FIREWALL RULE BEST PRACTICES

This page covers general best practices for Firewall Rule configuration:

1. DEFAULT DENY -

There are two basic philosophies in computer security related to access control: default allow and default deny. **A default deny strategy for firewall rules is the best practice**. Firewall administrators should configure rules to permit only the bare minimum required traffic for the needs of a network, and let the remaining traffic drop with the default deny rule built into NetXGATE Firewall. In following this methodology, the number of deny rules in a rule-set will be minimal. They still have a place for some uses, but will be minimized in most environments by following a default deny strategy.

In a default two-interface LAN and WAN configuration, NetXGATE utilizes default deny on the WAN and Limited allow on the LAN. Everything inbound from the Internet is denied, and Permit only what a network requires out to the Internet from the LAN side. All home grade routers use this methodology and most similar commercial offerings. It's what most people expect out of the box, therefore it is the default configuration. That said, while it is a convenient way to start, it is not the recommended means of long-term operation.

NetXGATE users often ask "What bad things should I block?" but that is the wrong question as it applies to a default allow methodology. Noted security professional 'Marcus Ranum' includes default permit in his "Six Dumbest Ideas in Computer Security" paper, which is recommended reading for any security allow all rule on the LAN and adding block rules for "bad things" above the permit rule.

2. KEEP IT SHORT -

The shorter a rule-set, the easier it is to manage. Long rule-sets are difficult to work with, increase the chances of human error, tend to become overly permissive, and are significantly more difficult to audit. Utilize aliases to keep the rule-set as short as possible.

3. REVIEW FIREWALL RULES-

We recommend a manual review of the firewall rules and DNAT configuration on a periodic basis to ensure they still match the minimum requirements of the current network environment. The recommended frequency of such reviews varies from one environment to another. In networks that do not change frequently, with a small number of firewall administrators and good change control procedures, quarterly or semi-annually is usually adequate. For fast changing environments or those with poor change control and several people with firewall access, review the configuration at least on a monthly basis.

Quite often when reviewing rules with customers we ask about specific rules and they respond with "We removed that server six months ago." If something else would have taken over the same internal IP address as the previous server, then traffic would have been allowed to the new server that may not have been intended.

4. DOCUMENT THE CONFIGURATION

In all but the smallest networks, it can be hard to recall what is configured where and why. We always recommend using the Rule Name field in firewall and NAT rules to document the purpose of the rules. In larger or more complex deployments, create and maintain a more detailed configuration document describing the entire firewall configuration. When reviewing the firewall configuration in the future, this will help determine which rules are necessary and why they are there. This also applies to any other area of the configuration.

It is also important to keep this document up to date. When performing periodic configuration reviews, also review this document to ensure it remains up-to-date with the current configuration. Ensure this document is updated whenever configuration changes are made.