To apply security in RHEL, there are four important approaches. First, you can use the application firewall [SELinux](http://searchenterpriselinux.techtarget.com/tip/When-to-use-SELinux-An-introduction-to-security-enhanced-Linux). Next, you have the [iptables firewall](http://searchenterpriselinux.techtarget.com/definition/iptables). Also, the [TCP Wrapper](http://searchcio-midmarket.techtarget.com/definition/TCP-Wrapper) can be used for specific services, and lastly many services have their own security features. Setting up a secure environment means that you carefully have to consider how you want to combine these different solutions.

**Using SELinux**Possibly the most striking security solution in RHEL, is SELinux. This security framework is enforced by the Linux kernel and makes sure that applications are limited in their possibilities. To do this, particular profiles are defined to specify what exactly an application can do, and what it cannot do. For example, if you want to allow an Apache Web server to read documents that are outside of the document root, you have to enable a Boolean setting. Apart from working with these Boolean settings, SELinux applies file system labels to make it clear which content is expected to be in each type of file system.

Working with SELinux makes your applications more secure, but it also means that it is a lot more work to set up an application properly. You'll notice that default settings will work in most cases, but if you want to go beyond the defaults, you need to modify SELinux settings and that can be difficult. Nevertheless, SELinux should always be enabled because it protects your applications from bugs that might give permissions to unauthorized users.

**Using iptables firewall**You can use iptables as the second line of defense. The command modifies the kernel-level firewall that exists in all Linux distributions. The purpose of using iptables, is to make sure that only those services are available that you really want to be available. After a default installation no services are reachable at all, only after you specifically allow a service will it be reachable. Not only does iptables allow you to limit access to specific services, you can also use it in combination with source addresses and destination addresses to allow particular networks access to services. In many enterprise networks it is not necessary as firewalls are implemented at the network periphery. If you have many servers to manage, it makes sense to have the router determine which ports are available for which networks and which ports are not.

**Using TCP Wrapper**TCP Wrapper is a rather old way to protect services and it's not available for all of the services on your RHEL server. Only those services that are programmed to use the [libwrap library](http://en.wikipedia.org/wiki/Libwrap), will also use TCP Wrapper. For those services, two configuration files can be used: /etc/hosts.allow and /etc/hosts.deny. In these configuration files, you can define which host can access which services. The limitation of using TCP wrappers is that it doesn't work for all services. Therefore, it's best to avoid it completely and regulate access to services via iptables.

**Service specific security**As the last part of the security settings, there's the service specific security. This is something that you should always apply. Using service specific security settings, you can fine-tune what exactly is offered by a specific service and which users are allowed access to those services. Also, the service specific security settings are a part of what is really needed to provide the service, so make sure you configure it.

But there is some overlap between what you can do with service specific security settings, and settings that are applied at a higher level. For example, you can tell your NFS server, your Samba server as well as your mail server that access from specific hosts has to be denied. You can also take care of such access regulations at the firewall level, or by using TCP Wrapper. So which one to choose?

The advantage of applying security settings at the service level, is that you can be very specific. Using Samba security for example, you can grant access for a specific host to one share, while denying it to another share. You can't use this kind of detailed security settings while working with iptables only. Also, when applying security at the service level, you can work with specific user accounts, which is not possible when using a solution like iptables.

**Setting up your RHEL security configuration**It's a good idea to start your RHEL security configuration while working with SELinux. In many cases you'll have to, because otherwise you risk that SELinux prevents you from performing some particular tasks. Once the service is opened using SELinux, you can go to the next level, which is the iptables firewall. But this level is optional, because you might already have a corporate policy that states that firewall issues should be handled at the routers. Better to avoid TCP wrappers. This type of security is not generic enough, because it works for some specific service only, while being ignored completely by others. Last and probably most important, you'll have to configure security settings at the individual services - and you need to do this correctly, or the services function properly.