

[» HP Home](#)[» Products & Services](#)[» Support & Drivers](#)[» Solutions](#)[» How to Buy](#)[» Contact HP](#)

Search:

Small & Medium Business

All of HP United States



Solutions - how-to guides

» Small & Medium Business

- » Products
- » Solutions
 - » How-to guides
- » Support & Drivers
 - » Network security policy
- » Services

Buying options

- » Shop online at HP
- » Other ways to buy
- » Business to business

Or call 800-888-0262

- » Special offers
- » News & Events
- » Request catalog & news

 [Printable version](#)



Overview

This How-To guide shows you how to define a network security policy and helps you understand how firewall hardware and software can turn your network security business rules into security reality:

- » **Understand it:** find out what a network security policy is and how it drives the security measures you implement.
- » **Plan it:** begin making decisions about how you want to manage internet access in your organization.
- » **Do it:** create your own security policy using one of several free templates and example policies available on the Web.
- » **Use it:** find out about what you need to do to configure your firewall hardware and software to implement your security policy.
- » **Buy it:** shop for the products that can help you implement your security policy.
- » Understand it

Network security policy

- » Overview
- » Understand it
- » Plan it
- » Do it
- » Use it
- » Buy it

Related links

- » Security solutions
- » Atalla security products

Related courses

The HP Learning Center offers a variety of courses related to networking and security. Visit it today and look for:

- Firewall basics
- Wireless networking solutions

[Privacy statement](#)

[Using this site means you accept its terms](#)

[Feedback to SMB webmaster](#)

© 2005 Hewlett-Packard Development Company, L.P.

[» HP Home](#)[» Products & Services](#)[» Support & Drivers](#)[» Solutions](#)[» How to Buy](#)[» Contact HP](#)

Search:

Small & Medium Business

All of HP United States



Solutions - how-to guides

» Small & Medium Business

- » Products
- » Solutions
 - » How-to guides
 - » Network security policy
- » Support & Drivers
- » Services

Buying options

- » Shop online at HP
- » Other ways to buy
- » Business to business

Or call 800-888-0262

- » Special offers
- » News & Events
- » Request catalog & news



Understand it

The network and data security measures you put in place for your business -- from a firewall to a data backup system -- are physical manifestations of business rules. You make business decisions about how important your computer network and the data it holds are to your business, and how you want to protect it. Security systems are the implementation of those business decisions.

Robust security systems don't begin with hardware and software, but instead begin with careful planning. If you don't know what you want your security systems to protect, or if you don't have an idea of how you want that protection to function, it will be difficult to configure those systems to actually protect your networks and your data.

A security policy is a general statement of the business rules that define the goals and purposes of security within an organization (even an organization of one or two people). Security policies are considered strategic documents, and they define the overall purpose and direction for security. When you start with a solid security policy, configuring your security systems -- or communicating with those who do -- is much simpler and more effective.

One of the most important elements of your overall company security policy is a network security policy that governs what communications you will allow between your internal network and the external Internet. While the Internet facilitates information exchange in what seems like more ways than you can count and is a fundamental component of the way many organizations do business today, it can also provide a direct route for those with less-than-good intentions to your computer networks and their data. The development of a thorough network security policy followed by a solid implementation of that policy can help you leverage the Internet as a communications medium while still protecting your valuable systems and data.

There are many moving parts in the security of your organization. In addition to thinking about how to keep your networks and data safe, you must consider the security of your offices, your staff's computer equipment while they travel, and much more. Although this How-To guide focuses specifically on security policies for protecting your networks and data with firewalls, keep in mind that a firewall security policy cannot exist in a vacuum. It must be accompanied by an overall organization-wide security policy that establishes goals for maintaining physical security, staff training and awareness, and system-specific security controls.

