What is Stateful Packet Inspection?

**Stateful packet inspection** is also known as the **dynamic packet filtering** and it aims to provide an **additional layer of network security**. Keep reading to learn more!

In business environments, we use **network technologies** very often. They allow us to share resources and files, set **communication protocols** and such. As much as they streamline and accelerate our business processes, they can also pose a serious **vulnerability for our cyber security**. An intruder or a hacker can infiltrate into our networks, steal our valuable information or lock us out of our systems. That is why **network security** is one of the most important practices in **cybersecurity**.

Most organizations rely on firewalls for their **network security needs**. A firewall can be defined as a **network security system** that allows the cybersecurity professionals to monitor and control the **network traffic**. In other words, a**firewall** sets the boundary between the internal and external network. There are two main**types of firewalls**:

* **Network-based firewalls:** They are often positioned on the LANs, intranets or WANs of the gateway computers.
* **Host-based firewalls:** They are implemented on the network host itself in order to protect the entire network traffic. **Host-based firewalls** can be a part of the operating system or an agent application in order to offer an **additional layer of security**.

**What is stateful inspection?**

The term **stateful inspection** (also known as the dynamic packet filtering) refers to a**distinguished firewall technology**. It aims to monitor the active connections on a network. Moreover, the process of stateful inspection determines which network packets should be allowed through the firewall by utilizing the information regarding active connections.

Stateful inspection keeps track of each connection and constantly checks if they are valid. That is why it offers a better protection than its predecessors.

In a firewall where the stateful inspection is implemented, the network administrator can **customise the parameters** in order to meet the unique needs of the organization.

**What is the benefit of implementing stateful inspection?**

Before stateful inspection has become mainstream, similar technology called **static packet filtering** was in use. This older alternative only checks the headers of the packets in order to determine whether they should be allowed through the firewall. As a result, a hacker can simply indicate “reply” in the header in order to**extract information from the network**. On the contrary, stateful inspection aims to carry out a more sophisticated investigation. That is why it analyses the application layer of the packets. A dynamic packet filter like stateful inspection can offer a **better security posture** for networks through recording the session information like port numbers or IP addresses.

In other words, stateful inspection is better at keeping the intruders away from your network since it uses a more refined technology.

If you would like to learn more about what you can do to **keep your organization safe**, you can contact us or take a closer look at our**SIEM** and **SOAR** products and check our [SOAR use cases](https://www.logsign.com/security-orchestration-use-cases).

<https://searchnetworking.techtarget.com/definition/stateful-inspection>

<https://en.wikipedia.org/wiki/Stateful_firewall>

<https://en.wikipedia.org/wiki/Firewall_(computing)>

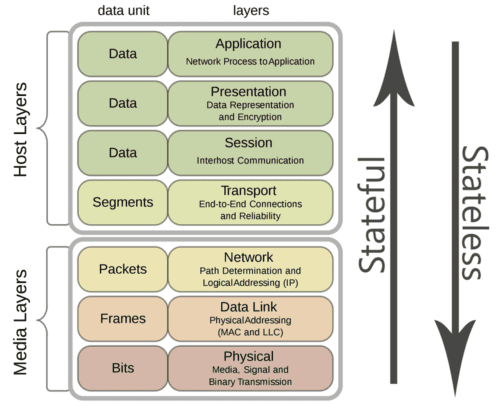
<https://www.sciencedirect.com/topics/computer-science/stateful-inspection>

<https://www.webopedia.com/TERM/S/stateful_inspection.html>

Today we live in the age of impending danger for every device capable of interfacing with the internet. Ingenuitive malware, determined hackers and the ever-increasing attack surfaces present, not just in computers/phones, but the innumerable  “smart” devices (IOT) has become a modern-day concern that has to be dealt with by the vast majority of individuals and industries. One of the most effective ways to deal with unknown cyber security threats is through the use of dedicated firewalls, designed to protect any & all devices on sensitive internal networks from external attackers or wrongdoers. However, truly effective firewalls need to consistently evolve and face new threats to businesses, organizations, processes and private individuals.

This is made increasingly difficult by the fact that these targets often possess little time, let alone the experience/resources necessary to implement & maintain a robust firewall security solution that best suits their requirements. Knowingly or unknowingly, everyone today has a device in their network that serves as a firewall between their devices and the internet, often provided by their Internet Service Provider (ISP). However rudimentary the implementation is, these firewalls still serve as an effective barrier to simple and constant attacks perpetrated by bots and motivated hackers. In this article we will take a look at the different implementations of firewalls, their effectiveness and use-cases in modern networks.

