E Com Security®
Solutions

Firewall / VPN Security Review

Gain visibility on firewall configuration and access lists to secure, optimize, comply with regulations and manage to keep them secure from external threats.

Expertise

Our consultants have years of expertise translating customer data and feedback to improve network infrastructures, systems, security domains, and processes in alignment with business objectives. We have assisted organizations in a variety of industries, providing us with knowledge of how different sectors secure their data.
Our expertise ranges from redesigning a branch office network topology, to meeting PCI requirements on an organization-wide basis.

Firewall Assurance

Firewalls serve as one of the first lines of defense protecting an organization's network infrastructure from an external attacker. If this defense is weak, an organization could face considerable risk of being compromised. During a Firewall Assessment, we perform a line-by-line analysis of the firewall's configuration for industry best practices that are taken from the Center for Internet Security, PCI-DSS, NIST, the DoD, and vendor-specific guidelines.

During firewall review, we will examine vendor specific vulnerabilities, ingress and egress access controls, logging and auditing, and system management. This review also helps avoid malicious infiltration and ensures true end-to-end security with the Virtual Private Network (VPN) Security Assessment.

Key Benefits

- **Ensure your "front door" is locked**
  Detailed analysis of your firewall protects against misconfigurations, poor policies, and faulty deployment architectures that can leave your enterprise vulnerable to intruders.
- **Comply with industry best practices**
  Verify that device configurations are properly set for the highest level of protection.
- **Get next step recommendations**
  Our deliverables include a Firewall Security Assessment Technical Report, an Executive Summary, and a half-day workshop that includes a Firewall Assessment Presentation.
- **Secure remote access**
  Prevent hackers from using your VPN as a tunnel to your internal network.
- **Verify complete security**
  Ensure your enterprise has end-to-end security and not just an encrypted tunnel. Also, confirm the security of both your SSL-based VPN and your IPSec-based VPN.

Three key steps of the Firewall security Assessment on Demand process.

1. Customer uploads
2. E Com Security Solutions on Demand conducts a thorough security review of the firewall.
3. Customer reviews and analyzes the results of the firewall review in the form of a detailed report or dashboard.

For more information

Visit www.ecomsecurity.org to learn how we can help secure your organization.

Proven Methodology

During a Firewall Security Assessment, our security consultants review device configurations and architectures, perform vulnerability scans as needed, and conduct interviews with firewall and network administrators. Device configurations are analyzed line by line to ensure that they conform to industry best practices applicable to the environment. Network diagrams and interviews with network administrators are conducted so that we can fully understand your network and its vulnerabilities.

Firewall Documentation and Process

- Review of the security access control model that denies access by default, such that explicit access permissions must be specified.
- Review of ruleset comments to ensure each provides business justification for the defined rules.
- Review the configuration file for the identification and protection of all network segments.
- Validate the implementation of open ports and services are required for operations.
- Review the security monitoring process and its ability to detect and alert for attempts at or successful unauthorized access where technically feasible.
- Review the overall configuration of the firewall to ensure that best practices are fulfilled.

Control Plane Baselines

- Review the processes for monitoring and logging that have been implemented on the firewall.
- Ensure that encryption and hashing operations, as well as the firmware in use do not have unnecessary vulnerabilities.
- Ensure that interactions with other devices meet best practices and offer only secured conversations.

Data Plane Baseline

- Review all ingress/egress points within the network.
- Verify rules have been implemented in accordance with the principle of least privilege.
- Verify the use of inspection rules to handle ephemeral ports, and to guard against common attack vectors.

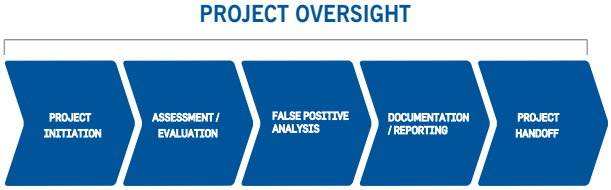
Management Plane Baselines

- Ensure default accounts, passwords, and network management authentication strings have been changed and meet complexity standards.
- Ensure the organization limits the use of clear text protocols such as Telnet, SNMP v1/v2 and FTP.
- Ensure that the implementation of banners, access controls, and been followed.
- Ensure limitation of administrative access is to as few endpoints as possible.
- Review controls for default accounts, passwords, and network management community strings.

Report Development & Delivery

During the testing, we will immediately report any critical and/or high risk vulnerabilities identified via a status update report. When the testing has been completed, you will receive a formal report that will contain:

- A detailed explanation of the testing activities that have been completed and the methods used by us to determine the results
- A listing of all identified vulnerabilities within your firewall architecture with a ranking of their level of risk, the ease with which they can be exploited, and mitigating factors
- An explanation of how to mitigate or eliminate the vulnerabilities including enhancement of your policies, adoption of industry best practices, changes to security processes and enhancement to your firewall architecture



Proven ITIL-based methodology

We apply a comprehensive, ITIL-based methodology and proven tools to every engagement. You receive not only the best expertise, but the best practices to help you deploy and use your firewalls securely and effiectively.