- » [Plan it](#)

 [Printable version](#)

Network security policy

- » [Overview](#)
- » [Understand it](#)
- » [Plan it](#)
- » [Do it](#)
- » [Use it](#)
- » [Buy it](#)

Related links

- » [Security solutions](#)
- » [Atalla security products](#)

Related courses

The HP Learning Center offers a variety of courses related to networking and security. Visit it today and look for:

- [Firewall basics](#)
- [Wireless networking solutions](#)

[Privacy statement](#)

[Using this site means you accept its terms](#)

[Feedback to SMB webmaster](#)

© 2005 Hewlett-Packard Development Company, L.P.

[» HP Home](#)[» Products & Services](#)[» Support & Drivers](#)[» Solutions](#)[» How to Buy](#)[» Contact HP](#)

Search:

Small & Medium Business

All of HP United States



Solutions - how-to guides

» Small & Medium Business

- » Products
- » Solutions
 - » How-to guides
- » Support & Drivers
 - » Network security policy
- » Services

Buying options

- » Shop online at HP
- » Other ways to buy
- » Business to business

Or call 800-888-0262

- » Special offers
- » News & Events
- » Request catalog & news



Plan it

As you begin to establish your network security policy, you need to address several issues that deal primarily with internal users' ability to access Internet-based resources and services. Many users automatically assume that if they have a computer connected to a network then they must also have Internet access. Unfortunately, the insecurities and threats of cyberspace have made unrestricted access to the Internet a thing of the past in most organizations.

Before you begin planning your network policy, take a hard look at what Internet resources company users need to do their jobs (such as access to e-mail or basic Web pages), as opposed to those resources they might like to have (such as access to streaming audio and video). Internet access is not an all-or-nothing entity; instead, it is comprised of innumerable individual information services. You are probably familiar with many of these services: Web, FTP, chat, messaging, newsgroups, e-mail, telnet, streaming audio, and video. Firewalls can be employed to individually grant or restrict traffic based on each of these services, and your network security policy should address usage of each service individually.

E-mail access

E-mail is the most widely used Internet information service. Unfortunately, it has also become the most popular delivery mechanism for viruses, Trojan horses, and other malicious code attacks. E-mail primarily consists of three protocols: SMTP, POP3, and IMAP. SMTP (Simple Mail Transfer Protocol) is the protocol used by clients to submit outbound messages to e-mail servers and by e-mail servers to move e-mail from server to server on its way to its destination (i.e. the recipients e-mail inbox). E-mail clients use POP3 (Post Office Protocol version 3) and IMAP (Internet Message Access Protocol) to retrieve e-mail from an inbox on an e-mail server. POP3 is the more widely used, but IMAP natively supports encryption.

You may want to write your network security policy so it requires the use of IMAP instead of POP3. You'll also need to specify that IMAP and SMTP should be allowed to pass through the firewall, although you may want to use content or source/destination filters to restrict abuses.

Another important aspect of e-mail you must consider is attachments. An attachment allows an e-mail message to deliver just about any object from the sender to the receiver. Unfortunately, an attachment can just as easily contain malicious code, such as a virus, as it can contain a harmless and useful document such as a sales presentation. As part of your security policy, you should require, at the least, virus scanning on all IMAP and SMTP traffic. You may also need to consider whether to allow attachments at all. If your network and your data are highly sensitive and valuable, stopping attachments at the border firewall may be a worthwhile safeguard against damage, theft, and infection.

Content filtering

Content filtering must be addressed in a network security policy. You must decide whether to allow all traffic through the firewall without restriction or to filter traffic based on a clearly defined set of acceptable use traffic and content rules. An acceptable use list tells users what they can and cannot do on the local network and on the Internet when using company equipment. To establish your acceptable use policy, create an exhaustive list of acceptable and unacceptable activities. Some items you might include are:

- No trafficking or trading in copy-protected files (such as audio and video).
- No pornography.
- No mailing distribution lists originating from the local network.
- NNTP newsgroups are restricted.

From this list, you can easily create firewall specific rules to control and manage inbound and outbound traffic. However, before you set up your content and traffic rules and configure your firewall appropriately, be sure you run the list of acceptable content by the people who it will most

Network security policy

- » Overview
- » Understand it
- » Plan it
- » Do it
- » Use it
- » Buy it

Related links

- » Security solutions
- » Atalla security products

Related courses

The HP Learning Center offers a variety of courses related to networking and security. Visit it today and look for:

- Firewall basics
- Wireless networking solutions

affect -- the organization's employees.