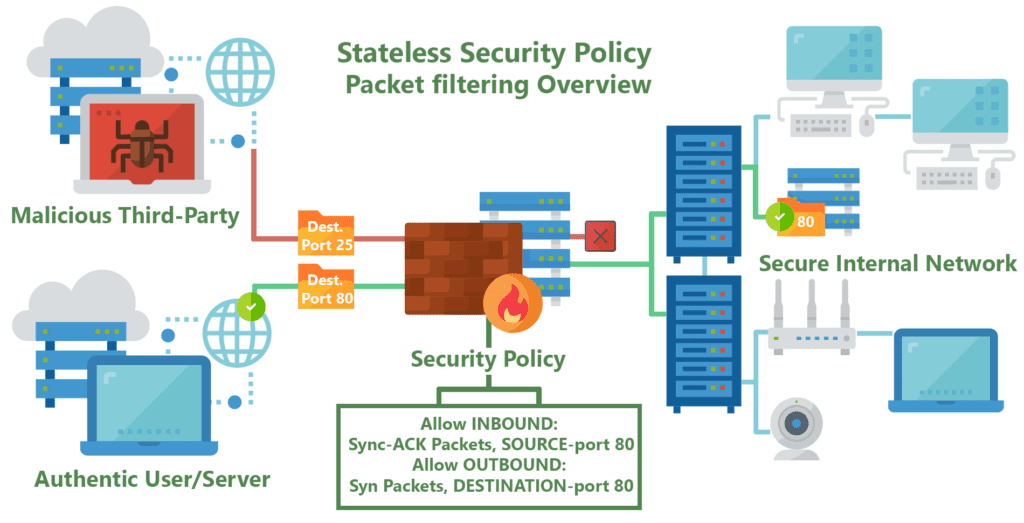
**Stateful Vs Stateless – What’s the difference?**

[](https://www.lanner-america.com/wp-content/uploads/stateful-vs-stateless.png)Inclination of Stateless vs Stateful firewalls in the[7 layers of the OSI model](https://www.lanner-america.com/knowledgebase/networking-basics/#tcpip).

Stateless and stateful firewalls may sound pretty similar with being denoted with a single distinction, but they are in fact two very different approaches with diverging functions and capabilities. Packet filtering potential, is one of principle ways in which stateless and stateful firewalls differ from each other. While both firewall implementations perform packet filtering, the differences between them is in the methodology, depth and lengths they go to performing this function.

With these details in mind, well define the main distinctions between the two as this will help categorize and explain these implementations and the differences that exist between stateless and stateful firewalls. The main focus will be on how they compare to each other in terms of packet filtering performance, levels of security features offered and latent hardware requirements to run these functions. Let’s start off by understanding what both stateless and stateful firewalls are, what they are meant to do, and finally how [stateless/stateful firewalls implemented as a solution](https://www.lanner-america.com/blog/managed-detection-response-boosting-cyber-security-smaller-businesses/) compare in the real world.

