fail-safe connection solution.

Red Helix

Always evolving. Always there.

The solution

Network TAPs were placed in the optimal positions to feed data to the advanced feature Network Packet Brokers.

The advanced features required to deliver security resilience included:

In-line Fail-Safe - automatically re-routing traffic to another IPS and performance monitoring layer in the event that an in-line security tool should fail, or be taken offline.

Load Balancing – to aggregate the data links and evenly spread security monitoring duties across multiple IPS and send traffic copies to network performance monitoring probes.

To further increase the resilience of the solution, the health of each security device was individually monitored and corrective action was automatically triggered to ensure security uptime.

To achieve this, the Security Visibility layer was configured to send and receive heartbeat packets, and in the event of an IPS going offline or experiencing a performance dip, traffic would be automatically sent to another IPS.

Network Visibility
DDoS Mitigation
SSL Decryption
Intrusion Protection
Malware Sandbox

Proof-testing scenarios

Prior to going live with the new IPS, the customer sought certainty that traffic would instantly divert to an alternative IPS in the event another such device should fail or experience a performance dip.

The customer also needed to know the desired IPS were right for their unique environment. The only way to know how they would perform was to test them under the real scenarios in which they would need to excel.

To achieve both objectives, we replicated the customer's intended security production environment and injected high volumes of stateful application traffic riddled with malware.

This allowed us to:

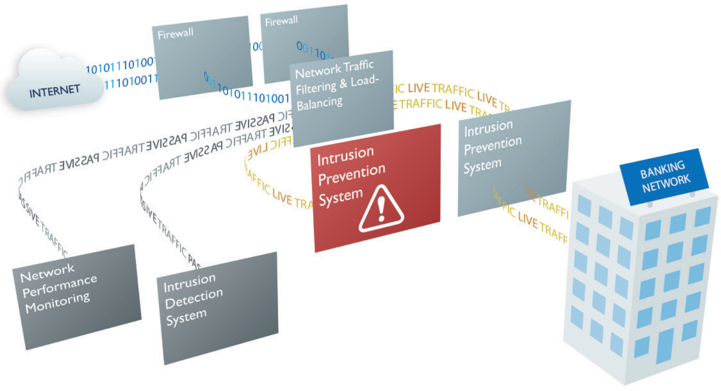
1. Measure the IPS' ability to locate and prevent malware from entering the network
2. Share the malware filtering load between IPS during peak utilisation periods
3. Ensure the desired continuity path came into action if an IPS failed.

The proof-testing scenarios also enabled us to show the real-world throughput performance results were well within the scope of the bank's requirements.

The outcome capability

The addition of the new Intrusion Prevention Systems was an important step to the bank's ability to better defend against the ever-growing threats of cyber-crime.

However, the building of the Security Visibility layer for in-line fail-safe significantly enhanced the bank's overall security maturity. In the event of an IPS failing or being taken offline for configuration updates, advanced security protection filtering could continue without impacting network availability.


INTERNET
Firewall
Firewall
Network Traffic Filtering & Load-Balancing
Intrusion Prevention System
Intrusion Prevention System
BANKING NETWORK
Network Performance Monitoring
Intrusion Detection System
LIVE TRAFFIC
PASSIVE TRAFFIC

The solution also provided the flexibility to quickly add or reconfigure other security protection and analysis layers - such as DDoS Mitigation, Malware Sandbox and Intrusion Detection Systems - making the Security Visibility layer a truly scalable solution allowing both security posture and fail-safe capability to grow with the evolution of the network.

Furthermore, with a 24/7/365 service wrap in place, the customer can contact us any time for dedicated technical support and guidance for anything related to the design and configuration of the Security Visibility layer.

About Red Helix

We provide services and solutions to improve security and performance for critical, large-scale and latency-sensitive networks.

Our integrated security solutions and network/application performance monitoring systems are coupled with our superior network visibility capabilities to provide cost-effective, comprehensive & resilient network coverage.

Red Helix

Always evolving. Always there.

rhlsvcsJuly2022