NetScreen's Approach to Scalable Policy-based Management

March 2002

A White Paper By
NetScreen Technologies Inc.

N E T S C R E E N™

Table of Contents

Introduction

The success of a security solution depends greatly on the effectiveness of the management system in deploying, maintaining, and monitoring the various infrastructure devices. Traditional methods of management require considerable manual effort which often result in service delays, budget overruns, or worse, security breaches.

NetScreen offers a new approach to security management that differs fundamentally from traditional methods by eliminating the majority of the manual effort. The NetScreen-Global PRO security management system introduces a policy-based management approach that greatly reduces the time and effort required to roll out even the most complex security deployments based on NetScreen's leading security systems and appliances.

Traditional Management vs. Policy-based Management

The traditional approach to security device management normally consists of managing each device as its own individual unit. Specific policies such as access filters/firewall rules or VPN definitions are created via a command line interface or perhaps through a more user-friendly Web interface. While straightforward in approach, this method has several issues [see figure 1]. First, there are little to no economies of scale as each configured devices is treated as a unique system. While this may not be a major issue for smaller security deployments, as the network grows, the complexity of the security deployment will grow exponentially—an issue often referred to as the "n-squared problem".

Traditional Management	Policy-Based Management
Per device management	Management by defined groups
Policies individually created	Policies set according to groups
Issues • No economies of scale; network growth increases complexity • Lack of overall view of ecurity posture • Potential for user input error	Benefits • Scalability; Administration burden controlled even with growth • Ability to assess overall security protection ser error mitigation

Figure 1: Traditional vs. Policy-Based Management

Second, the security administrator must go to each and every device to understand their current security posture—what is being protected, who can talk to whom, etc. There is no single up-to-date view on the status or configuration of the overall system, which can prove to be very dangerous if the system comes under attack.

Finally, if each device configuration is created manually, the chance for human error is high. At best, these errors can cost the administrator extra hours of troubleshooting. At worst, they can lead to costly security breaches. Even some approaches that consist of building bulk batch script files can prove error-prone as much of the scripting operation is often still done on a manual basis. Virtual private network [VPNs] creation adds an additional layer of complexity as peer devices require exactly matching security association [SA] parameters in order to successfully engage in a VPN.

In contrast, the Policy-based approach provides some clear advantages. Configurations are defined not on a device by device basis, but rather according on policy groups. These groups are created based on various parameters, such as location, device type, customer type, level of trust/threat, etc. The economies of scale are striking—what in the past had required hundreds of individual policy rules is now reduced to just a few high-level policy rules. This translates into considerable time and money savings and allows the administrative staff overhead to grow at a slower pace than the growth of the security infrastructure. Budget that had been earmarked for staff can now be redirected at investing in profitable core infrastructure [see figure 2]
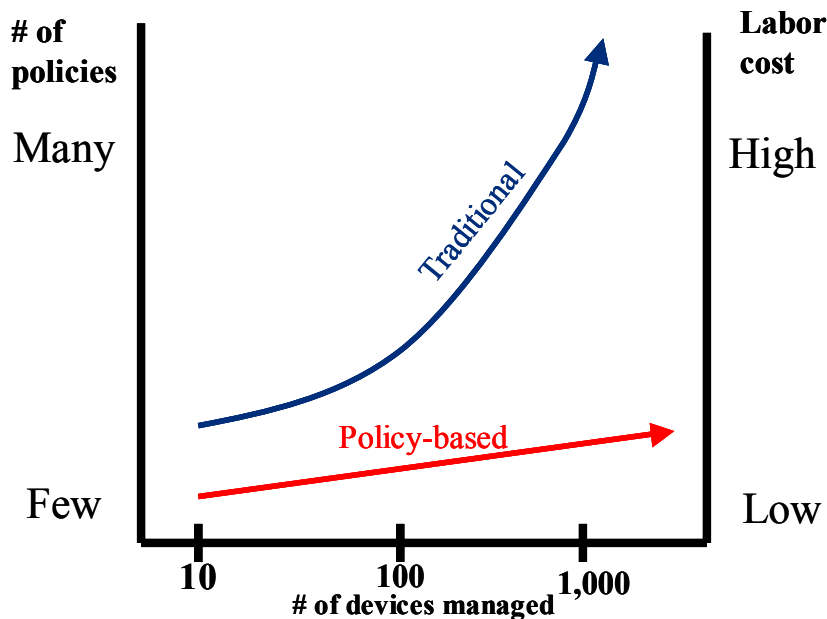

Figure 2: The Economies of Policy-Based Management

The second major advantage of a policy-based management approach is the ability for administrators to obtain a unified view of the organization's security posture. As all security policies and profiles are stored in a common database system, configuration parameters can be assessed in real-time across multiple locations. This "knowledge capture" helps ensure that critical information is effectively shared among administrators.