**Stateless Firewalls**

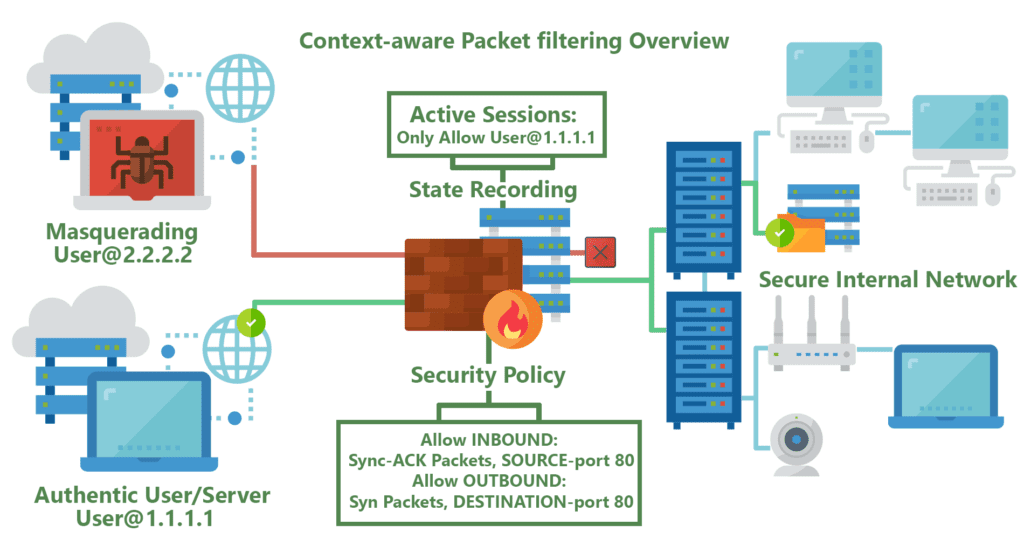


Stateless firewalls are some of the oldest firewalls on the market and have been around for almost as long as the web itself. The purpose of stateless firewalls is to protect computers and networks — specifically: routing engine processes and resources. They provide this security by filtering the packets of incoming traffic distinguishing between udp/tcp traffic and port numbers. The packets are either allowed entry onto the network or denied access based either their source or destination address or some other static information such as the traffic type (udp/tcp).These days completely stateless firewalls are far and few inbetween.

Today they are most commonly seen in the form of CPE’s (modems/router combos) given to customers by typical service providers. This equipment, usually given to residential internet consumers, provide simple firewalls using packet filtering and port forwarding functionality built on top of low-power CPE’s. Providing very basic but powerful security restricting incoming and outgoing traffic useful to protect commonly abused ports often by self-propagating or DDOSing malware, such as ports 443, 53, 80 and 25. This blanket port filtering is mostly implemented using white-lists allowing only a few key ports for application-specific traffic such as VoIP, as 90% of all internet traffic traverses with the Hyper-Text Transfer Protocol (HTTP) through proxy requests to Domain Name Servers (DNS). In other cases, such as when hosting servers for: multiplayer video games, email/web services, or live-streaming video, users must manually configure these firewalls outside of their default security policy to allow different ports & applications through the filter.

One commonly known pitfall of stateless firewalls is that they are unable to view packets as part of wider traffic and will inspect them in isolation and are mostly unable to distinguish the myriad of application-level traffic types (such as HTTP, HTTPS, FTP, VoIP, SSH, etc). This can make them susceptible to attacks that are not hidden within single packets but spread out across many of them. Stateless firewalls also do not keep track of the status of the network as a whole or the connections made to it. However, this does mean that stateless firewalls are much quicker and function more efficiently due to them only checking the header part of an inspected packet.

**Stateful Firewalls**



Most firewalls today offer at least some basic level of stateful monitoring. The main distinction between what can be very rudimentary stateful firewalls, and [extremely robust packet-processing solutions](https://www.lanner-america.com/), is in the level of protocol support. Greater support for differentiating between the diverse traffic and protocol types provides firewalls with the efficacy needed to analyze numerous application-level traffic, such as multimedia protocols, datagram protocols, file-transfer protocols, authentication/security protocols and so on.

Stateful firewalls are a more advanced, modern extension of stateless packet filtering firewalls in that they are continuously able to keep track of the state of the network and the active connections it has such as TCP streams or user datagram protocol (UDP) communication. The ability to acknowledging & utilize the context of incoming traffic and data packets is one of the principle advantages stateful firewalls have over their stateless cousins, allowing them to understand how to tell the difference between legitimate and malicious traffic or packets. This ultimately gives stateful firewalls one of the most powerful security tools in modern policies that protect their network connections through the implementation of additional security procedures for new or ongoing/active connections. In most cases, new connections will need to introduce themselves to the firewall with what most experts denote as a handshake, before being allowed onto the list of established connections.

