On this page

Protected Network

In subject area: Computer Science

A 'Protected Network' is a secure network environment that safeguards information from unauthorized access or attacks, especially in the context of increasing commercial interest and threats in the digital landscape.

AI generated definition based on:
Firewall Policies and VPN Configurations, 2006

On this page

Chapters and Articles

You might find these chapters and articles relevant to this topic.

Network Security Policy

In Firewall Policies and VPN Configurations, 2006

Untrusted Networks

The federation of networks that became the Internet consisted of a relatively small community of users by the 1980s, primarily in the research and academic communities. Because it was rather difficult to get access to these systems and the user communities were rather closely knit, security was not much of a concern. The main objective of connecting these various networks together was to share information, not keep it locked away. Technologies such as the UNIX operating system and the TCP/IP networking protocols that were designed for this environment reflected this lack of security concern; security was simply viewed as unnecessary.

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 1 of 24

on security, often in opposition to those of academia. Commercial information had value, and access to it had to be limited to specifically authorized people. UNIX, TCP/IP, and connections to the Internet became avenues of attack and did not have much capability to implement and enforce confidentiality, integrity, and availability. As the Internet grew in commercial importance, with numerous companies connecting to it and even building entire business models around it, the need for increased security became acute. Connected organizations now faced threats they never had to consider before.

When the corporate computing environment was a closed and limited-access system, threats mostly came from inside the organizations. These *internal threats* came from disgruntled employees with privileged access who could cause a lot of damage. Attacks from the outside were not much of an issue since there were typically only a few, if any, private connections to trusted entities. Potential attackers were few in number, since the combination of necessary skills and malicious intent were not widespread.

With the growth of the Internet, *external threats* grew as well. There are now millions of hosts on the Internet as potential attack targets, which entice the now large numbers of attackers. This group has grown in size and skill over the years as its members share information on how to break into systems for both fun and profit. Geography no longer serves as an obstacle, either. You can be attacked from another continent thousands of miles away just as easily as from your own town.

Threats can be classified as structured or unstructured. *Unstructured threats* are from people with low skill and perseverance. These usually come from people called *script kiddies*—attackers who have little to no programming skill and very little system knowledge. Script kiddies tend to conduct attacks just for bragging rights among their groups, which are often linked only by an Internet Relay Chat (IRC) channel. They obtain attack tools that have been built by others with more skill, and use them, often indiscriminately, to attempt to exploit vulnerability in their target. If their attack fails, they will likely go elsewhere and keep trying. Additional risk comes from the fact that they often use these tools with little to no knowledge of the target environment, so attacks can wind up causing unintended results. Unstructured

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 2 of 24

detectable with current security tools.

Structured attacks are more worrisome because they are conducted by hackers with significant skill. If the existing tools do not work for them, they are likely to modify them or write their own. They are able to discover new vulnerabilities in systems by executing complex actions the system designers did not protect against. Structured attackers often use so-called *zero-day exploits,* which target vulnerabilities the system vendor has not yet issued a patch for or does not know about. Structured attacks often have stronger motivations behind them than simple mischief. These can include theft of source code, theft of credit card numbers for resale or fraud, retribution, or destruction or disruption of a competitor. A structured attack might not be blocked by traditional methods such as firewall rules or detected by an IDS. It could even use noncomputer methods such as social engineering.

Note

Social engineering, also known as *people hacking,* is a means of obtaining security information from people by tricking them. The classic example is calling up a user and pretending to be a system administrator. The hacker asks the user for his or her password to ostensibly perform some important maintenance task. To avoid being hacked via social engineering, educate your user community that they should always confirm the identity of any person calling them and that passwords should never be given to *anyone* via e-mail, instant messaging, or the phone. To guard against social engineering and similar security hazards, user education should be an integral part of any network security policy.

Another key task in securing your systems is closing vulnerabilities by turning off unneeded services and bringing them up to date on patches. Services that have no defined business need present an additional possible avenue of attack and are just another component that needs patch attention. Keeping patches current is one of the most important activities you can perform to protect yourself, yet one that many organizations neglect.

The Code Red and Nimda worms of 2001 were successful primarily because so many systems had not been patched for the

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 3 of 24

vulnerabilities. Patching, especially when you have hundreds or even thousands of systems, can be a monumental task. However, by defining and documenting processes, using tools to assist in configuration management, subscribing to multiple vulnerability alert mailing lists, and prioritizing patches according to criticality, you can get a better handle on the job.