Finally, a policy-based management system can greatly reduce the chance of human error by allowing the administrators to focus on the high-level security goals while the majority of the "heavy lifting" is now done by the automated processes in the system. With policy based management, changes in security or VPN policies don't cause hours of device reconfiguration.

Building-Block Approach

NetScreen-Global PRO has at its foundation a policy-based approach to security management. This foundation can be viewed as a somewhat "building block" structure for system and configuration management [see Figure 3], where various layers of security polices are attached to devices or device groups.

First, device-specific parameters, such as IP address, contact information, local subnet address, etc. need to be set up for each device managed. These parameters can either be input manually or can be imported from existing devices.
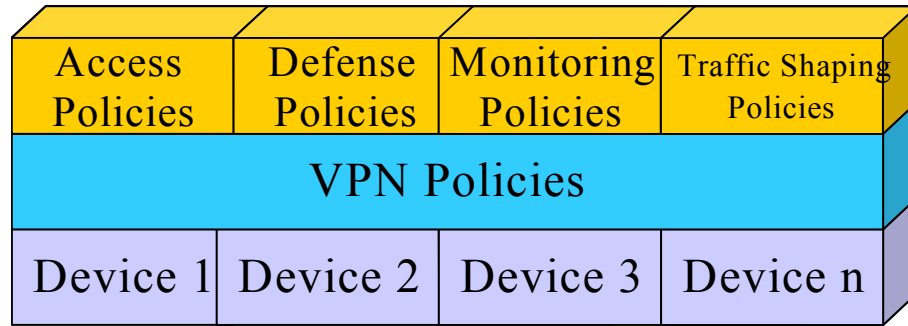

Access Policies	Defense Policies	Monitoring Policies	Traffic Shaping Policies
VPN Policies			
Device 1	Device 2	Device 3	Device n

Figure 3: Building Block Security Policies

Next, VPN polices are layered across the devices by defining the basic VPN parameters [type of encryption, mesh or point-to-point, etc] and then simply selecting which locations are to participate. VPNs can be set up to be as general as allowing all traffic to be encrypted among the locations or can be as granular as specific applications on individual devices.

Finally, the remaining access control and other policies are defined as global template objects that can be assigned to groups of devices. These policy objects provide a powerful mechanism to share policies across devices and quickly enforce bulk policy changes. If the policy object changes, the specific configurations of all affected devices are updated accordingly. Furthermore, if a new device is added to a device group, it will automatically receive the policies for that group.

The Global PRO system's flexible grouping architecture is one of the key features that set it apart from other security management products on the market. Rather than requiring all members of a policy group to share the exact same policy configuration profile, the Global PRO system allows a device to be a member of multiple groups. Combined with the ability to prioritize one set of policies over another there are virtually no limitations as to how groups and policies can be assigned or combined for a given device.