You may find that prohibiting certain kinds of content (like zip files or executables) may have a negative affect on the way some employees do their jobs. This doesn't mean you have to change your security rules -- you may be able to find other, more secure ways for employees to receive those files -- but gathering input from employees early in the process will save you time in the end.

VPN access

Virtual Private Networks (VPNs) are a means to establish a normal network connection between distant systems and allow remote users to connect to the office network without compromising network security. The remote user connects to the Internet via a local connection (modem dialup, cable, DSL, etc.) then establishes a VPN link with the network over the Internet.

If you have employees that need to work remotely -- either from home or while on the road -- then VPN is a necessary component of your network security system. As you begin to formulate a policy for VPN access, you'll need to define what VPN protocols are allowed and exactly who can use VPN connections.

A step in the right direction

While this list of Internet access issues to think about as you plan your security policy isn't exhaustive, it should give you a good idea of the areas you need to consider as you begin to plan your security policy. A thorough investigation of users' Internet access needs balanced with your data security needs will help your security policy begin to take shape.

» Do it

 [Printable version](#)

[Privacy statement](#)

[Using this site means you accept its terms](#)

[Feedback to SMB webmaster](#)

© 2005 Hewlett-Packard Development Company, L.P.

[» HP Home](#)[» Products & Services](#)[» Support & Drivers](#)[» Solutions](#)[» How to Buy](#)[» Contact HP](#)

Search:

Small & Medium Business

All of HP United States



Solutions - how-to guides

» Small & Medium Business

- » Products
- » Solutions
 - » How-to guides
 - » Network security policy
- » Support & Drivers
- » Services

Buying options

- » Shop online at HP
- » Other ways to buy
- » Business to business

Or call 800-888-0262

- » Special offers
- » News & Events
- » Request catalog & news



Do it

Once you have a good understanding of how your company users and systems need to integrate with resources and services on the Internet, you can start writing your network security policy. The best way to develop a policy is to work from a template or an example policy. Many organizations on the Internet specialize in policy development or overall security issues. The SANS Institute offers numerous templates and examples of security policies. The Internet DMZ Equipment Policy, the Router Security Policy, and the Server Security Policy are particularly useful and each is an excellent example of a security policy that can be used to define the goals, purpose, and mission of network security within an organization.

Tip: Even if you are just setting a security policy for your home office or a small business, it's a good idea to review these sample documents so you know what kind of issues you need to address. While you may not have formal processes and procedures in place, you should have a plan for how you want to regulate traffic using your firewall.

To build your own network security policy, start with one or more templates or example policies and customize them to fit your organization's security needs. Although each organization's policy is unique, most security policies address a handful of common elements, such as:

- **Purpose:** a clear statement of the reason(s) the security policy exists. For example: *This document discusses the security configuration baseline with which all firewalls deployed at XYZ Corp should comply.*
- **Scope:** identifies which sections, divisions, or departments of an organization are subject to the policy. The scope can also define or indicate those sections that are exempt from the policy. For example: *This document applies to all departments of XYZ Corp. The extranet department and the R&D department are exempt from this document if their department specific policy defines a contradictory requirement.*
- **Policy:** clearly defines exactly what requirements, conditions, configurations, and standards must be adhered to, followed, or implemented. Items in this section of the policy might include conditions under which VPN connections are enabled, what Internet services are allowed to cross through the firewall, and what content is filtered.
- **Responsibilities:** identifies the individual or group responsible for implementing the conditions of the policy.
- **Enforcement:** discusses the consequences of violating the policy.
- **Definitions:** defines terms and acronyms to ensure that everyone reading the policy will clearly understand exactly what is being discussed.
- **Revision History:** documents and dates all changes to the firewall policy after its initial creation and deployment. This essential part of any policy ensures that only the latest and most up-to-date version is actually used.