Stateful firewalls are not without their vulnerabilities, however. The special handshake involved in establishing new active connections requires a significant increase in software/network connection complexity & the computational power needed to implement them, leaving such firewalls vulnerable to cyber threats such as distributed denial of service ([DDoS](https://www.lanner-america.com/network-computing/lanners-high-performance-x86-rackmount-network-appliances-ddos-attacks-prevention/)) attacks. This threat has been mitigated by many users of stateful firewalls by spreading out a network’s traffic across more [firewall appliances](https://www.lanner-america.com/products/network-appliances/), with many using third-party cloud-based service middle-men, in order to reduce the risk and necessary infrastructure.

|  |
| --- |
| *L*IKE *T*HIS *A*RTICLE? *S*IGN *U*P *F*OR *O*UR *N*EWSLETTER!  As you are reading this article, we are working hands on with some of the leading technology companies around the globe as their hardware partners. Together with these companies we are creating cutting edge solutions for IoT, NFV, A.I. and Intelligent Edge for a variety of industries. Sign up now so we can share with you our insights on these topics, latest trends and updates on our solutions.    Subscribe Now |

**Which is better?**

As is with most things, this varies on a case-by-case basis, with only the most basic residential users likely served well with their mostly stateless firewall given by their service providers. When it comes to power-users or business oriented networks, they are best served by the powerful stateful firewall implementations provided by dedicated systems running software such as PFSense, Endian or another robust offering. Having said this, while next-gen stateful firewalls offer all of the same security features present in stateless firewalls, they do not come without the need for cost-benefit analysis that should be done in regards to their feature-set and packet-filtering depth. The as important trade-offs and aspects of modern firewalls boil down to these requirements:

* Security Level (How secure/sensitive the information & network is)
* Performance Requirements (packets per second, devices on network, application overhead)
* Cost in terms of initial Capital Expenditure and ongoing Operating Expenditure for the hardware/software
* Networking & Computing Hardware Requirements along with the underlying infrastructure, space
* Software/Hardware Complexity, in terms of the integrations of upgradability, maintenance & support/EOL

[](https://www.lanner-america.com/contact-us/?subject=ihaq)  
For simple home use, modern computers have more than enough power to run robust software-based firewalls on desktop PC’s for example, but to easily secure the entire network using always-on purpose built low-power appliances like the [NCA-1210 Edge Security Appliance](https://www.lanner-america.com/product/nca-1210/) is a more cost-effective solution. Much more stable as a whole, these dedicated appliances can be configured to consistently protect all home & handheld devices like smart thermostats/lights, IP cameras and smart phones from unwanted snooping/tampering by intruders – 24/7 while keeping maintenance, power, space and heat footprints to a minimum.

For more advanced usage such as small businesses, power users (online collaborators, home labs, tech enthusiasts, live-streamers) & larger entities, robust stateful firewalls are almost certainly the most viable option to protect sensitive user data, connections and active services. Here the heavier upfront cost of powerful hardware like the [FW-8894 NGFW](https://www.lanner-america.com/product/fw-8894/) is less significant compared to the massive issues arising from the damages of lackluster security. Sub-par security can enable data breaches bringing issues such as: lawsuits, corporate/public image taint, service outages and contract/privacy breaches can all easily dwarf any upfront security investments.

Today businesses looking for the right security solution are best served by experts in the field of network security & hardware/software integration like Lanner. Capable of providing full services like validation, security module integration & quality assurance from the start –  [from the silicon & factory assembly all the way to the business premises](https://www.lanner-america.com/blog/youve-implemented-data-security-supply-chain-secure/).

The main disadvantage of basic packet filtering is that it is stateless. It does not remember the state of a telnet connection or an FTP connection flow already established or source port number of the client. In any application service, the TCP destination port is typically identified. For example, destination port for HTTP is 80 or FTP is 21. However, an FTP client can use any port and typically, this is dynamically chosen at run time. In basic packet filtering, since the firewall does not remember the previous state, and relies only on filtering rules, there is an amount of risk introduced, as some of the packets may bypass the firewall.

This type of risk is unavoidable for a basic packet filtering firewall. Therefore, all modern firewalls go beyond basic packet filtering, and are **stateful**. This means, the firewall keeps track of the **state** of connection flows for all the packets, in both directions – entering and exiting the firewall. The stateful firewall also keeps track of all the IP addresses currently being connected to the firewall.

A stateful firewall allows only those packets belonging to an allowed session. For example, instead of permitting any host to send data to the TCP port 8080, the firewall allows only those packets which already have the full TCP connection. Furthermore, it can check whether the packets are really of 8080 protocol traffic and it can enforce constraints at the application layer.