Global PRO System Architecture

The NetScreen-Global PRO security management system is a highly scaleable solution that can manage and monitor NetScreen security deployments of up to 10,000 devices. It consists of a core policy manager engine and a distributed data collection infrastructure for performance and event monitoring [see figure 4]
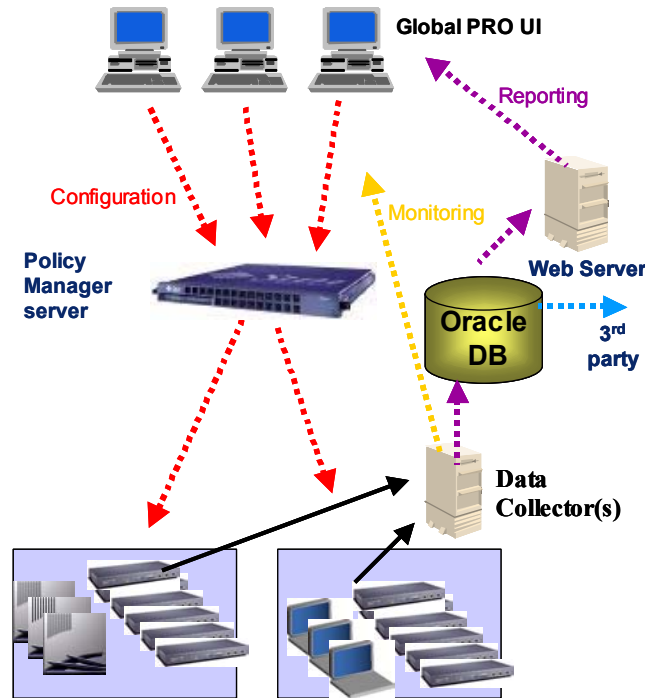
Figure 4: NetScreen-Global PRO Architecture

On the policy management side, which is the focus of this paper, the core of the system is a policy management server. This server is delivered as a turnkey solution with all the necessary software and hardware elements preconfigured. The solution is client-server based, with distributed management consoles able to operate from anywhere in the world which enables follow-the-sun management. The Policy Manager server can arbitrate different requests for policy changes originating from multiple administrators, thereby allowing for flexible management of a common set of NetScreen security devices. All configuration data is stored in an LDAP directory within the Policy Manager server. Devices are updated in bulk by compiling the specific device configurations from the LDAP directory and pushing them on demand down to the target systems. In this way, the security infrastructure can be pre-configured and fine tuned before even deploying the devices.

On the monitoring and reporting side, distributed data collectors receive all events, alerts, and performance data from the NetScreen devices. Real-time event and performance data are forwarded to the consoles while long-term trend information is stored in an Oracle database. Global PRO features various Web-based historical performance and analysis reports that can be run for an individual site or multiple site basis. An open database schema is also provided for integration of the Global PRO collected data into 3rd party reporting tools.

NetScreen's Policy-based Management: Multi-national Corporation Example

The power of NetScreen's policy-based management solution is best displayed with an example. Acme Corp. wishes to deploy a multi-national VPN with regional hubs interconnecting local meshed VPNs. The company also has a base set of access and other security policies that it wishes to deploy to all devices worldwide, but have the flexibility to assign exception rules to specific locations.

Step 1—Set Up Admins

The first step in the process is for the central administrator to define the various levels of administrative privileges for the system. In this case, two administrator groups will be created. SuperAdmins have the ability to control virtually all of the configuration parameters within the Global PRO system, except create new SuperAdmins. The second group are Regional Site Admins who have control only over the devices in their region and only for a subset of administrative tasks.

One key area of this role-based administration is in the management of the regional VPN. A Regional Site Admin is restricted to "read-only" for the specific security parameters used in the VPN, but has full read/add/modify/delete control for the resources that are part of the VPN [see figure 5] . In other words, they cannot change the type of encryption that is used in the VPN, but they can add new sites or remote access users to the VPN. This proves very useful in relieving the central SuperAdmins from day to day management of what new local sites are coming on line and allows them to focus on more complex issues in managing their security infrastructure.
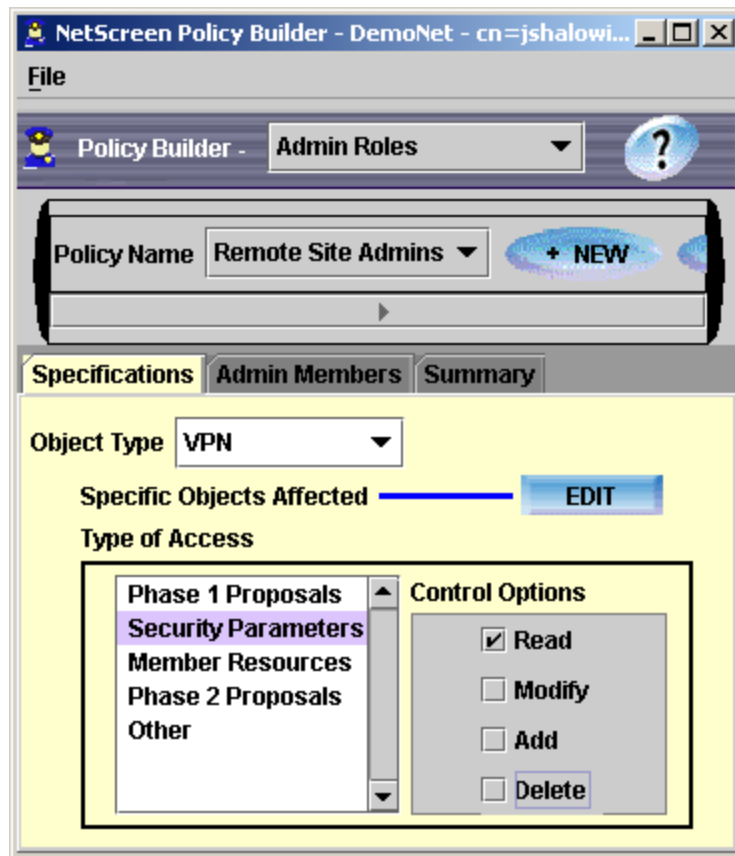