One useful document to assist in this process has been published by the U.S. National Institute of Standards and Technology (NIST), which can be found at http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf (800-40 is the document number).

Also important is having a complete understanding of your network topology and some of the key information flows within it, and in and out of it. This understanding helps you define different zones of trust and highlights where re-architecting the network in places might improve security—for example, by deploying additional firewalls internally or on your network perimeter.

Identifying Potential Threats

As you prepare your overall security plan and de-militarized zone (DMZ), it is important to identify and evaluate the potential risks and threats to your network, systems, and data. You must evaluate your risks thoroughly during the identification process to assign some sort of value to the risks to determine priorities for protection and likelihood of loss resulting from those risks and threats if they materialize. You should be looking at and establishing a risk evaluation for anything that could potentially disrupt, slow, or damage your systems, data, or credibility. In this area, it is important to assign these values to potential threats such as:

- Outside hacker attacks
- Trojans, worms, and virus attacks
- DoS or Distributed Denial of Service (DDoS) attacks
- Compromise or loss of internal confidential information
- Network monitoring and data interception
- Internal attacks by employees
- Hardware failures
-

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 4 of 24

policies, and implementation of your security environment. You should realize that this is an ongoing evaluation that is subject to change as conditions within your company and partners, and employee need for access, change and morph over time. Security is a process and is never truly “finished.” However, a good basic evaluation goes a long way toward creating the most secure system we can achieve.

Using VPNs in Today’s Enterprise

Ensuring that your data arrives safe and sound when it passes through a network is something everyone wants to have. In an ideal world, your data’s integrity and confidentiality would be guaranteed. If this sounds like a fantasy, you are wrong. These types of guarantees can be made when you use IPSec VPN technologies. When you use an IPSec connection between two networks or a client and a network, you can ensure that no one looked at the data and no one modified it. Almost every company today uses VPN technologies to secure its data as it passes through various networks. In fact, many regulations specify that a VPN connection must be used to pass specific types of data.

IPSec provides integrity checking to ensure your data was not modified. It also provides encryption, ensuring no one has looked at the data. When two sides create a VPN connection, each side is authenticated to verify that each party is who they say they are. Combined with integrity checking and encryption, you have an almost unbeatable combination.

The Battle for the Secure Enterprise

This book covers the NetScreen firewall product line and focuses on that specific product and technology. A firewall is the core of securing your network, but other products should also be implemented in your network. These additional devices help ensure a network that has security covered from all angles. The following technologies are usually the minimum that companies should implement to provide security in the organization.

A *firewall* can contain many different types of technology to increase its importance in your network. Many firewall products today can integrate several different technologies, and almost all provide VPN services. This allows secure streams of data to terminate to your firewall. This is usually over the Internet, but also over other unprotected networks. When the traffic gets to your secured network it no longer requires encryption. You can

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 5 of 24

to systems until the user authenticates. When doing this, clients cannot see the resource *until authentication has occurred.*

URL filtering is another requirement in many organizations, and provides a way to accept or reject access to specific Web sites. This allows companies to reduce liability by users accessing inappropriate Web content. Many firewalls can integrate with this type of scanning when used with another product.

Anti-virus is a requirement for any organization today. With more viruses being written, the last thing you want in your network is a virus outbreak. The Windows operating system is built to provide so many different functions that there are many ways it can be exploited. In recent months, Microsoft has done a great job of coming out with security patches when or before an exploit is discovered. Typically, though, when vulnerability is discovered an anti-virus company has a way to stop it much faster than Microsoft. An outbreak on your network can mean disaster, data loss, or loss of your job. Data is a company's most valuable asset today, and loss of that data or access to it can cost companies millions of dollars or more per day. Firewalls can be used to perform virus scanning. These devices are usually deployed in a central area on the network. A tiered anti-virus solution is a requirement for any organization.

You should have anti-virus scanning on all your desktops and servers to stop infections at the source. This will help prevent most virus outbreaks. In addition, you should have anti-virus scanning on your Simple Mail Transfer Protocol (SMTP) mail forwarder and should be resident directly on your mail server. Your chances for a virus outbreak should be small as long as you keep all of those devices up to date with the appropriate virus definitions. New technologies such as inline virus scanning in firewalls and other network appliances can provide extra protection from viruses.

Patch management has become a Herculean effort with all of the software an organization needs to run today. Patching operating systems and applications as soon as a vulnerability occurs is a must. With limited staff and increased software deployed, this task is almost impossible to accomplish. However, by providing an anti-virus system, you can provide a first level of defense against the spreading of malicious software or malware.

