



828 West Taft Avenue
Orange, CA 92865
714-282-6111
714-282-6117 Fax
www.8e6.com

8e6 3000 | Enterprise Filter



R3000 Multi-Tiered Administration

Scope

The scope of this white paper is to give a description of operation of the Multi-Tiered Administration available on the R3000.

Product Definition

The 8e6 R3000 Enterprise Filter is a hardware-based appliance solution that allows users to monitor, filter and log an organization's Internet traffic. Through user-defined parameters based on 8e6's 75+ categories of Web content, an R3000 filter will help improve employee productivity, reduce liability and preserve network resources.

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 four use cases. In each of the use cases the features would not be exclusive to that particular use case. The use cases include an enterprise business, a school district, a statewide school environment, and a state government.

Use Case One – Enterprise Business

Joe is the Information Security Director for a worldwide shipping company. He is responsible for the Internet connection for all US operations. Joe has a T3 connection to the Internet in the data center at the corporate office in Chicago. There are several shipping hubs that are connected to the main office via T1 connections from Los Angeles, New York, and Atlanta. All of these locations receive their Internet feed from the T3 connection at the corporate office.

All of the traffic that Joe wants to filter is NAT'd at the firewall, so Joe installs the R3000 on the switch just inside the firewall so that it can see all traffic that is received by the firewall. Joe has set the network up such that all Internal IP addresses will exist within the private range of 10.0.0.0/8

Joe has distributed the IP addresses as follows:

10.10.0.0/16 - Corporate Office
10.11.0.0/16 - Los Angeles
10.12.0.0/16 - Atlanta
10.13.0.0/16 - New York

Joe does not have a corporate wide Acceptable Use Policy. Instead it is up to the Human Resources Department at each location to enforce a regional Acceptable Use Policy. Since this is the case, Joe will be setting the filtering level for the corporate office, but he will be creating groups for each of the shipping hubs, and allowing the network administrator at each shipping hub to enforce the regional Acceptable Use Policy. Joe will not be using the Minimum Filtering Level.

Joe configures the R3000 so that the Range to Detect is 10.0.0.0/8. He then creates four groups, a group, and group administrator account, is created for each shipping hub, and one for the corporate office. Each shipping hub group is created using the IP range that is assigned to that particular location.

Corporate Office

Since the corporate office has its own designated authentication system, Joe opts to set the filtering levels at his office based on Windows NT login. He uses the Transparent Authentication function on the R3000 so that all of the users at the corporate office are assigned their filtering level based on the NT group that they are assigned to at the time of workstation login.

Los Angeles Shipping Hub

The HR department at the Los Angeles shipping hub has determined that all employees with access to a computer can surf the Internet, but are not allowed to access sites that would be classified as Pornography, Gambling, or Hate and Discrimination. The network administrator at the Los Angeles shipping hub, logs into the R3000 GUI using his group account. He then sets the filtering such that his entire location is blocked from access to sites from the categories that the HR department has deemed inappropriate.

Atlanta Shipping Hub

The HR department at the Atlanta shipping hub has determined that all employees will be restricted from using the Internet, all web-browsing activity should only take place on the company's internal web-server, or intra-net. The network administrator logs into the R3000 GUI using the group account provided. He creates a custom-filtering category that is populated with the IP addresses and/or URLs of the company's intra-net web servers. He then sets a filtering level that blocks access to the Internet, but opens access to the custom category that he has created. The result is that all web browsing access in the Atlanta shipping hub is restricted to the company intra-net.

New York Shipping Hub

The HR department at the New York shipping hub has determined that the filtering level will be different based on job title. For office workers, Internet access will be allowed, with the exception of Pornography, Gambling, and Hate and Discrimination. The shipping and receiving departments will be limited to accessing only the company intra-net. The network administrator at the New York shipping hub logs into the R3000 GUI using the provide group account. He creates two sub-groups. One sub-group is called Office and is designated as 10.13.10.0/24, and the other is called Shipping and is designated as 10.13.11.0/24. For the Office sub-group, he creates a filtering level that blocks access to the sites designated as restricted by the HR department. For the Shipping sub-group he creates a custom-filtering category that is populated with the IP addresses and/or URLs of the company's intra-net web servers. He then sets a filtering level which blocks access to the Internet, but opens access to the custom category that he has created.

Use Case Two – 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 Three – 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.

Use Case Four – State Government

Dave is the Chief Information Security Officer for a state network. He is responsible for enforcing the states Internet security requirements on all state government agencies. However, since there are so many divisions of the state government, he is also responsible for acquiring tools which will allow the different government agencies to enforce their own policies, while not effecting the Internet traffic of another agency. The State has no Acceptable Use Policy, however, many of the agencies do.

Dave has had several of the agencies contact him in regard to Internet Filtering. In the past, Dave has handled Internet filtering by placing the URLs of some of the known problem sites in the State's proxy/cache servers. However, this has proved ineffective, since the number of sites that need to be blocked is far more than the proxy/cache server can handle. Dave has attempted to use a software tie in product for his proxy/cache servers, but has found that he and his team were receiving a large number of help desk calls from the state agencies wanting to add or delete a site for filtering. The state agencies are also calling frequently to make changes to the filtering level for the agency. As well as complaining that the filtering level is not granular enough to allow for different filtering levels that are required within the agency. Dave has also found that the use of the filter has greatly increased the number of proxy/cache servers needed to handle his traffic load since filtering has been tied in with proxy/cache servers.

Dave makes the switch to the R3000. He configures the R3000 such that there is no MFL. He creates a group for each agency and creates group administration accounts for each group.

At each agency, the network administrator is able to login to the R3000 and change the filtering level for the agency, at any time, without impacting the filtering levels at the other agencies.

For example, at the Department of Motor Vehicles, the network administrator is able to set the filtering level to match the DMV Acceptable Use Policy.

The Department of Law Enforcement is able to set the filtering level for it's group. Additionally, since the Department of Law Enforcement is frequently doing investigations, they are able to remove a site from the filter list for their group. However, that site would remain blocked for all other agencies.

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.