Figure 5: Role-based Administration

Step 2—Create Devices and Device Groups

Adding a new devices consists of defining just a few basic parameters, such as the type of device, the operation mode, contact information,etc. [see Figure 6].

Devices can be easily added via the user interface directly or an existing device configuration may be imported as well.
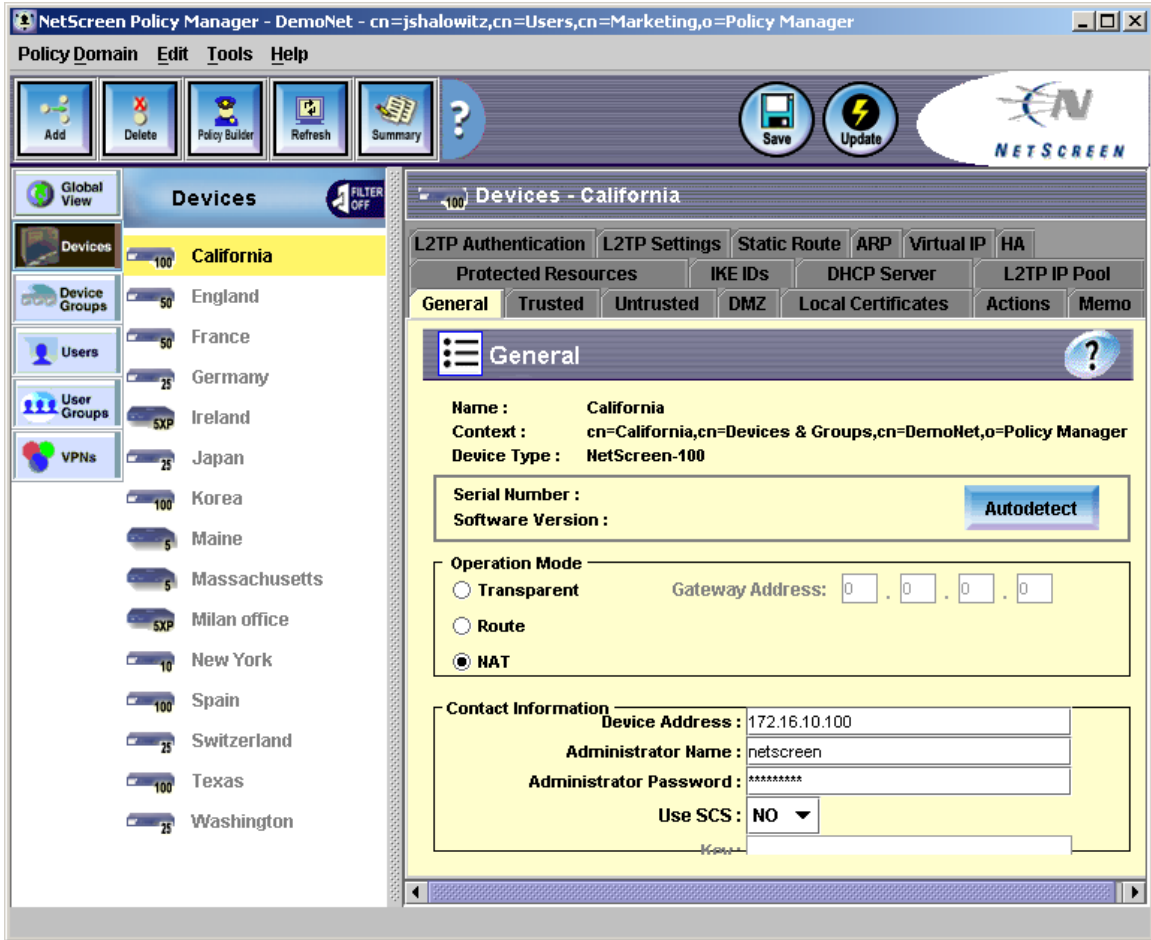
Figure 6: Device Setup

