



8e6 Professional Edition Multi-Tiered Administration

INTRODUCTION

The scope of this white paper is to give a description of operation of the Multi-Tiered Administration available with the 8e6 Professional Edition Internet Filter.

PRODUCT DEFINITION

The 8e6 Professional Edition is the most comprehensive appliance-based solution available to protect schools and districts against threats arising from Internet-based learning. Integrating best-in-class URL filtering, forensic Web usage reporting and real-time monitoring and mitigation of insider threats, the Professional Edition's award-winning performance delivers power, ease of use and unmatched scalability.

The Professional Edition Suite includes:

R3000 Internet Filter: Offers high-performance, enterprise-level filtering optimized for speed and scalability. Filters URL's, anonymous proxies, spyware, Instant Messaging, Peer-to-Peer and other emerging threats utilizing M86's 100+ Category Database enhanced by Intelligent Footprint Technology™.

Enterprise Reporter: Processes and displays Internet filtering logs without impacting filtering and network functions. Built on a dedicated MySQL database, it uses a graphical interactive data-mining interface to generate detailed or summarized reports.

Threat Analysis Reporter: Delivers up-to-the-minute graphical snapshots of Internet traffic and is supported by real-time management tools to identify and control user-generated Web threats

FEATURE DEFINITIONS

Global Administrator

The Global Administrator is defined as the account that has complete management control over all R3000 functionality. There can be multiple Global Administrator accounts created. The Global Administrator can create groups on the R3000 for the purpose of filtering and can also create a Group Administrator account for each group. The Global Administrator has unrestricted control over all R3000 features.

Group Administrator

The Group Administrator is an account that has control over the filtering level of a group that has been created by a Global Administrator. The Group Administrator can only affect changes that will impact the filtering of the given group. There can only be one Group Administrator account per group.

Minimum Filtering Level

The Minimum Filtering Level (MFL) is a level of filtering which the Global Administrator can define. The Minimum Filtering Level will then be enforced on all existing groups. For example, if the MFL is set to block General Pornography, the Group Administrator can set the filtering level for his group, however, the Group Administrator cannot remove the filtering of General Pornography from his groups filter.

The MFL is useful when applying a filter that meets an organization's Acceptable Use Policy, while still giving filtering control to downstream Group Administrators. The downstream administrator would be able to add to the MFL, but not remove restrictions enforced by the MFL.

Group

A group is defined as a group of users designated by the Global Administrator. For example, the Global Administrator could create a group designated as all users that exist in the subnet 10.10.10.0/24

Sub-Group

A Global Administrator, or a Group Administrator can create a sub-group. A sub-group is used to further delineate the members of a group. Using the example above, if a group is created using the subnet 10.10.10.0/24, sub-groups could be created within this group, such as 10.10.10.0/25 and 10.10.10.129/25.

Range to Detect

A feature on the R3000 that allows the Global Administrator to determine exactly which range of IP addresses all Internet traffic should source from.

By-pass Account

A by-pass account, is a username/password, which can be created by a Global Administrator or a Group Administrator for the purpose of bypassing the filtering level. The Global Administrator has the option of allowing the by-pass account to override the MFL, or to have the MFL enforced on all by-pass accounts. A by-pass account can be assigned to any user.

CENTRAL MANAGEMENT CONSOLE/ SYNCHRONIZATION

A feature on the R3000, which allows a Master/Slave Relationship to be established between R3000 units for the purpose of configuration, creating a Central Management Console for all R3000 units, such that any change made on the master R3000, is also enforced on the slave R3000 units. This is useful for ensuring that in a multiple R3000 environment, a change is not manually effected on all R3000 units. Instead the change is made one time, and replicated in a near real-time manner to all R3000 units.

For the purpose of defining the use of the multi-tiered administration, we will examine two use cases. In each of the use cases the features would not be exclusive to that particular use case. The use cases include a school district and a statewide school environment.

USE CASE ONE – SCHOOL DISTRICT

Sally is the network administrator for West Area School District. The school district consists of five elementary schools, 3 middle schools, and 2 high schools. The district has a T3 Internet feed at the district office, with T1 connection to each school. All Internet requests go through the Internet connection at the district office.