The main advantage of a stateful firewall is that the administrator no longer needs to write broad filtering rules, mentioning all the TCP services to allow or deny. The administrator needs to list the attributes of the flow's first packet in the rule base and the rest is taken care of by the firewall cache mechanism. An additional benefit is that the rules can be shorter. A single rule can describe the flow. Maintaining firewall rules becomes easy and prevents errors from creeping in. Finally, the stateful firewall provides better performance. With better structure of the table, a cache lookup can be made more efficient.

Network Address Translation (NAT)

An IP address is 32 bits long, and with the current schema, the maximum number of hosts you can have is about

4 billion different IP addresses. This puts a limit on the number of hosts that you can connect to the Internet. Since many companies have many hosts that need to communicate with the Internet, these 4 billion addresses are not enough and very quickly, these addresses get depleted. In 1994, RFC 16315 suggested a short term solution to this problem known as NAT (Network Address Translation). As it turned out, NAT not only solved the addressing problem, it became one of the ways to protect our internal network identity. RFC 7913, defines a set of IP addresses in each

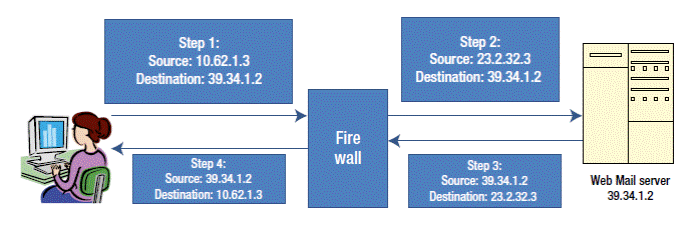
class as private addresses, used only within the private network and the rest of the addresses can be used as public addresses. The reserved ranges for private network are:

• 10.0.0.0 – 10.255.255.255 (10/8 prefix)

• 172.16.0.0 – 172.31.255.255 (172.16/12 prefix)

• 192.168.0.0 – 192.168.255.255 (192.168/16 prefix)

The primary reason for this is to ensure that the IP addresses are allocated efficiently. A private range of IP address, for example, 10.0.0.0/8, which is not in use on the Internet, when tries to connect to the outside world, has to be replaced by a public address. This is done using NAT. For example, a host is listed as 10.62.1.3, which is the source IP address. After NATing, the source address is replaced by a public address of 23.2.32.3. The destination computer sees just this IP address; the internal network address is never known to the outside world. Therefore, NAT provides protection to the inside network resources. This process is shown in Figure 10-9.



***Figure 10-9. NAT protecting internal network resources***

With NATing, companies can have only one public IP address. Any internal host that connects to the Internet or an outside network is NATed at the firewall. Internal hosts will never know that NATing has taken place. The destination host is also not aware of the NATing that has taken place. Thus NAT saves IP addresses. If more than one internal computer system is communicating with the Internet, as per the RFC 16315, all NAT firewall has to do is to change the source IP address, while it also needs to change the source port number with an unused port number above 1023 and keep track of this list temporarily during the connection.

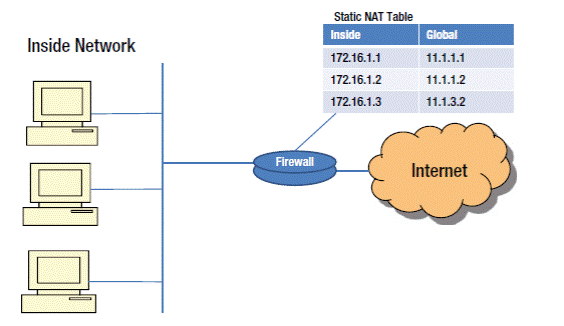
NATing serves as a *basic security* measure that can make it a bit more difficult for an external attacker to map

to the internal network IP addresses. When NATing is performed, the firewall rewrites the source IP address and stores both the altered source and destination IP addresses in the IP header. Internally, the firewall keeps track of the interface that is connected inside the network and interfaces connected to the outside network (global network).

Global addresses are registered and assigned by an Internet Service Provider (ISP). The firewall internally identifies the packets as inbound or outbound, that is, in which direction the traffic is actually moving, and accordingly does the translations (NATing).

Static Translation

The NAT can use either a static or a dynamic mapping. In static NAT, configuration mapping is always fixed in a specific way. In a static NAT, a pool of inbound IP addresses are mapped to a pool of outbound IP addresses on a one-to-one basis. Once it is configured, it is fixed. This is particularly useful for a web server which has a consistent address that is accessible from the Internet. Figure 10-10 shows an example of a static NAT. Each inside address (172.16.1.1, 172.16.1.2, and 172.16.1.3) is mapped one-to-one with a global address (11.1.2.1, 11.1.2.2, and 11.1.3.3).