One of the very useful abstractions in the Global PRO system is the concept of "protected resources" for a given device. A protected resource represents the users, user groups, or services [ie. Mail, intranet servers] that are located behind a given device. A device can have one or multiple protected resources. These resources will be used later when we create VPNs. In this example, Acme defines a protected resource for each of its remote office subnets.

Finally, it is advised to place devices into device groups wherever possible to reduce the number of discrete units that must be managed. This will also prove very useful later when new sites are added to the infrastructure as a new device automatically receives all the policies of the group. In Acme's case, as devices are managed by regional administrators, five regional groups are created—Western USA, Central USA, Eastern USA, Asia, and Europe.

Step 3—Set Up VPNs

Acme's business is mostly regional with some core services maintained at Corporate. Therefore, they design their VPN with regional meshed structures and with regional hubs connecting back to the corporate network [see figure 7]
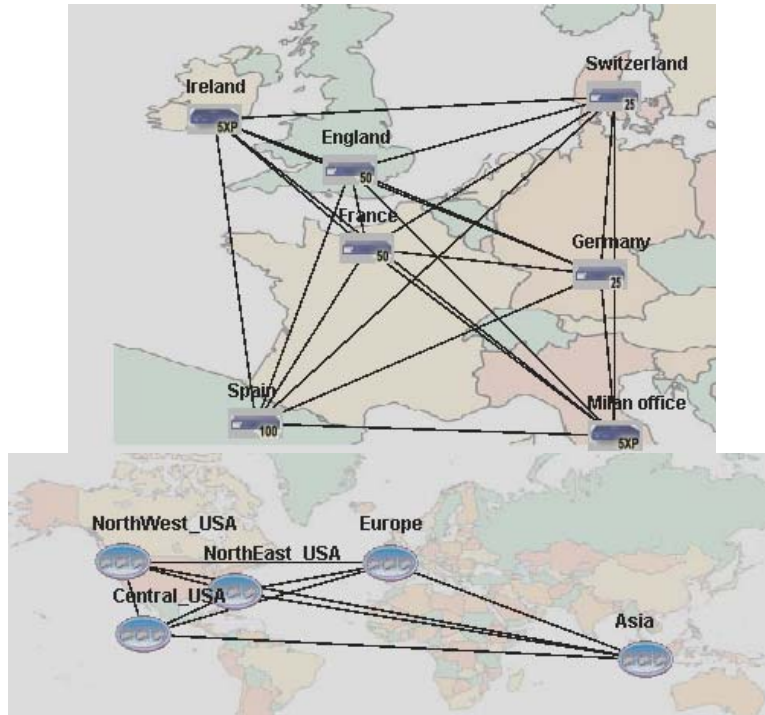
Figure 7: Acme Corp's Regional/Multinational VPN

