Designing and implementing a firewall solution for an enterprise can be a daunting task. Choices made early in the design process can have far-reaching security implications for years to come. In this series of tips, we take a detailed look at the process used to implement a firewall and help guide you through the design process.

We've divided the process into four stages:

- How to choose a firewall
- Choosing the right firewall topology
- Placing systems in a firewall topology
- Auditing firewall activity
There are dozens of firewalls on the market today. Choosing one for your organization can be a daunting task – especially in an industry filled with buzzwords and proprietary trademarks. Let's take a look at the basics of firewall technology and five questions you should ask when choosing a firewall for your organization.

1. **Why are you implementing a firewall?** Sure, this sounds like a simple question. You're probably thinking to yourself, "Because we need one!" But it's important that you take the time to define the technical objectives that you have for implementing a firewall. These objectives will drive the selection process. You don't want to choose an expensive, feature-rich firewall that's complicated to administer when your technical requirements could be met by a simpler product.

2. **How will the firewall fit into your network topology?** Will this firewall sit at the perimeter of your corporate network and be directly connected to the Internet, or will it serve to segment a sensitive LAN from the remainder of the organization? How much traffic will it process? How many interfaces will it need to segment your traffic? Performance requirements such as these contribute a significant amount to the total cost of new firewall implementations, making it easy to under- or over-purchase.

3. **What type of traffic inspection do you need to perform?** This is where the buzzwords start to come into play. Every vendor out there has a different trademark for their traffic-inspection technology, but there are essentially three different options (listed in order of increasing complexity and cost):
   - **Packet-filtering** firewalls use simple rules to evaluate each packet they encounter on its own merits. They maintain no history from packet to packet, and they perform basic packet header inspection. The simplicity of this inspection makes them speed demons. They're the most inexpensive option, but they are also the least flexible and vulnerable. There's a good chance you already own equipment capable of performing packet filtering – your routers!
   - **Stateful-inspection** firewalls go a step further. They track the three-way TCP handshake to ensure that packets claiming to belong to an established session (i.e., the SYN flag is not set) correspond to previous activity seen by the firewall. Requests to open the initial connection are subject to the stateful-inspection firewall rulebase.
   - **Application-proxy** firewalls contain the highest level of intelligence. In addition to stateful inspection, they broker the connection between client and server. The client connects to the firewall, which analyzes the request (including application-layer inspection of packet contents). If the firewall rules indicate that the communication should be allowed, the firewall then establishes a connection with the server and continues to act as an intermediary in the communication. When combined with Network Address Translation, both hosts may not even be aware that the other exists – they both believe they are communicating directly with the firewall.

4. **Is your organization better suited for an appliance or a software solution?** Appliances are typically much easier to install. You normally just plug in the appropriate Ethernet cables, perform basic network configuration and you're ready to configure your firewall rules. Software firewalls, on the other hand, can be tricky to install and require tweaking. They also lack the security that's often built into the hardened operating systems of firewall appliances. What's the tradeoff? You guessed it! Appliances are more expensive.

5. **What operating system is best suited for your requirements?** Even appliances run an OS and, chances are, you'll need to work with it at some point in your firewall administration career. If you're a Linux jockey, you probably don't want to choose a Windows-based firewall. On the other hand, if you don't know/devhull from /var/log, you probably want to steer clear of Unix-based solutions.

While I can't recommend a specific firewall to you without knowing your needs, the process of answering these questions can help you solidify your thoughts and put you in the right direction. With these answers in hand, you should be able to intelligently evaluate the cost/benefit tradeoff for the various products available on the market today.
When developing a perimeter protection strategy for an organization, one of the most common questions is "Where should I place firewalls for maximum effectiveness?" In this tip, we'll take a look at the three basic options and analyze the scenarios best suited for each case.

Before we get started, please note that this tip deals with firewall placement only. Anyone building a perimeter protection strategy should plan to implement a defense-in-depth approach that utilizes multiple security devices including firewalls, border routers with packet filtering and intrusion-detection systems.

Option 1: Bastion host

The first and most basic option is the use of a bastion host. In this scenario (shown in figure 1 below), the firewall is placed between the Internet and the protected network. It filters all traffic entering or leaving the network.