***Figure 10-10.****Static NAT*

Dynamic Translation

In dynamic NATing, the mapping is not static. Mapping is based on the available IP address from a pool of public addresses. When a host inside the network requests access to the Internet, dynamic NAT picks up an IP address from a pool of addresses that has not been assigned and is not in use by any other host and assigns it to the host. Dynamic NATing is useful when fewer addresses are available and a larger number of hosts are to be

connected to the Internet.

Port Address Translation (PAT)

When there is only one global IP address and multiple hosts inside the LAN trying to access the Internet, then we use what is called Port Address Translation (PAT). This situation is called overloading. The NAT/PAT box needs a way

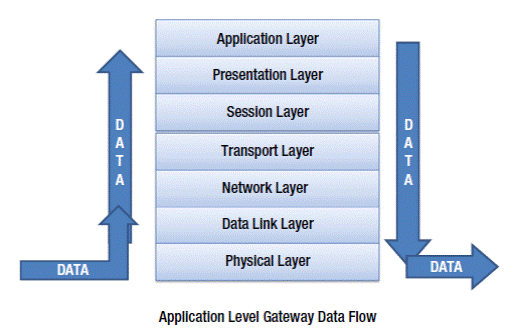
to keep track of the local addresses trying to connect to the Internet. This mapping is done using TCP/UDP ports. TCP/UDP uses 16 bits port numbers, which allows 65536 different services or source ports to be identified. When performing translation, PAT tries to use the original port number, if it is not used. If it is already in use, then the next available port number from the appropriate group is used.

The advantage of PAT is that multiple internal hosts can share a single global IP address. Global IP addresses are provided by ISP and they are expensive. Having one global IP address and with the help of PAT, organizations can save money. The second advantage is security. Internal networks are never exposed to the outside public network, making attacks from the outside more difficult and less frequent.

One disadvantage of PAT is the limitation on the number of hardware connections it supports. If too many internal hosts are trying to connect at the same time, then the hardware may run out of unused ports.

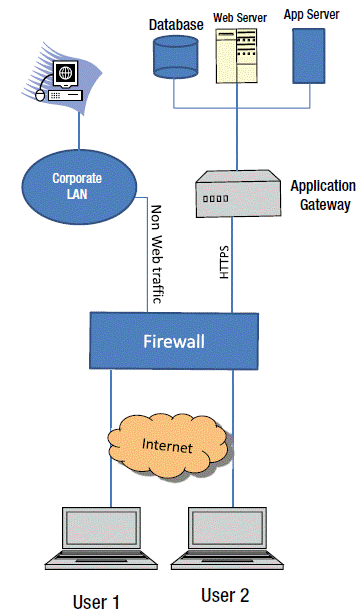
Application Level Gateways (Application Proxy)

As the name implies, an Application Level Gateway (ALG) inspects packets all the way up to the application layer and determines whether a packet is allowed or denied. It gives higher security than the packet filtering as the inspection is done all the way up to the application, as illustrated in Figure 10-11. However, this takes more CPU processing time and the necessity of having the knowledge of application protocol.



***Figure 10-11. How the Application Level Gateway Works***

An Application Level Gateway runs independently, copies and forwards information across the gateway and functions as a proxy server. It prevents a direct connection between a trusted server or client and an untrusted host. The proxies are application specific. Any new application that comes into the network needs to be informed to the application proxy, so that the rules may be set up and get executed for this application. It sits between a network firewall and a trusted host as shown in Figure 10-12. It can filter packets at the application layer.



***Figure 10-12. Packet Filtering at the application layer using the Application Level Gateway***

An Application Layer Gateway maintains a complete TCP connection state and sequencing. ALG typically evaluates packets that are applied to the interface after security policies are applied. ALGs operate behind the NAT or a firewall.

Some of the advantages of ALG include:

• Direct connection between internal and external hosts are not allowed

• User-level authentication is supported

• Packet is inspected right up to application data payload

However, there are limitations. The disadvantages of ALG include:

• More processing power required

• Slower than packet filtering

• Not every application protocol is supported. Whenever there is a new application, corresponding proxies must also be implemented.