By utilizing Global PRO, they can quickly define the parameters for regional VPNs and clearly visualize which locations are members of which VPN. When creating a VPN, the specific security parameters [preshare keys, encryption algorithm, phase 1/phase 2 proposals, etc.] only need to be defined once for the group. Next, the protected resources that Acme defined in Step 2 are now simply selected and added into the VPN membership as appropriate [see figure 8]. All the required security associations and access filters for all affected devices are automatically generated by the Global PRO system.
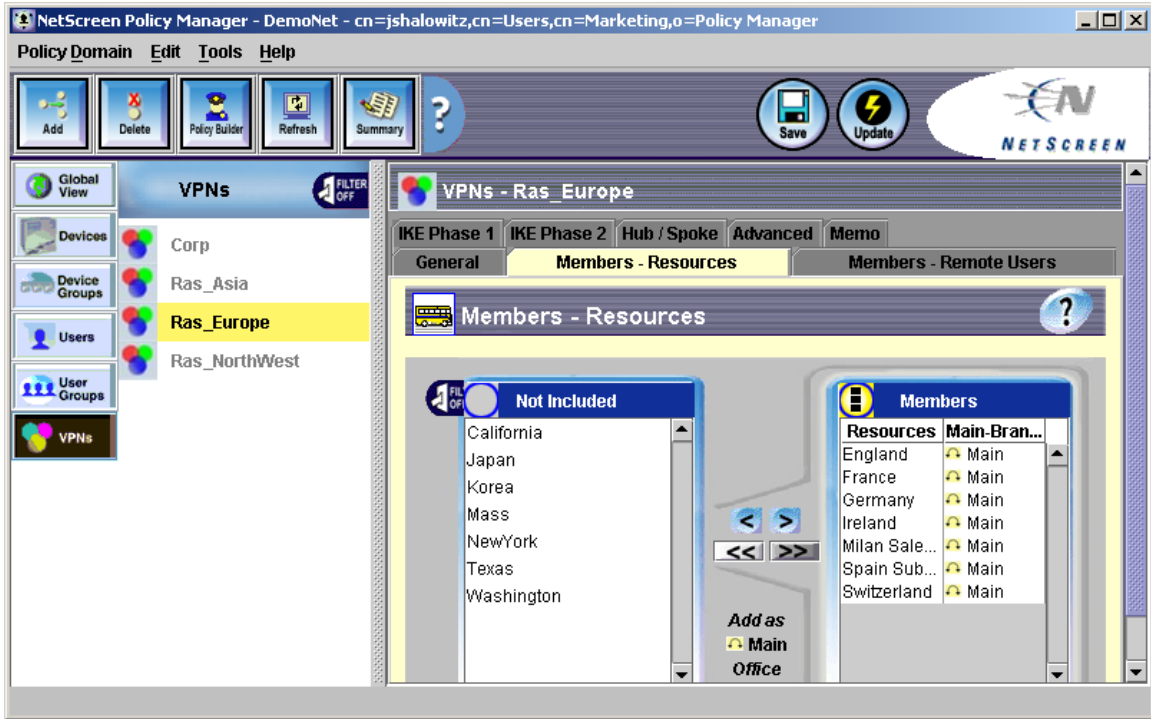
Figure 8: Bulk VPN Setup

In addition, the concept of protected resources provides a very logical and convenient way for Acme to understand the goal of their VPN deployment. No longer do they look at their VPN as just the 'external interface on device A creating a tunnel to the external interface on device B which in turn has a tunnel to device C', but can now view their VPNs as connecting user groups to corporate resources.

Step 4—Layer on Policies

The final configuration step once the VPNs have been configured is to layer on policy rules for the device groups as well as policy rule exceptions for individual locations. For Acme Corp, one set of policy rules pertain to the global policy of restricting Web access during work hours for all groups except the marketing group, which requires Web access to conduct competitive analysis [see Figure 9]. This rule is then applied to all regional device groups.