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 6 of 24

and password. Using static usernames and passwords is not enough anymore. Even 15 to 30 days may be too long to keep the same password. Two-factor authentication, digital certificates, and personal entropy are leading the march to provide a stronger nonstatic type of authentication that is hard to break.

Your network has millions of packets traversing it every day. Do you know what they are all doing? This is where an intrusion detection or intrusion detection and prevention device comes into play. These devices detect application- and network-based attacks. Intrusion detection devices sit on your network and watch traffic. They provide alerts for unusual traffic, and TCP resets to close TCP sessions. The newer technology of intrusion detection and prevention provides the ability to stop malicious traffic altogether and alert on it. However, heavy tuning of the products is required to make them effective.

Access into your network should be encrypted whenever possible. This ensures that parties not authorized to see your data do not get access to it by any means. IPSec VPN clients are one of the most popular ways to do this. This type of client provides strong encryption of your data and access to your internal resources without having them publicly accessible. A new trend in VPN solutions is the Secure Sockets Layer (SSL) VPN. These products allow you to put more behind them and do not require predeployment of a VPN client.

External Communications (also see “Remote Access”)

- **Modems are not disconnected** The problem with unsecured modems is that they can be attacked by wardialers who simply look for modems connected to corporate networks. These can create significant security holes and are often overlooked in our quest to lock down the wired network.
- **An ISP connection exists without written approval** In most companies, this might be a difficult trick to achieve, but it certainly warrants examination to ensure the ISP connection(s) is managed by the IT department and not some errant user who managed to get the local ISP provider to run a cable into the office on a Saturday morning.
- **Communications devices are not password protected** This seems like a giant “Duh!” but you’d probably be surprised how often communication devices such as modems, routers,

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 7 of 24

came with the device out of the box.

- **No warning banner** Failure to display the required login banner prior to logon attempts will limit the site's capability to prosecute unauthorized access. It also presents the potential for criminal and civil liability for systems administrators and information systems managers. Not displaying the proper banner will also hamper the site's capability to monitor device usage. Displaying a banner warning users of the consequences of unauthorized access helps ward off the bad guys and draws a line in the legal sand that you might need later.

DMZ Concepts

The use of a DMZ and its overall design and implementation can be relatively simple or extremely complex, depending on the needs of the particular business or network system. The DMZ concept came into use as the need for separation of networks became more acute when we began to provide more access to services for individuals or partners outside the LAN infrastructure. One of the primary reasons why the DMZ has come into favor is the realization that a single type of protection is subject to failure. This failure can arise from configuration errors, planning errors, equipment failure, or deliberate action on the part of an internal employee or external attack force. The DMZ has proven more secure and offers multiple layers of protection for the security of the protected networks and machines. It is also very flexible, scalable, and relatively robust in its capability to provide the protection we need. DMZ design now includes the ability to use multiple products (both hardware- and software-based) on multiple platforms to achieve the level of protection necessary, and are often designed to provide failover capabilities as well.

When we are working with a DMZ, we must have a common ground from which to work. To facilitate understanding, we examine a number of conceptual paths for traffic flow in the following section. Before doing so, however, let's make sure we understand the basic configurations that can be used for firewall and DMZ location and how each can be visualized. In the following figures, we'll see and discuss these configurations. Please note that each of these configurations is useful on internal networks needing protection, and protecting your resources from networks such as the Internet. Our first configuration is shown in Figure 1.1.

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 8 of 24

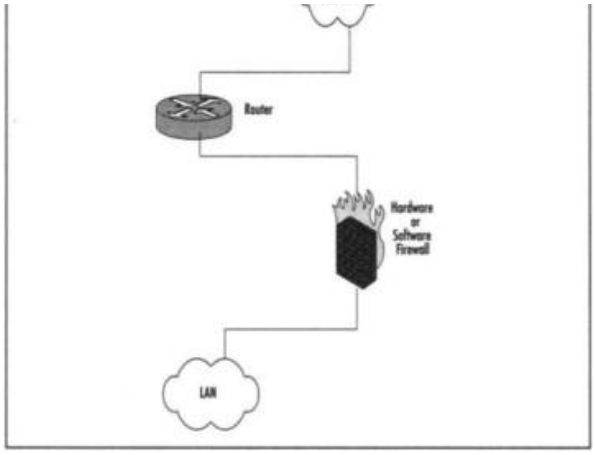


Figure 1.1. A Basic Network with a Single Firewall

Designing & Planning…

Know What You Want to Secure First

As you begin your DMZ design process, you must first be clear about what your design is intended for. A design that is only intended to superficially limit internal users' access to the Internet, for instance, requires much less planning and design work than a system protecting resources from multiple access points or providing multiple services to the public network or users from remote locations. An appropriate path to follow for your predesign path might look like this:

- Perform baseline security analysis of existing infrastructure, including OS and application analysis
- Perform baseline network mapping and performance monitoring
- Identify risk to resources and appropriate mitigation processes
- Identify potential security threats, both external and internal
- identify needed access points from external sources
- Public networks
- VPN access
- Extranets
- Remote access services
- Identify critical services
- Plan your DMZ

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 9 of 24

external services. This configuration would typically be used to begin to protect a small business or home network. It could also be used within an internal network to protect an inner network that had to be divided and isolated from the main network. This situation could include Payroll, Finance, or Development divisions that need to protect their information and keep it away from general network use and view.

Figure 1.2 details a protection design that would allow for the implementation and provision of services outside the protected network. In this design, it would be imperative that rules be enacted to not allow the untrusted host to access the internal network. Security of the bastion host machine would be accomplished on the machine itself, and only minimal and necessary services would be enabled or installed on that machine. In this design, we might be providing a Web presence that did not involve e-commerce or the necessity to dynamically update content. This design would not be used for provision of virtual private network (VPN) connections, FTP services, or other services that required other content updates to be performed regularly.

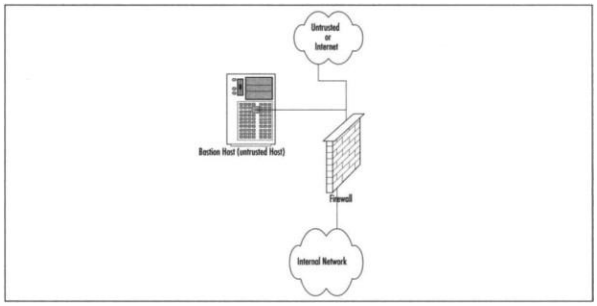


Figure 1.2. Basic Network, Single Firewall and Bastion Host (Untrusted Host)

Figure 1.3 shows a basic DMZ structure. In this design, the bastion host is partially protected by the firewall. Rather than the full exposure that would result to the bastion host in Figure 1.2, this setup would allow us to specify that the bastion host in Figure 1.2 could be allowed full outbound connection, but the firewall could be configured to allow only port 80 traffic inbound to the bastion host (assuming it was a Web server) or others as necessary for connection from outside. This design would allow connection from the internal network to the bastion host if necessary, and potentially allow updating of Web server content from the internal network if allowed by firewall rule, which could

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 10 of 24

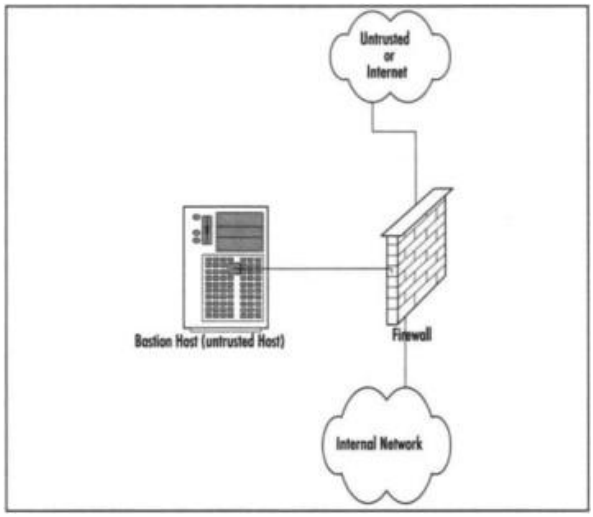


Figure 1.3. A Basic Firewall with a DMZ

Figure 1.4 shows a generic dual-firewall DMZ configuration. In this arrangement, the bastion host can be protected from the outside and allowed to connect to or from the internal network. In this arrangement, like the conditions in Figure 1.3, flow can be controlled to and from both of the networks away from the DMZ. This configuration and method is more likely to be used if more than one bastion host is needed for the operations or services being provided.

