Firewall Rule Review

OVERVIEW

Firewall technologies have evolved from first-generation technologies that focused on access control at the port and protocol layers. They have advanced to next-generation devices that enable capabilities around granular user and application controls. Many vendors have integrated additional capabilities into a UTM (Unified Threat Management) solution that enables features like:

- URL Filtering
- Malware detection
- Threat Intelligence Exchange
- IPS (Intrusion Protection System)
- IDS (Intrusion Detection System)

While firewalls have traditionally been deployed in a North-South configuration, or at the edge of the perimeter, more solutions are being designed to be placed around the East-West segments, which essentially refer to protecting specific servers (in many cases virtual environments) that form an integral part of software defined networking (SDN).

*East/West Traffic flows often greater than North/South flows*

OnX will review customer’s firewall to ensure it is meeting best practices, compliance, and utilizing all of its capabilities.
FOCUS AREA

Regardless of its feature set, the firewall contains at its core a set of rules that dictate what traffic is allowed or denied through the network. As networks continuously evolve, such rule sets undergo a significant amount of changes.

It is a recommended best practice to review the entire rule set periodically to ensure that rule sets do not contain overly promiscuous rules that may allow malicious traffic through the firewall and into the network.

ONX APPROACH

1. Review Documentation and Artifacts
2. Interview Key Personnel
3. Sensor Deployment
4. Analysis
5. Verify Findings and Re-interview

Phase 1: Review Documentation and Artifacts

> The team will collect and review documentation regarding the organization’s corporate layouts, network diagrams, architectures, Firewall Request / Modification / Change Process, and other relevant information that is in scope for the assessment.

Phase 2: Interview Key Personnel

> Interviews of key personnel will be conducted to help determine best practice recommendation and compliance checks.

Phase 3: Sensor Deployment

> If a Firewall (FW) sensor is used, it will be deployed using industry best practices and the experience/judgment of the security engineer.

Phase 4: Analysis

> Analyze the configuration and policies of customer’s FW in scope for the project.

Phase 5: Verify Findings and Re-interview

> The team will investigate specific issues in the scope of the FW review.
> Identify and evaluate the gaps in security.
> Second interviews of key personnel will be conducted verify issues with artifacts.

Once Review is Complete:

> Security Engineer will conduct analysis and report creation.
> A detailed presentation of findings and recommendation is provided.
RELATED SERVICES

- OnX Security Posture Assessments
- OnX Security Audit
- OnX Security Governance Support
- OnX Security PenTest
- OnX SaaS Application (SAS) Assessments
- OnX Information Security Consulting Services
- OnX Threat to Network & Cloud Forensic (TNCF) Assessments
- OnX Fortify Software Training
- OnX Source Code Assessment Services

PROJECT MANAGEMENT

OnX includes a project manager as part of all projects to manage the overall project team, create and maintain the project plan, communicate status on a recurring basis and facilitate escalations as needed. This will minimize risks and ensure timely and successful service delivery. The caliber of the Project Management team allows us to tackle the complexity of projects and ensure successful implementations for our clients.

Additionally, OnX maintains a knowledge base of “lessons learned” comprised of feedback from all service deliveries to help prevent unforeseen delays and other impacts on the project.

WHY ONX?

OnX’s full-lifecycle support services encompass design, installation, integration, implementation, and project management. Our core competencies have scaled to include Software Development Security improvements, Security Operations Services, and Information System Security Management.

- Our security consultants are members of (ISC)², ISACA, SANs, Cisco, and many other organizations. Our team members hold certifications including CISSP, CISM, CEH, CHFI, PMP, CCIE, and much more.
- Our experienced Information Systems Security Professionals (ISSPs) work with our other IT subject matter experts (e.g., OpenStack, Hadoop, VMware, Cloud, etc.) to design and integrate custom enterprise security solutions, giving our clients access to skills and expertise beyond their in-house IT teams and traditional resellers.
- We have 30+ years as a Solution Provider with Data Center and Managed Services heritage and expertise.