One powerful feature that Acme will leverage is the concept of relational priorities for policies. Each specific policy template is treated as a unique object that is ordered relative to other similar policy objects according to its priority number. The higher the number, the higher up on the policy list that the rules in this object will be placed. In other words, higher placed rules will take precedence over lower placed rules.
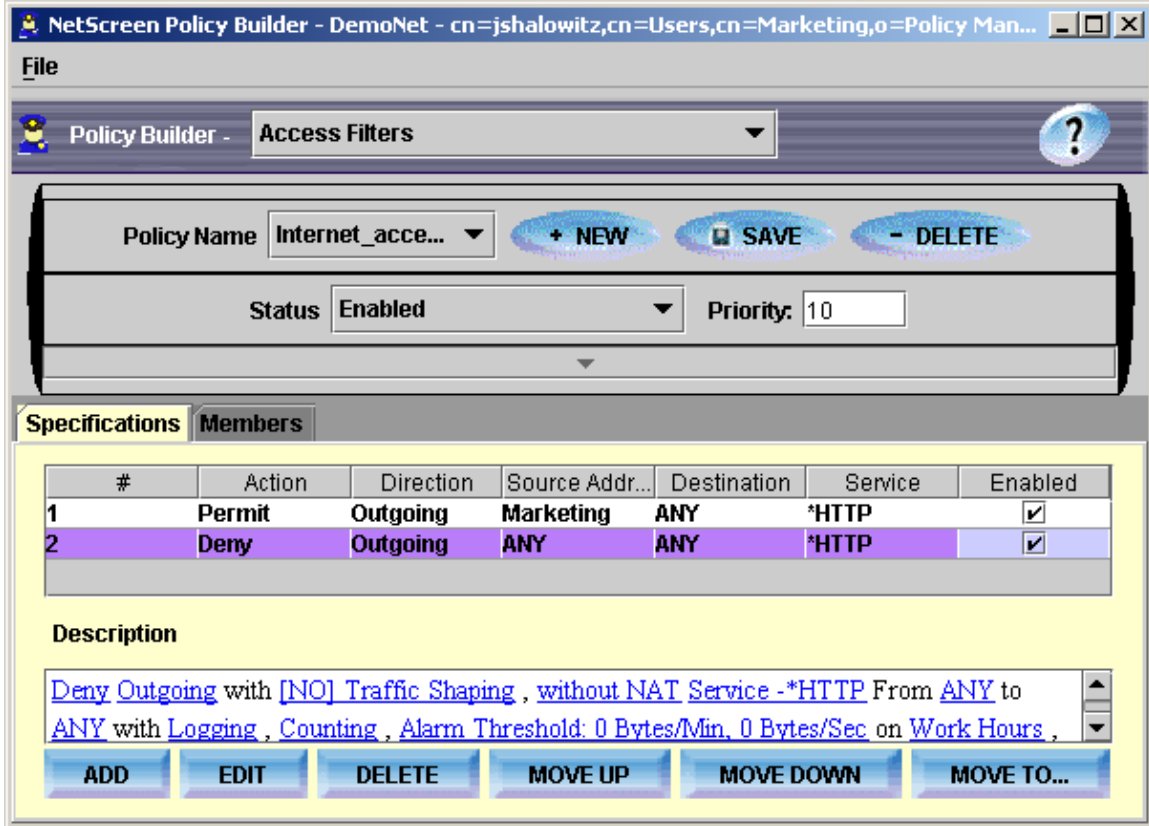
Figure 9—Creating a Global Access Filter Policy

As a result, Acme can create a set of generic global polices and assign them relatively low priority numbers. Meanwhile, a critical exception policy for a given site can be assigned a higher priority number, ensuring that for that device, the exception rule will take precedence. For example, Acme's England office is test marketing the company's new European Web site and all employees in that office require Web access during work hours. Rather than having to go and create a complicated exception for an address group to the generic rule set [Figure 9], Acme can create an exception rule set and assign it to the England office with a priority of 11. This will ensure that this exception rule takes precedence over the "Deny Web access for non-marketing employees during work hours" rule that has a priority of 10.

Step 5—Bulk Deployment of Policies

The final step in the process is to push all of the policy updates to the devices. This represents another key strength of the Global PRO system in that administrators normally do not communicate policy changes directly to the devices in real-time. All changes are made against the policy model stored in the LDAP directory. This provides a high degree of control through a structured change management process.

Acme Corp takes advantage of this feature and creates a process whereby all regional admins must check in their changes to the policy model every Tuesday at midnight GMT. On Wednesday, the SuperAdmins will review and approve all changes, leveraging Global PRO's full audit trail of who made which change requests to which policy sets. On Thursday, a subset of SuperAdmins who have authority to execute device updates conducts bulk updates of devices during the respective weekly maintenance window in each region.

Conclusion

Traditional methods of managing security deployments present considerable risks to the long-term viability of the security infrastructure. Inefficiencies in the management system will inevitably lead to budget overruns, delayed service turn-ups, and at worst security breaches.

The NetScreen-Global PRO security management system provides a very scalable and intuitive approach to security management. As enterprises and service provides seek to further integrate disparate networks around the world, the need for powerful security management systems will grow even greater. Therefore, security administrators must start putting in place the systems today that will ensure the growth of networks tomorrow.