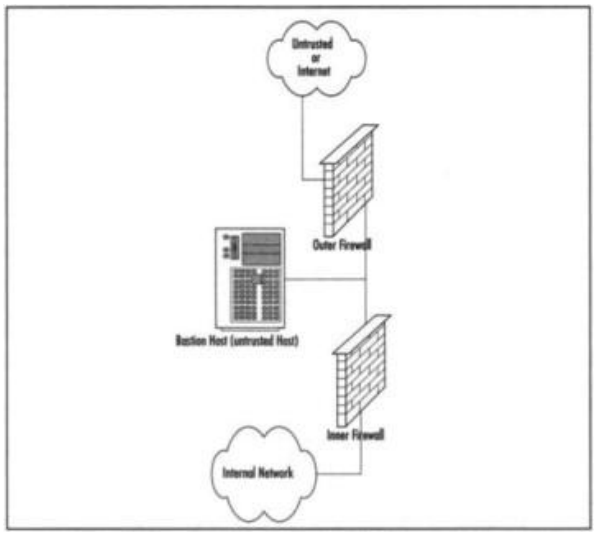


Figure 1.4. A Dual Firewall with a DMZ

Traffic Flow Concepts

Now that we've had a quick tour of some generic designs, let's look at the way network communications traffic typically flows through them. Be sure to note the differences between the levels and the flow of traffic and protections offered in each.

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 11 of 24

achieved through hardware or software and is the basis for familiar products such as Internet Connection Sharing (ICS) and the NAT functionality provided by digital subscriber line (DSL) and cable modems used for connection to the Internet. Note that flow is unrestricted outbound, but the basic configuration will drop all inbound connections that did not originate from the internal network.

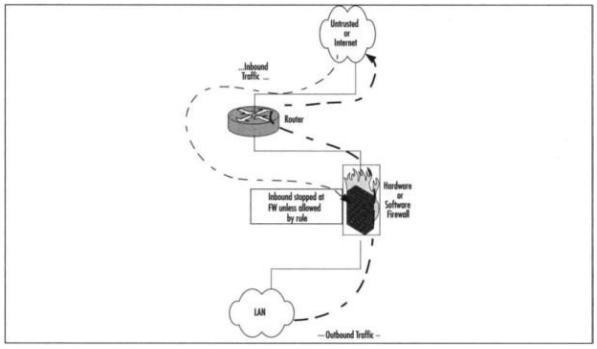


Figure 1.5. Basic Single-Firewall Flow

Figure 1.6 reviews the traffic flow in a network containing a bastion host and a single firewall. This network configuration does not produce a DMZ; the protection of the bastion host is configured individually on the host and requires extreme care in setup. Inbound traffic from the untrusted network or the bastion host is dropped at the firewall, providing protection to the internal network. Outbound traffic from the internal network is allowed.

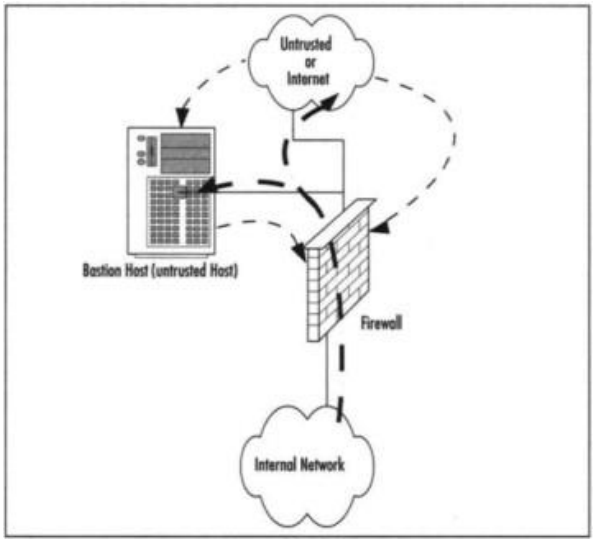


Figure 1.6. A Basic Firewall with Bastion Host Flow

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 12 of 24

host if allowed through the firewall and is dropped if destined for the internal network. Two-way traffic is permitted as specified between the internal network and the bastion host, and outbound traffic from the internal network flows through the firewall and out, generally without restriction.

