Fortinet Firewall Health Check

Why do I need a firewall health check?

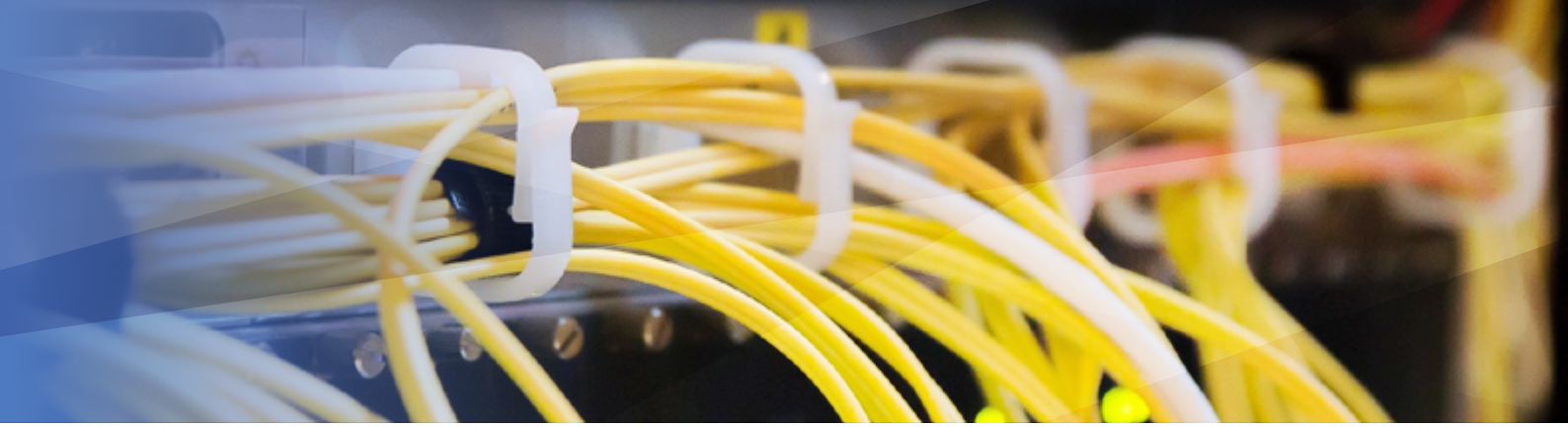
- The organisation has changed - is the firewall still meeting the needs of the business?
- Firewall rules have changed since installation and may no longer adhere to best practice.
- Organisations are often unaware what their firewall is doing.
- Organisations often lack understanding of the traffic traversing their firewall and the protocols and applications that make up that traffic.
- Firewall services availability, resilience and risk assessments are often lacking.
- The firewall may have additional features available which could improve security or the functionality of the firewall. Mitigate risk and increase peace of mind with expert validation of the firewall function.
- To ensure your firewall meets PCI Compliance and not using non-compliant (SSLv3 and TLS1).

When should I have a firewall health check?

- We usually recommend a firewall health check on an annual basis, depending on how often the firewall rules are updated or changes are made within the organisation.
- Business drivers include a major change in the business, a merger, on-boarding new web applications, or a change of technical administration staff.

Where is the work completed?

- The entire exercise can be done remotely using remote meeting capabilities, or via a direct remote connection to the firewall (we only require read-only access), or on site, according to the customer's preference.
- For larger Fortigate models, the first half of a health check will often be done on site and the second half will be completed remotely.



Who will complete the health check?

- One of our friendly, fully certified security consultants with years of extensive experience will complete your firewall health check.

How long does it take?

- Typically, a complete health check can take up to 2 days per firewall or firewall HA cluster (based on up to 200 rules per firewall).
- The first day is for gathering intelligence and analysis of the firewall with the second day being used to complete the comprehensive report detailed above.

What will we do?

Firewall Health Check

- Software Revision
- CPU / Memory utilisation
- Admin accounts
- Certificates
- UTM features
- Interfaces
- VLANs
- High Availability review (failover test optional)
- SSL VPN
- IPSec
- Static routing
- Equal Cost Multi Path routing
- Policy based routing
- Logging and logs
- Alerting and alerts
- 3rd party integration review
- Network integration and positioning
- Licensing

Policy Health Check

Then we review firewall policies. The related features that are used in the policy would also be reviewed.

- Security profiles
- Objects
- Source NAT
- Destination NAT
- SSL inspection
- Traffic shapers

Health Check & Summary Report

Finally, you receive a complete and comprehensive report covering: executive summary, documentation of the environment, detailed findings and recommendations.

Why Choose Nouveau?

Whether your goals are to take advantage of new technology capabilities, simplify network management, safeguard data or reduce operating costs, we can supply all your infrastructure requirements, and support you with:

- Knowledge and Expertise
- Customer-Centric Approach
- IT Support Excellence

nouveau.

T: 0118 918 6822 E: sales@nouveau.co.uk