A security policy, even for a specific issue or area such as firewalls, can become a complex and detailed document. It is important to expend sufficient time and effort to properly research and develop any security policy. Statistics have shown that most security breaches occurred not due to deficiencies in hardware or software security controls but blatant oversights or errors in the guiding security policy documentation.

Remember that a security policy is a strategic document that helps you carefully define how you want to implement a particular element of security for your business, such as network security. After you develop the document, you can turn to hardware and software systems to implement the rules it defines.

» [Use it](#)

Network security policy

- » Overview
- » Understand it
- » Plan it
- » Do it
- » Use it
- » Buy it

Related links

- » Security solutions
- » Atalla security products

Related courses

The HP Learning Center offers a variety of courses related to networking and security. Visit it today and look for:

- Firewall basics
- Wireless networking solutions

[» HP Home](#)[» Products & Services](#)[» Support & Drivers](#)[» Solutions](#)[» How to Buy](#)[» Contact HP](#)

Search:

Small & Medium Business

All of HP United States



Solutions - how-to guides

» Small & Medium Business

- » Products
- » Solutions
 - » How-to guides
 - » Network security policy
- » Support & Drivers
- » Services

Buying options

- » Shop online at HP
- » Other ways to buy
- » Business to business

Or call 800-888-0262

- » Special offers
- » News & Events
- » Request catalog & news



Use it

A firewall sits between your company's private network and the more public Internet, and its primary job is to examine inbound traffic -- that is, traffic coming from the public side of the link destined for the private side of that link -- to make sure it's okay before permitting that traffic to pass through to the private side of the link.

Although every organization's firewall is configured to meet the organization's unique needs, there are two fundamental activities involved in setting up a secure firewall that reflects the business rules set down in a network security policy.

Acquire the right firewall hardware

There are two kinds of firewalls:

- **Software-only firewalls:** A firewall program that runs on some computer that's attached to the Internet.
- **Hardware firewalls:** A kind of device that is attached to the Internet on one side and to an internal, private network on the other side. In some cases, this device may include other functions besides that of a firewall, such as a cable modem or Digital Subscriber Link (DSL) interface, and more. Hardware firewalls typically include both hardware and software, but you manage the two together as a single unit.

While the hardware portion of hardware firewalls is optimized for firewall functionality, when you deploy a software firewall, it is up to you to create and secure a host computer system to support the firewall software. Without a solid and reliable host, your firewall will be worthless.

The computer you install your firewall on must meet the minimum system requirements for whatever firewall software you choose to employ. Whenever possible, you should install as much high-speed high-capacity hardware on a host system as your budget can afford. Software firewalls require a significant level of computing power and it's better to build in more than you need so you don't restrict yourself with an under-performing communications bottleneck that hinders productivity.

Configure your firewall filters to reflect your security policy

When traffic passes through a firewall:

- The firewall inspects that traffic and looks into the various packets (i.e. small, manageable chunks) of information that make up Internet traffic.
- As it looks at packet content, it compares what it finds to existing filters or rules you define as part of your firewall setup.
- It applies any filters or rules you've configured in your firewall to decide if it should allow content to pass through or not.

A filter defines some specific pattern for which a firewall seeks a match. An exclusionary filter is one that results in traffic being blocked if a match occurs; an inclusionary filter is one that results in traffic being allowed if a match occurs.

Largely, filters and rules are two different ways of stating the same kind of information. A filter might take this form:

```
Block port 80
```

In English, this filter will block all packets destined for port 80 (the port requests for Web pages almost always comes through). If this filter were set up on your firewall, the firewall would reject any requests from users outside your system for Web pages inside your system. An equivalent

Network security policy

- » Overview
- » Understand it
- » Plan it
- » Do it
- » Use it
- » Buy it

Related links

- » Security solutions
- » Atalla security products

Related courses

The HP Learning Center offers a variety of courses related to networking and security. Visit it today and look for:

- Firewall basics
- Wireless networking solutions

rule to block port 80 might be stated as:

```
If port=80 then deny
```

The difference is a filter specifies an action for some specific value (like all traffic coming in on port 80), while rules usually apply a conditional statement that takes the form "if pattern match x, then take action y."