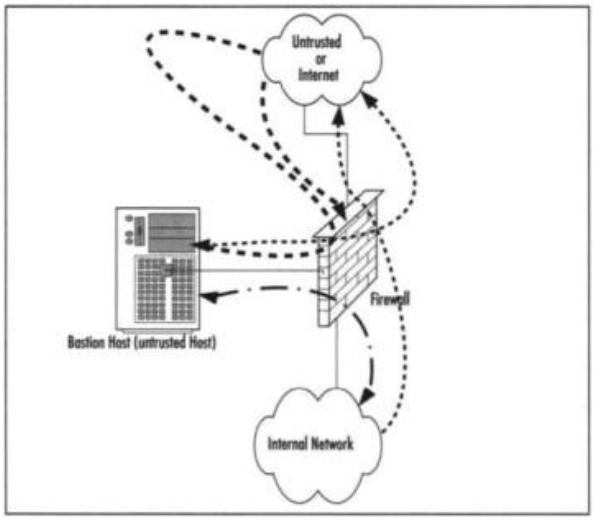


Figure 1.7. A Basic Single Firewall with DMZ Flow

Figure 1.8 contains a more complex path of flow for information, but provides the most capability in these basic designs to allow for configuration and provision of services to the outside. In this case, we have truly established a DMZ, separated and protected from both the internal and external networks. This type of configuration is used quite often when there is a need to provide more than one type of service to the public or outside world, such as e-mail, Web servers, DNS, and so forth. Traffic to the bastion host can be allowed or denied as necessary from both the external and internal networks, and incoming traffic to the internal network can be dropped at the external firewall. Outbound traffic from the internal network can be allowed or restricted to the bastion host (DMZ network) or the external network.

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 13 of 24

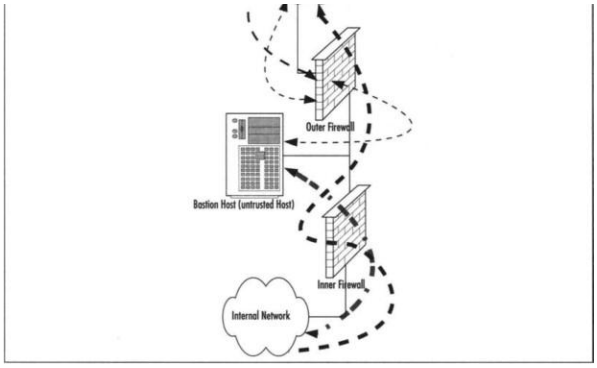


Figure 1.8. A Dual Firewall with DMZ Flow

As you can see, there is a great amount of flexibility in the design and function of your protection mechanisms. In the sections that follow, we expand further on conditions for the use of different configurations and on the planning to implement them.

Networks with and without DMZs

As we pursue our discussions about the creation of DMZ structures, it is appropriate to also look at the reasoning behind the various structures of the DMZ, and when and where we'd want to implement a DMZ or perhaps use some other alternative.

During our preview of the concepts of DMZs, we saw in Figures 1.5 to 1.8 some examples of potential design for network protection and access. Your design may incorporate any or all of these types of configuration, depending on your organization's needs. For instance, Figure 1.5 shows a configuration that may occur in the case of a home network installation or perhaps with a small business environment that is isolated from the Internet and does not share information or need to provide services or information to outside customers or partners. This design would be suitable under these conditions, provided configuration is correct and monitored for change.

Figure 1.6 illustrates a network design with a bastion host located outside the firewall. In this design, the bastion host must be stripped of all unnecessary functionality and services and protected locally with appropriate file permissions and access control mechanisms. This design would be used when an organization needs to provide minimal services to an external network, such as a Web server. Access to the internal network from the bastion host is generally not allowed, because this host is subject to compromise.

Figure 1.7 details the first of the actual DMZ designs and incorporates a screened subnet. In this type of design, the firewall

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 14 of 24

This design might be used when it is necessary to regularly update the content of a Web server, or provide a front end for mail services or other services that need contact from both the internal and external networks. Although better for security purposes than Figure 1.6, this design still produces an untrusted relationship in the bastion host in relation to the internal network.

Finally, Figure 1.8 provides a design that allows for the placement of many types of service in the DMZ. Traffic can be very finely controlled through access at the two firewalls, and services can be provided at multiple levels to both internal and external networks.

In the next section, we profile some of the advantages and disadvantages of the common approaches to DMZ architecture and provide a checklist of sorts to help you to make a decision about the appropriate use (or not) of the DMZ for protection.

Pros and Cons of DMZ Basic Designs

Table 1.6 details the advantages and disadvantages of the various types of basic design discussed in the preceding section.

