HP Network Security Design Review Service

HP Networking Consulting

**Service overview**

The HP Network Security Design Review Service provides an examination and assessment of your organization's internal and external network environment.

This network security design review and analysis on your existing network environment will include firewalls, Web proxy and content filtering, network load balancing, intrusion prevention, application firewalls, wireless access for employees and guests, security incident and event management, external DNS architecture, security compartment zones, operational staffing, and security-incident– and device-compliance–readiness procedures.

As part of this service, HP consultants will:

- Conduct face-to-face working sessions with your organization’s network and security SME stakeholders as a first step to assess your current network security environment and develop a plan for improving your organization’s security posture by implementing HP security best practices in the area of network security
- Holistically evaluate the current Internet network edge architecture and security compartment zones to determine if it is optimally designed for network security and business continuity
- Understand each use case and site profile that needs to be upgraded, replaced, moved, or re-configured to improve operational readiness
- Perform a gap analysis that identifies and compares your organization’s current network security infrastructure against industry standards and HP best practices; identify any gaps; and use that information to optimize the confidentiality, integrity, and availability of the network
- Create an executive and technical report
Service benefits
This service is related to your organization’s network security strategy. The objective of this 6-week project is to collect, analyze, and document the security requirements, and network use cases in order to detail a strategy to improve the security posture of the enterprise by articulating best practices in the areas of confidentiality, integrity, and availability for network requirements such as these:

- Remote access
- Network segmentation
- Network filtering
- Compliance reporting

HP will use the Customer’s current network design and the Customer’s provided future-state requirements as input for the review. HP’s recommendations will comply with industry standards and HP best practices. HP will provide analysis and reporting based on industry trends, available technologies, and the Customer’s business and IT requirements to achieve the shared vision.

Service feature highlights
- Pre-engagement requirements
- Delivery of Network Security Design Review Service
- Network Security Design Review reports

Specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Delivery specification</th>
</tr>
</thead>
</table>
| Pre-engagement requirements    | As a prerequisite to HP’s provision of the Network Security Design Review Service, an HP security consultant service specialist will conduct a meeting to review the Customer’s network security environment, oversee the Customer’s signature of the confidential disclosure agreement has been signed, and verify that the service prerequisites have been met. The session will include discussion and agreement of the following Customer data and materials to be provided by the Customer:  
  • Names of staff who will interact with the HP delivery consultant conducting the review  
  • Any security-related documentation  
  • Architecture drawings or output from an automated e-Discovery tool  
  • Network security policies and any other information useful for describing and defining the Customer’s network environment  
  • Any other pertinent data on the network security infrastructure.  
  HP will schedule the onsite delivery of the service at a time mutually agreed upon by HP and the Customer, which shall be during local HP standard business hours excluding HP holidays, unless otherwise agreed by HP. Any services provided outside of HP standard business hours may be subject to additional charges. |
| Delivery of Network Security Design Review Service | Face-to-face working sessions will be conducted between the HP security consultant, the Customer’s network and security staff, and other technical resources to collect and review all pertinent available data over the course the first week of the engagement.  
  Data discovery and collection activities will include:  
  • Review of existing network topology, availability, and implementations  
  • Review of existing Internet edge use cases and site profiles for each location  
  • Review of existing intrusion prevention use cases and site profiles for each location  
  • Review of security incident and event management use cases and site profiles for each location  
  • Documentation of use cases, findings, and future-state strategy along with a prioritized roadmap by provision of a high-level network security design document that contains components including: |
Internet-facing network security design recommendations
Remote-access network security design recommendations
Intrusion prevention network security design recommendations
Security incident and event management network security design recommendations

The HP security consultant will then leave to conduct further analysis off site and to prepare the executive and technical reports.

Network Security Design Review

Executive summary report – This report is written for an executive-level audience. It will document the Customer’s future-state strategy with a prioritized roadmap for each site profile, to include:

- Existing network security topology review and high-level recommendations
- Internet-facing network security review and high-level recommendations
- Intrusion prevention network security review and high-level recommendations
- Wireless network security review and high-level recommendations
- Security incident and event management network security review and high-level recommendations

This deliverable is the result of face-to-face working sessions with the Customer and analysis of the Customer’s available data. It will contain a gap analysis between the current infrastructure and industry standards and HP’s best practices for network security architectures. The report will contain the recommended network security high-level design that was reached by HP and the customer consensus. Also included in the report will be an analysis of the Customer’s current network security staffing and a rationale for improved optimization of IT resources, if indicated. The report will be delivered as a Microsoft® Word document.