For many firewalls, filters or rules are set up to work together to define a general rule that established a basic filtering level, then setting exceptions to that rule to handle special cases. In this example, the first filter explicitly blocks all incoming traffic port addresses by default, then goes on only to allow use of well-known ports for FTP, SMTP, and Web services, plus the range of addresses reserved for temporary port use:

```
Block port all  
Allow port 21, 22, 25, 80, 49,152-65,535
```

By contrast, this filter configuration allows all traffic through by default, and blocks only Telnet and NetBIOS-related services:

```
Allow port all  
Deny port 23, 135-139
```

In reality, this second set of filters not a very effective security barrier since many other kinds of well-known attacks might be allowed through.

Rules and filters don't just apply to ports as in the previous examples, but can apply to a variety of different criteria that a firewall can learn about incoming traffic based on the packets of information that pass through it. For example, you could create a set of filters that allow employees to access local or Internet Web servers but that prevent users from outside the company from accessing a Web server on the company's side of the firewall.

Regardless of the size of your organization or the level of security you want to impose on your systems, firewalls are designed specifically to help you put your security policy into action. Home and small business firewalls usually have interfaces that make it very easy to configure your firewall rules and filters without much knowledge of ports, services, protocols, and the like. However, it's best if you have an IT professional configure an enterprise-level firewall, as firewalls at this level have more options and require more networking knowledge to secure your network properly.

When you start with a solid security policy that carefully balances employee needs for Internet connectivity with your organization's need for network security, you can easily find the right combination of hardware, software, and IT resources to implement that policy. Always remember that firewall configurations stem directly from business rules.

» [Buy it](#)

 [Printable version](#)

[Privacy statement](#)

[Using this site means you accept its terms](#)

[Feedback to SMB webmaster](#)

© 2005 Hewlett-Packard Development Company, L.P.

>> HP Home

>> Products & Services

>> Support & Drivers

>> Solutions

>> How to Buy

>> Contact HP

Search:

Small & Medium Business

All of HP United States



Solutions - how-to guides

HP recommends Microsoft® Windows® XP Professional

>> Small & Medium Business

- >> Products
- >> Solutions
 - > How-to guides
 - Network security policy
- >> Support & Drivers
- >> Services

Buying options

- >> Shop online at HP
- >> Other ways to buy
- >> Business to business

Or call 800-888-0262

- >> Special offers
- >> News & Events
- >> Request catalog & news



Buy it

>> HP Business Desktop PCs



With an Intel® Pentium® 4 processor and powerful processing capabilities, HP's business desktop PCs are the ideal PCs for power users who want to protect their home network with a firewall.

Buy Online >>

or call 800-888-0262

- >> Promotions & offers
- >> Other ways to buy

>> ProLiant servers



- Easy, powerful, and flexible
- Choose blades, density optimized, I/O flexibility, and more to meet your needs
- Add a ProLiant essentials value pack of optional software that lowers server lifecycle cost of ownership
- Available for all major OSs

Buy Online >>

or call 800-888-0262

- >> Promotions & offers
- >> Other ways to buy

>> HP Storage solutions



Even with a robust firewall solution in place, no business should be without a data recovery device. To make sure you never lose data, browse HP and Compaq's selection of cost-effective, automated storage systems.

Buy Online >>

or call 800-888-0262

- >> Promotions & offers
- >> Other ways to buy

>> Return to network security overview

Network security policy

- >> Overview
- >> Understand it
- >> Plan it
- >> Do it
- >> Use it
- >> Buy it

Related links

- >> Security solutions
- >> Atalla security products

Related courses

The HP Learning Center offers a variety of courses related to networking and security. Visit it today and look for:

- Firewall basics
- Wireless networking solutions

[Printable version](#)

[Privacy statement](#)

[Using this site means you accept its terms](#)

[Feedback to SMB webmaster](#)

© 2005 Hewlett-Packard Development Company, L.P.