Table 1.6. Pros and Cons of Basic DMZ Designs

Basic Design	Advantages	Disadvantages	Appropriate Use

Show less

View chapter

Explore book

Read full chapter

URL: https://www.sciencedirect.com/science/article/pii/B9781597490887500037

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 15 of 24

Edge/Fog Computing Paradigm: The Concept Platforms and Applications

M.P. Anuradha, K. Lino Fathima Chinna Rani, in
Advances in Computers, 2022

4.4.1 Network attack

While the network is the greatest protected port, it is only as good as the safety in place. Entirely unprotected nodes can no longer continue by hoping to remain under the radar. For e.g., Web tools can crawl the network by recognizing every vulnerable node. The vulnerabilities may persist due to bugs in the poor random number usage in crypto algorithms, unobserved malware and violent protocol attacks by determining professionals, and even by weaknesses in the protocols themselves. Even with a significantly protected network, an intruder might compromise a poorly fortified edge node by replicating a firmware update and substitute the genuine code with code written by the attacker.

View chapter

Explore book

Read full chapter

URL: https://www.sciencedirect.com/science/article/pii/S0065245822000407

Cisco Firewall/IDS IOS

In
Cisco Security Professional's Guide to Secure Intrusion Detection Systems
, 2003

Configuring Protected Networks

When a router sends an alarm, it will add an IN or OUT designator to the alarm if the victim's address is part of a configured, protected network. This flag will define an IP address as inside or outside the protected network. This means that if no protected network is configured at all, the router will consider all addresses as outside the protected network. Configuring a protected network will not have an impact on IDS performance or functionality as it only adds the flag discussed earlier.

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 16 of 24

shown next.

```
Router1(config)#ip audit po protected 172.16.20.1 to
172.16.20.254
```

To remove all protected IP addresses, you can use the following command in global configuration mode.

```
Router1(config)#no ip audit po protected
```

Configuring & Implementing....

Changes in IOS

IOS-IDS commands have been added and changed since IDS

View chapter

Explore book

Read full chapter

URL: https://www.sciencedirect.com/science/article/pii/B9781932266696500318

Network Access Protection

Tony Piltzecker, Brien Posey, in

The Best Damn Windows Server 2008 Book Period (Second Edition)

, 2008

Working with Network Access Protection

- The Network Access Protection (NAP) platform main objective is to validate the state of a client computer before connecting to a private network and offer a source of remediation.
- NAP clients include Windows Vista, Windows Server 2008 and Windows XP Service Pack 3.
- The NAP API will allow other ISVs to write software to be enforced by NAP.
- NAP provides the following areas of functionality: Health State Validation, Network Access Limitation, Automatic Remediation and Ongoing Compliance.
- DHCP NAP enforcement is the easiest enforcement implementation of NAP available.
- IPv6 is not supported with DHCP enforcement implementation.

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 17 of 24

Show more

View chapter

Explore book

Read full chapter

URL: https://www.sciencedirect.com/science/article/pii/B9781597492737000094

Targeting the Network

Thomas Wilhelm, in
Professional Penetration Testing (Second Edition), 2013

Wireless Network Protocols

If a corporation has a wireless network for its employees, from an external pentest perspective, infiltrating the network will give the professional penetration tester access to additional systems and network devices. Although plenty of news has been generated about the risk of including wireless access to corporate networks, using a wireless network is much cheaper than purchasing and installing wired network equipment.

Even though a wireless network is an inexpensive alternative to wired networks, lack of proper security measures can be costly to a company. If a malicious user was able to access the “protected” network, data loss and system compromises are sure to follow. From a professional penetration tester’s perspective, wireless networks are prime targets for attack because wireless networks are often less protected than wired networks. Even if a company does secure access points (such as placing firewalls and intrusion detection systems between the access point and the internal systems), employees are notorious for installing rogue access points in the network, circumventing all efforts by the network

Show more

View chapter

Explore book

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 18 of 24

Information Security Essentials for IT Managers

Albert Caballero, in
Computer and Information Security Handbook, 2009

Operation on Open Networks

Rules for operation on open networks are as follows:

- The mobile IT system must be operated in open network environments using a personal firewall.
- The configuration of the personal firewall must be in accordance with the corporate policy or, in the case of other personal firewall systems, must be subject to restrictive settings.
- A mobile IT system must be operated in an unprotected open network only for the duration of a secure access link to the organization's own network. The connection establishment for the secure access link must be performed as soon as possible, at least within five minutes.
- Simultaneous operation on open networks (protected or unprotected) and the organization's own networks is forbidden at all times.
- Remote access to company internal resources must always be

View chapter

Explore book

Read full chapter

URL: https://www.sciencedirect.com/science/article/pii/B9780123743541000145

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 19 of 24

Publishing Network Services with ISA 2004 Firewalls

Dr.Thomas W. Shinder, Debra Littlejohn Shinder, in Dr. Tom Shinder's Configuring ISA Server 2004, 2005

Provide Proxied Access to Web Sites Protected by the ISA firewall

Web Publishing Rules provide proxied access to Web sites located on an ISA firewall Protected Network. Any Network that is not part of the default External Network is considered an ISA firewall Protected Network. A proxied connection is more secure than a routed and NATed connection because the entire communication is deconstructed and reconstructed by the ISA firewall. This allows the ISA firewall to perform very deep application-layer inspection of Web requests made to published Web sites that have been published using Web Publishing Rules.