![Figure 1: Bastion host](image)

The bastion host topology is well suited for relatively simple networks (e.g. those that don’t offer any public Internet services.) The key factor to keep in mind is that it offers only a single boundary. Once someone manages to penetrate that boundary, they’ve gained unrestricted (at least from a perimeter protection perspective) access to the protected network. This may be acceptable if you’re merely using the firewall to protect a corporate network that is used mainly for surfing the Internet, but is probably not sufficient if you host a Web site or e-mail server.

Option 2: Screened subnet

The second option, the use of a screened subnet, offers additional advantages over the bastion host approach. This architecture uses a single firewall with three network cards (commonly referred to as a triple homed firewall). An example of this topology is shown in figure 2 below.

![Figure 2: Screened subnet](image)

The screened subnet provides a solution that allows organizations to offer services securely to Internet users. Any servers that host public services are placed in the Demilitarized Zone (DMZ), which is separated from both the Internet and the trusted network by the firewall. Therefore, if a malicious user does manage to compromise the firewall, he or she does not have access to the Intranet (providing that the firewall is properly configured).

Option 3: Dual firewalls
The most secure (and most expensive) option is to implement a screened subnet using two firewalls. In this case, the DMZ is placed between the two firewalls, as shown in figure 3 below.

![Figure 3: Dual firewalls](image)

The use of two firewalls still allows the organization to offer services to Internet users through the use of a DMZ, but provides an added layer of protection. It's very common for security architects to implement this scheme using firewall technology from two different vendors. This provides an added level of security in the event a malicious individual discovers a software-specific exploitable vulnerability.

Higher-end firewalls allow for some variations on these themes as well. While basic firewall models often have a three-interface limit, higher-end firewalls allow a large number of physical and virtual interfaces. For example, the Sidewinder G2 firewall from Secure Computing allows up to 20 physical interfaces. Additional virtual interfaces may be added through the use of VLAN tagging on the physical interfaces. What does this mean to you? With a greater number of interfaces, you can implement many different security zones on your network. For example, you might have the following interface configuration:

- Zone 1: Internet
- Zone 2: Restricted workstations
- Zone 3: General workstations
- Zone 4: Public DMZ
- Zone 5: Internal DMZ
- Zone 6: Core servers

This type of architecture allows you to take any of the three topologies described above and add a tremendous degree of flexibility.

That's a brief primer on firewall architectures. Now that you're familiar with the basic concepts, you should be able to help select an appropriate architecture for use in various situations.
In the previous tip we explored the basics of choosing a firewall topology. We covered the differences between bastion hosts, screened subnets and combining multiple firewalls for maximum security. Once you have decided which topology best suits your IT infrastructure, you need to decide where to place individual systems within the chosen topology.

As we discuss this topic, we'll use the concept of security zones to further define our requirements. For our purposes, consider a security zone to be all of the systems connected to a single interface of a firewall – either directly or through network devices other than firewalls.

**Bastion host**

First, let's look at the simplest case: the bastion host. In this scenario, all traffic entering or leaving the network passes through the firewall and it has only two interfaces: a public interface directly connected to the Internet and a private interface connected to the intranet. This leaves us with two security zones, making it fairly easy to place systems. We simply put all systems that we would like protected in the private zone!

In the case of a bastion host topology, we're assuming that you are not planning to offer any public services to the Internet. If you do need to offer public services (such as DNS, SMTP or HTTP), you should seriously consider the use of an alternate topology. If that is not possible, you have a difficult decision to face: should you place your public servers in the public or private zone? If you place them in the public zone, they don't gain any protection from the firewall and are more vulnerable to attack. On the other hand, placing them in the private zone raises the possibility that other, more sensitive systems, may be compromised if the public server falls victim to an attack. You need to carefully weigh the risks and benefits when making this decision.

