AT&T Consulting

Firewall Assessment Services

A number of key factors make firewall change management and compliance issues complex and prone to security vulnerabilities. The natural aging of firewall rulebases combined with administrator error increase the risk of device misconfiguration. Unwieldy rulesets resulting from cumulative changes make it increasingly difficult to map rulebases against current policy. Furthermore, fast paced business decisions tend to trump controlled change management procedures. As a result, seemingly "protected" networks can be exposed to significant risks.

Firewall Security Assessment

The AT&T Consulting Firewall Assessment Service ("FAS") addresses the complex configurations of today's firewall environment. FAS was created to assist organizations with internal and regulatory compliance requirements regarding firewall audits and policy review, provide administrators with information to help troubleshoot rulebase issues, help identify risks to the security of protected environments and help bring order to an otherwise chaotic rulebase.

AT&T Consulting brings deep experience in the industry and an intimate knowledge of the controls required to achieve compliance with prominent standards. Our experience in thousands of networking environments including Fortune 50 organizations, coupled with our extensive experience in network security architecture and firewall management practices, makes for a strategic security service that can help improve firewall security and efficiency.

Firewall Assessment Services Overview

Whereas firewall administrators typically spend countless hours analyzing rulebases and determining the requirements for each rule, our FAS service takes a top-down risk-based approach. We take a comprehensive look at the firewall implementation, from its underlying hardware and software configuration to the network placement, rule implementation and management practices. This helps you more effectively manage future rule changes, promoting more efficient and cost effective firewall administration. The AT&T Consulting Firewall Assessment Service is comprised of three tiers: Standard Assessment, Enhanced Assessment, and Premium Assessment.

Standard Firewall Assessment

A standard security assessment of the rulebase analyzes each rule against the rule of least privilege, pinpoints temporary, unused or overly loose rules and assigns security risks where needed. This assessment takes into account the asset values of the systems involved, attack vectors and other threats and any existing vulnerability known with the systems involved.

One of the underlying principles in rule design is known as the principle of least privilege. This principle ensures that a rule is constructed so it only provides the minimum access required to perform an operation or meet a business need. The Standard Firewall Assessment uses the principle of least privilege as a guide for uncovering the following:

Promiscuous Rules
Rules allowing more access than necessary to meet business requirements.

Potential Benefits

- Help provide your organization with the analysis and refinement required for an effective firewall security policy
- Assist in eliminating administrative overhead and comply with internal and external regulations
- Help boost firewall performance and security through a tiered, cost-effective and comprehensive assessment methodology

Features

- Standard Assessment
- Enhanced Assessment
- Premium Assessment

To learn more about AT&T Security Consulting, visit www.att.com/security-consulting or have us contact you.

Share this with your peers

Shadowed Rules
Rules that are incorrectly ordered in the firewall rulebase and as a result prevent the execution of other rules. For example, a rule permitting access to a server appearing before a rule denying access to the server from the same source will alter the intent of the proposed rule and increase risk exposure.

Redundant Rules
Rules that duplicate all or a portion of the access allowed or denied by other rules. For example, a rule providing access to a system over a specific port is redundant when another rule already exists allowing that access due to the port's assignment in a service container or group.

Enhanced Firewall Assessment
An enhanced security assessment combines the actions and benefits in the Standard Assessment with an additional ruleset consolidation effort to help streamline the rulebase and improve overall firewall performance.

Building on the value provided by the Standard Firewall Assessment, the Enhanced Firewall Assessment provides the opportunity to refine and organize the firewall configuration by taking the existing rulebase and distilling it down into a more clear and concise rulebase.

The Enhanced Firewall Assessment helps uncover Orphaned Rules, which are rules that are never referenced by the firewall software and are no longer required because the systems specified in the rule no longer exist or presently serve other functions. Unused objects within rules that are not necessarily orphaned are also identified during this process and help refine the object list and enhance the overall firewall performance.

Premium Firewall Assessment
A premium security assessment provides a more investigative approach to the ruleset by documenting business justifications and providing a risk rating for each rule.

As rulebases grow and become more complex, rule implementation becomes more time consuming. Often emergency outages require fast paced rule changes, bypassing normal change management checks and balances. When these rule changes remain in rulebases they may present a significant security risk to the organization. The Premium Firewall Assessment begins with the analysis and organization work of the Standard and Enhanced Firewall Assessments and helps uncover additional rulebase errors, such as the following:

Rule Specification Errors
Rules that are incorrectly specified in the rulebase due to misinterpretation of the change request or business requirement.

Rule Composition Errors
Rules that are composed incorrectly in the rulebase. For example, specifying TCP port 32 when the business requires TCP port 23 or neglecting to input a rule required by a business specification is a rule composition error.

Firewalls provide a means to document or comment on an implemented rule, but often these descriptions – if specified – involve ticket numbers or reference codes that are unavailable. The Premium Firewall Assessment will help document the business rationale for each rule while assessing the risk each rule has on the overall business.

Each of the above assessment levels includes a specific level of review aimed at the firewall's operating and overall device configuration as part of the Firewall Design, Configuration and Management Review.

Firewall Design, Configuration and Management Review
AT&T Consulting will perform a comprehensive assessment of your organization's firewall management processes and firewall network design. The information uncovered during the Firewall Design, Configuration and Management Review will serve as background for each Firewall Assessment Service. Key components and objectives of the review, based on level of Firewall Assessment Service chosen are:

- A Security Configuration Review (Standard Level) aimed at reviewing the operating system security settings of the firewall, such as administrative access, user groups, password settings, SNMP settings, running services, high availability configuration, and audit and log settings.
- A Hardware/Software/Operating System Review (Enhanced Level) that includes the security configuration review plus an analysis of the underlying hardware platform and operating system including CPU and memory usage, disk capacity/usage, BIOS revision, patching, and end of life/end of support checks.
- A Network Configuration Review and Statistical Analysis (Premium Level) that includes the Hardware/Software/Operating System review plus a review of network settings and performance on the firewall, such as interface usage/configuration, routing accuracy and consolidation opportunities, as well as NAT and ARP accuracy. This review also includes a statistical analysis of the firewall, such as interface errors, interface state transitions, HA and uptime statistics.
- A review of management practices (all levels) that can directly affect the security of the device including secure remote access, access controls, rule change management, and backups.

Security Solutions: Expertise from a Trusted Provider
AT&T provides a unique and world-class portfolio of compliance and related security services. Our experience, expertise and commitment to open standards have established us as a strategic and trusted advisor. By leveraging AT&T, you can expect best-in-breed solutions, a global network of proven technology, and a cost-effective program-based approach to meet your security and compliance needs.

For more information contact an AT&T Representative or visit www.att.com/security-consulting.

Share this with your peers

To learn more about AT&T Security Consulting, visit www.att.com/security-consulting or have us contact you.

Scan this code to learn more.

03/04/14 AB-1996-02