The ISA firewall's Web Proxy filter handles all incoming Web connections made through Web Publishing Rules. Even when you unbind the Web Proxy filter from the HTTP protocol definition, the Web Proxy filter is always enabled for Web Publishing Rules

View chapter

Explore book

Read full chapter

URL: https://www.sciencedirect.com/science/article/pii/B9781931836197500150

Defining a Firewall

In Firewall Policies and VPN Configurations, 2006

Physical Security

One of the most important and overlooked aspects of a comprehensive network security plan is physical access control. This matter is usually left up to facilities managers and plant security departments, or outsourced to security guard companies. Some network administrators concern themselves with sophisticated software and hardware solutions to prevent intruders from accessing internal computers remotely, while at the same time not protecting the servers, routers, cable, and other physical components from direct access. To many “security-

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 20 of 24

computer espionage experts to pose as members of cleaning crews to gain physical access to machines that hold sensitive data. This is a favorite ploy for several reasons:

- Cleaning services are often contracted out and their workers are often transient, so your company's employees might not know who is a legitimate member of the cleaning company staff.

Show more

View chapter

Explore book

Read full chapter

URL: https://www.sciencedirect.com/science/article/pii/B9781597490887500050

Firewalls

Kaushal Chari, in Encyclopedia of Information Systems, 2003

Glossary

bastion host
Computers that run proxy software to screen inbound or outbound messages of a protected network.

circuit-level proxy
Computer programs that provide security services by screening application layer messages without interpreting application layer protocols.

dual-homed host
A special type of bastion host that has two network interfaces for connection to two different networks.

firewalls
System consisting of hardware and/or software components that enforce various access control policies and collectively shield organizations from multiple types of security attacks.

The network layer protocol of the Internet that is responsible for routing packets from source to destination hosts.

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 21 of 24

network address translation (NAT)
System that shields IP addresses within protected network from being exposed to an external network. This provides security as well as the use of fewer valid IP addresses within an organization.

Communication devices called routers that use screening rules to filter packets in addition to performing their basic function of routing. They operate at the network and transport layers of the OSI model.

proxy gateways
Computer programs that provide security services by screening application layer messages. An *application-specific proxy gateway* uses logic specific to a particular application layer protocol to provide proxy services for that protocol. A *generic proxy gateway* supports proxy services for multiple application layer protocols. In practice, generic proxies are referred to as circuit-level proxies.

Screening of packets based on state information

View chapter

Explore book

Read full chapter

URL: https://www.sciencedirect.com/science/article/pii/B0122272404000708

Information Security Essentials for Information Technology Managers

Albert Caballero, in
Computer and Information Security Handbook (Third Edition)
, 2017

8 Wireless and Mobile Security

Wireless networking enables devices with wireless capabilities to use information resources without being physically connected to a network. A wireless local area network (WLAN) is a group of wireless networking nodes within a limited geographic area that is capable of radio communications. WLANs are typically used by devices within a fairly limited range, such as an office building or building campus, and are usually implemented as extensions to existing wired local area networks to provide enhanced user

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 22 of 24

of the most active standards organizations that address wireless networking is the Institute of Electrical and Electronics Engineers (IEEE). Like other wireless technologies, WLANs typically need to support several security objectives. This is accomplished through a combination of security features built into the wireless

Show more

View chapter

Explore book

Read full chapter

URL: https://www.sciencedirect.com/science/article/pii/B9780128038437000247

Related terms:

Authentication, Internet Protocol, Malware, Virtual Private Networks, Operating Systems, Intrusion Detection System, Transmission Control Protocol, Internal Network, Server Publishing Rule, Web Publishing Rule.

Recommended publications



Computer Networks

Journal



Network Security

Journal

All content on this site: Copyright © 2025 Elsevier B.V., its licensors, and contributors. All rights are reserved, including those for text and data mining, AI training, and similar technologies. For all open access content, the Creative Commons licensing terms apply.

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 23 of 24



Book • 2004



Future Generation Computer Systems

Journal

INFOEXPRESS, INC. - EX2502
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 24 of 24