![Figure 1: Bastion host](image)

**Screened subnet**

The screened subnet scenario, the most commonly deployed firewall topology, is also somewhat straightforward. We add an additional zone – the screened subnet (or DMZ) – that contains all hosts offering public services. In this case, the public zone is directly connected to the Internet and contains no hosts controlled by the organization. The private zone contains systems that Internet users have no business accessing, such as user workstations, internal file servers and other nonpublic applications. The DMZ contains all systems that are intended to provide services to the Internet. This zone contains your public Web server, SMTP server, DNS servers and other similar systems. Your IMAP/POP server may or may not reside in this zone, depending upon your security policy.
Multi-homed firewall

The final scenario, a multi-homed firewall with more than three interfaces, poses the most interesting challenge. In this case, you have more than three zones, so you have the luxury of further subdividing systems. You'll need to make these subdivisions based upon the specific security objectives of your organization. One division you might want to make is to place workstations into different zones to provide isolation for sensitive systems. For example, you might place all systems belonging to the accounting into one zone, executive workstations in another zone and other workstations in yet a third zone. You also may wish to subdivide systems offering services to the Internet. For example, systems that provide services to the general public (such as a company Web site) may be placed in a different zone than systems that offer services only to authenticated users (such as a Web mail server).

In the end, the choices are yours to make. Now that you've read this tip, you should have plenty of ideas running through your mind. Sit down and commit them to paper, discuss the options with your colleagues and develop a system placement strategy suitable for your organization.
In the first three parts of this series, we explored choosing a firewall platform, choosing an appropriate topology, and placing systems within that topology.

Once you've made it through the challenging phases of firewall selection and architecture design, you're finished setting up a DMZ, right? Your rulebase should remain stable and you'll never have a need to make configuration changes. We can only dream! In the real world of firewall management, we're faced with balancing a continuous stream of change requests and vendor patches against the operational management of our firewalls. Configurations change quickly and often, making it difficult to keep on top of routine maintenance tasks. In this tip, we explore some ways to leverage the logging capabilities of your firewall to help keep things in order.

Let's take a look at four practical areas where some basic log analysis can provide valuable firewall management data:

1. **Monitor rule activity** System administrators tend to be quick on the trigger to ask for new rules, but not quite so eager to let you know when a rule is no longer necessary. Monitoring rule activity can provide some valuable insight to assist you with managing the rulebase. If a rule that was once heavily used suddenly goes quiet, you should investigate whether the rule is still needed. If it's no longer necessary, trim it from your rulebase. Legacy rules have a way of piling up and adding unnecessary complexity. Over the years, I've had a chance to analyze the rulebases of many production firewalls, and I estimate that at least 20% of the average firewall's rulebase is unnecessary. I've seen systems where this ratio is as high as 60%.

2. **Traffic flows** Also monitor logs for abnormal traffic patterns. If servers that normally receive a low volume of traffic are suddenly responsible for a significant portion of traffic passing through the firewall (either in total connections or bytes passed), then you have a situation worthy of further investigation. While "flash crowds" are to be expected in some situations (such as a Web server during a period of unusual interest), they are also often signs of misconfigured systems or attacks in progress.

3. **Rule violations** Looking at traffic denied by your firewall may lead to interesting findings. This is especially true for traffic that originates from inside your network. The most common cause of this activity is a misconfigured system or a user who isn't aware of traffic restrictions, but analysis of rule violations may also uncover attempts at passing malicious traffic through the device.

4. **Denied probes** If you've ever analyzed the log of a firewall that's connected to the Internet, you know that it's futile to investigate probes directed at your network from the Internet. They're far too frequent and often represent dead ends. However, you may not have considered analyzing logs for probes originating from inside the trusted network. These are extremely interesting, as they most likely represent either a compromised internal system seeking to scan Internet hosts or an internal user running a scanning tool – both scenarios that merit attention.

Your firewall audit logs are a veritable goldmine of network security intelligence. Use them to your advantage!

**ABOUT THE AUTHOR:**

Mike Chapple, CISSP is an IT Security Professional with the University of Notre Dame. He previously served as an information security researcher with the National Security Agency and the U.S. Air Force. Mike is a frequent contributor to SearchSecurity, a technical editor for Information Security magazine and the author of several information security titles including the CISSP Prep Guide and Information Security Illuminated.

**DISCLAIMER:** Our Tips Exchange is a forum for you to share technical advice and expertise with your peers and to learn from other enterprise IT professionals. TechTarget provides the infrastructure to facilitate this sharing of information. However, we cannot guarantee the accuracy or validity of the material submitted. You agree that your use of the Ask The Expert services and your reliance on any questions, answers, information or other materials received through this Web site is at your own risk.