Firewall Migration

The Juniper Networks Firewall/VPN solution helps you to reduce the total cost of ownership, increase scalability and enhance the stability of their networks. To take full advantage of these benefits, the customer needs to migrate quickly and effectively.

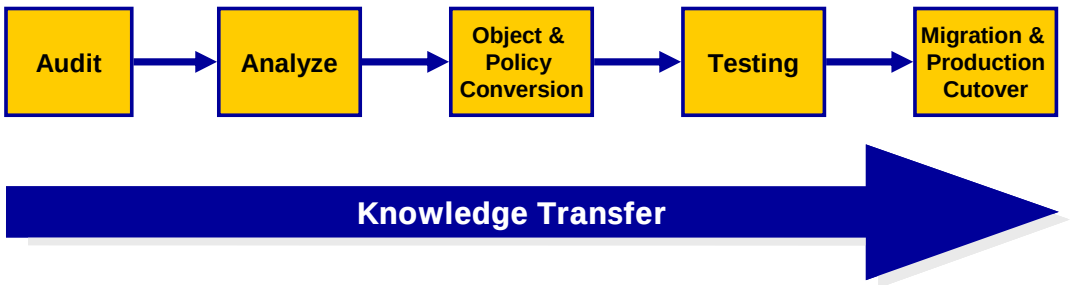
Juniper Networks Professional Services has the skills, processes, and tools to reduce the risk and ensure a rapid migration in as little time as possible. Our proprietary tools help reduce the tedious tasks and minimize errors, thus reducing the time and cost to migrate. However, the value of our Firewall Migration service is in the people. The biggest challenge is analyzing a given network and system to determine the best way to migrate and the best tools to use, and then designing a solution. The tools do not eliminate the need for follow-on analysis and are just a portion of the total solution.

Service Overview

The primary benefits of the Juniper Firewall Migration Service include:

- **Speed of Conversion**. Juniper's proven methodology converts legacy firewall configurations more rapidly than if done manually and with fewer errors.
- **Minimal Configuration Errors**. Juniper Networks Professional Services thoroughly checks each configuration that it created from a legacy configuration. Juniper procedures avoid the errors that can be introduced by manual conversions.
- **Custom Tools**. Juniper has invested in creating tools and procedures that have been tested by Juniper PS and hardened by numerous previous migrations in customer networks.
- **Experience**. Juniper understands the NetScreen Firewalls and its capabilities better than anyone and uses this knowledge to provide the best implementation possible. Not only do we know what needs to be considered in doing a migration, but we understand where problems may be encountered and how to resolve these problems.
- **Cost**. The cost of manual conversion or developing similar migration capabilities can be cost prohibitive. Utilizing the Firewall Migration Service:
  - Eliminates the time and effort to develop the migration process
  - Reduces the time and effort required to create the ScreenOS configuration files
  - Reduces or eliminates the cost of debugging and fixing errors introduced in the configuration files during the migration
  - Provides your staff with valuable knowledge transfer related to the migration to NetScreen firewalls – significantly lowering the learning curve in the process

Project Summary



Juniper has developed a proven methodology to migrate legacy firewall gateways to Juniper Networks NetScreen Firewall/VPN systems and devices. This methodology consists of the following process steps:

Step 1: Audit

The Juniper consultant works with you to understand the present firewall design and its configuration. An initial firewall policy and configuration review is performed to identify any security issues with the configuration, and to identify areas where policy clean-up can be performed.

Step 2: Analyze

The Juniper consultant analyzes the policy to determine the optimum design given your security requirements while effectively utilizing ScreenOS features. Feature differences are identified, policy and object grouping issues are examined, and a zone-based policy migration is planned. In addition, design issues such as Network Address Translation (NAT), High Availability (HA) and user authentication are explored.

Step 3: Network and Workstation Object, Service Object and Policy Conversion

Using the results from the prior step, the Juniper consultant works onsite using automated and manual methods to convert the firewall policy and configuration to a ScreenOS configuration. The ScreenOS configuration includes:

- A custom service book and service group configuration
- A custom zone-classified address book and address group configuration
- A zone-classified set of ScreenOS policies

Additionally, if utilized in the firewall configuration:

- A local database of user and group authorizations
- NAT configuration
- User authentication policies

The new configuration is imported into the ScreenOS device(s) and preliminary testing is performed. If the NetScreen Security Manager (NSM) is being used for centralized device management, the device(s) will be imported. The configuration may be changed and optimized based upon the results of this initial testing.

Step 4: Function and Other Testing

Based upon test requirements identified in the prior steps, additional tests are planned and executed. These may include function tests that verify routing and policy sets. We also perform HA testing in this step if it applies, in order to verify the HA design and its configuration.

Step 5: Migration and Production Cutover

A migration plan is developed and the Juniper consultant will work onsite to execute the cutover to production, monitor the function of the NetScreen devices after the cutover, and fine tune the configuration if needed.

Deliverables

As part of these activities, the following deliverables are provided:

- High Level security design
- Detailed migration plan
- Functional and implementation test plan
- Finalized ScreenOS configuration files for each firewall migrated

September 2005