Detailed technical report – Whereas the executive report explains what needs to be done, the detailed technical report describes how it can be done. This document, written for the Customer’s technical staff, will document the findings and recommendations of the HP technology consultant as a result of the working sessions with the Customer and the analysis conducted by the HP technology consultants. The report will discuss the observed and recommended methodology for running a secure highly available, high-performance network. Identified risks to network security and availability will be documented, along with recommended mitigations for those risks. There will be a detailed analysis of the current-state network security architecture and the rationale for the recommended changes, both tactical and strategic, achieved by consensus between HP and the Customer. The report will be delivered as Microsoft Word document.

Customer responsibilities

The Customer will:

- Assign managers and others, as appropriate, to work with HP throughout the project
- Review status or acceptance reports, as provided, and provide acceptance or feedback as specified
- Purchase or provide all hardware, software, licenses, staff, current maintenance contracts, and environments necessary for HP to provide these services
- Provide HP personnel with access to the Customer’s facilities, computer room, systems, passwords, etc., as needed during normal business hours and after hours, if needed.
- Provide a suitable work area based on the number of onsite HP consultants. The work area will include desks, chairs, phones, and Internet/HP network access through a Virtual Private Network (VPN).
- Perform any backups needed before changes are made, and back up the target systems and work implemented by HP.
- Perform all entries and approval tracking for the Customer’s internal change management process.
- Be responsible for schedule management and execution
- Assign a project sponsor from the Customer’s staff who:
  - Is available to HP personnel throughout the life of the project
  - Acts as an escalation point when conflicts cannot be resolved by the project manager
- Assign a project manager from the Customer’s staff who:
  - Is responsible for directing the work efforts for the Exchange systems architect
  - Is responsible for the accuracy, completeness, and timely provision of all information provided by the Customer
- Is responsible for all Customer aspects of this project
- Has authorization to make all decisions relative to the project, including identification and assignment of Customer resources
- Is available to HP consulting personnel throughout the project’s life
- Is authorized to sign status reports, approve consultant hours, and approve project changes
- Will coordinate all interviews or meeting schedules
- Is authorized to approve project changes

Service limitations

- Service is limited to identification of security issues. HP will not make changes to the Customer’s configurations, hardware, or applications.
- Any corrective measures to mitigate the risks identified by this service are the responsibility of the Customer.
- The review is valid only for the time period in which it is performed. Security risks and countermeasures are always changing; continued security vigilance is the responsibility of the Customer.
- HP does not guarantee that services will identify all security vulnerabilities. HP shall not be liable for security breaches.
- The service is custom priced on the basis of the activities included in the agreed statement of work, and any services not clearly specified in that document are excluded.
- All deliverable documentation created for this engagement will be available in electronic format.

General Provisions/Other exclusions

- HP reserves the right to charge, on a time and materials basis, for any additional work over and above the service pricing that may be requested by the Customer or may result from work required to address service prerequisites or other requirements that are not met by the Customer.
- HP reserves the right to re-price this service if the Customer does not schedule and provide for subsequent delivery within 30 days of purchase.
- HP’s ability to deliver this service is dependent upon the Customer’s full and timely cooperation with HP.
- This engagement is deemed fully completed and accepted as soon as the summary reports have been presented to the Customer.
- Minimum consulting period is one (1) business week.
- This services engagement will be performed at the Customer’s facilities between the hours of 8:00 a.m. and 5:00 p.m. local time Monday through Friday excluding HP holidays, unless otherwise agreed between the Customer and HP in the statement of work.
- HP’s ability to deliver this service is dependent upon the Customer’s full and timely cooperation with HP, as well as the accuracy and completeness of any information and data the Customer provides to HP.
For more information

For more information please contact your HP Network Consulting Sales representative or visit our worldwide web site at:

www.hp.com/services/consulting