The district has an Acceptable Use Policy that states that all students and district employees are restricted from accessing any Internet sites which contain materials that would be classified as Pornography, R-Rated, Gambling, Non-Educational Games, Web-Based E-mail, Hate and Discrimination, Alcohol, Illegal Drugs, Cults, and Hacking. However, there is provision in the Acceptable Use Policy that states that district employees can be granted access to these materials for the purpose of research for the betterment of the students, if the school principal provides approval. This clause was put in specifically for school psychologists and counselors that may be dealing with these issues among some of the student population.

Sally installs the R3000 at the district office so that it is filtering all Internet traffic. She then creates a Minimum Filtering Level which blocks access to all of the categories that relate to the districts Acceptable Use Policy. When setting up the MFL, Sally selects the option allowing bypass accounts to override the MFL.

Sally then creates a group for each school, and creates a Group Administrator account for each group. These Group Administrator accounts are then given to the principal of each school. The principal is then able to create, and delete bypass accounts on an as needed basis. The net result is that the Acceptable Use Policy is enforced for all users. However, an on-site school official can grant district employees, who need to do research, access to the needed information.

USE CASE TWO: STATEWIDE SCHOOL ENVIRONMENT

Sam is the Chief Network Administrator for the statewide education network. He is responsible for providing Internet access to all of the school districts across the state. At his data center, Sam has an OC-3 Internet connection. He also has connections of varying size going to each school district. In order for a school district to access the Internet, their connection must come through Sam's data center.

The state has enforced an Acceptable Use Policy, which states that all school Internet access must be free of Pornography, Gambling, Hate and Discrimination, and Illegal Activity. The AUP also states that school districts can have their own AUP, but at no time should access be granted to the information, which the state had deemed inappropriate for schools.

At the data center, Sam installs 3 load balanced R3000 servers; two R3000s to handle the load of a 155.5Mbps pipe, and a third as a redundant unit. These units are setup to use the Master/Slave Central Management Console Synchronization feature on the R3000. Sam configures the R3000s such that there is a MFL that meets the states Acceptable Use Policy. He then creates a group, and a group administration account for each school district that receives an Internet connection from his data center. At each district, the network administrator can login using the group account provided. The network administrator can then choose to use the MFL provided by the state or add to the minimum filtering level. The important thing is that the network administrator cannot lift the restriction implemented by the state.

For example, West School District could receive the group account and never login to the R3000. The result would be that all users at West School District would receive filtering based on the state enforced acceptable use policy.

At East School District, the network administrator may be tasked with enforcing an Acceptable Use Policy that is more restrictive than what been provided by the state. In this case the network administrator would login with the existing group account. He could then apply additional categories for filtering as needed to meet with the district's Acceptable Use Policy.

At North School District, the Acceptable Use Policy calls for all students to meet the state's AUP but also see that all elementary school students receive a greater level of filtering. In this case, the North network administrator would login using the provided group account and create sub groups for each school within the district. He could then apply a greater filtering level to each elementary school and leave the middle schools and high schools to receive the MFL.

At South School District, there is no Acceptable Use Policy, though they are still governed by the state Acceptable Use Policy. However, the network administrator at South School District is a political activist, and does not believe in Internet Filtering. So he decides that he will use the group account to disable the filtering for his school district, despite the AUP given by the state.

The South network administrator would login to the R3000 GUI using the provided group account. However, he would find that he would be unable to lift the restrictions enforced by the MFL that was put in place by Sam on behalf of the state. The Department of Library Services may have no Acceptable Use Policy and determine that the Internet should remain unfiltered. Since Dave has enforced no MFL, all traffic for the Department of Library Services would remain unfiltered.

In short, the net result is that Dave is able to provide filtering to the state agencies that the state agency has complete control over. However the agencies are not able to affect the filtering levels of any of the other agencies. Additionally, Dave has found that the number of calls to his team and the help desk has decreased dramatically. As an additional benefit, Dave has found that the performance on the proxy/cache servers has increased by a very large amount since the filtering was moved off of them.

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters

828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Asia-Pacific

Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Auckland, New Zealand

Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 09.01.09