

Securing Internal Networks with Proxy Servers

Proxy servers are an essential part of network security. They act as intermediaries between clients (like users or devices on an internal network) and external servers or the internet. By filtering and forwarding traffic, proxy servers help secure both internal networks and external communications. Here’s how they work and the different types of proxy servers that contribute to overall network security.

What is a Proxy Server?

A proxy server is a dedicated server that sits between the internet and an organization’s internal network. When a request to connect to the network comes from the internet, the proxy server evaluates whether the request is safe before allowing it to pass through. It does this by using a different IP address than the internal network, effectively hiding the private network’s IP from malicious actors on the internet. This adds an extra layer of security.

How Proxy Servers Enhance Security

1. Hiding Internal IPs:
   * When a client accesses a resource on the internet (e.g., a website), the proxy server will forward the request while masking the real IP address of the internal web server.
   * This prevents hackers from targeting internal IP addresses directly.
2. Blocking Unsafe Websites:
   * Proxy servers can be configured to block access to malicious or unsafe websites, preventing users from accidentally visiting harmful sites that could compromise network security.
3. Caching Data:
   * Proxy servers store copies of frequently requested data (known as caching). This reduces the need to repeatedly contact the organization’s internal servers for the same data, which not only boosts performance but also reduces the risk of internal servers being exposed to the internet.

Types of Proxy Servers

There are several types of proxy servers that serve different purposes within an organization. Here are the key types:

1. Forward Proxy Server

* Purpose:  
  A forward proxy server is used to control and regulate outgoing traffic from an internal network to the internet.
* How it works:
  + It receives outgoing requests from an internal client (e.g., an employee) and forwards those requests to the destination on the internet.
  + It hides the user's internal IP address and may restrict access to specific sites or services based on predefined rules.
* Use case:  
  This type of proxy server is commonly used to manage internet access for employees and restrict their ability to visit unsafe or inappropriate websites.

2. Reverse Proxy Server

* Purpose:  
  A reverse proxy server is used to protect internal servers from external traffic. It handles incoming requests from external parties (e.g., customers or the public) and forwards them to the correct internal server.
* How it works:
  + It receives requests for a web server or other internal resource, processes them, and then passes them to the internal network’s servers.
  + This ensures that the internal server's IP address is hidden, and the proxy server can filter malicious or suspicious requests before they reach the internal resources.
* Use case:  
  A reverse proxy is typically used for web servers to protect confidential data and prevent attackers from gaining access to the server’s true IP address.

3. Email Proxy Server

* Purpose:  
  An email proxy server filters email traffic, typically used to block spam and phishing attempts.
* How it works:
  + The proxy server intercepts emails before they reach the internal mail system, checking for malicious attachments, forged addresses, or suspicious content.
  + It helps prevent phishing attacks, which attempt to impersonate known individuals or organizations to steal sensitive information.
* Use case:  
  Used to improve email security, especially in larger organizations where email phishing is a common attack vector.

Real-World Example:  
In one organization, an email proxy server was set up to filter spam. It successfully tagged around 95% of messages as spam before they even reached the internal email platform. This not only protected users from phishing attacks but also allowed for better scalability of anti-spam measures.

Key Takeaways

* Proxy Servers help protect both internal networks and external communications by acting as intermediaries, filtering traffic, and hiding internal IP addresses.
* Different types of proxy servers, such as forward proxies, reverse proxies, and email proxies, serve different purposes, from controlling outgoing traffic to protecting internal web servers and filtering emails.
* By caching data, blocking unsafe websites, and inspecting incoming/outgoing traffic, proxy servers contribute significantly to enhancing network security.

As a security analyst, it's important to understand the role of proxy servers and to monitor the traffic passing through them to ensure that they are configured correctly and are functioning as an additional layer of protection for the network.

In the next section, we’ll explore securing internal networks in more detail, looking at tools and methods to ensure the safety of an organization’s private network.

# Virtual networks and privacy

This section of the course covered a lot of information about network operations. You reviewed the fundamentals of network architecture and communication and can now use this knowledge as you learn how to secure networks. Securing a private network requires maintaining the confidentiality of your data and restricting access to authorized users.

In this reading, you will review several network security topics previously covered in the course, including virtual private networks (VPNs), proxy servers, firewalls, and security zones. You'll continue to learn more about these concepts and how they relate to each other as you continue through the course.

## ****Common network protocols****

Network protocols are used to direct traffic to the correct device and service depending on the kind of communication being performed by the devices on the network. Protocols are the rules used by all network devices that provide a mutually agreed upon foundation for how to transfer data across a network.

There are three main categories of network protocols: communication protocols, management protocols, and security protocols.

1. Communication protocols are used to establish connections between servers. Examples include TCP, UDP, and Simple Mail Transfer Protocol (SMTP), which provides a framework for email communication.
2. Management protocols are used to troubleshoot network issues. One example is the Internet Control Message Protocol (ICMP).
3. Security protocols provide encryption for data in transit. Examples include IPSec and SSL/TLS.

Some other commonly used protocols are:

* HyperText Transfer Protocol (HTTP). HTTP is an application layer communication protocol. This allows the browser and the web server to communicate with one another.
* Domain Name System (DNS). DNS is an application layer protocol that translates, or maps, host names to IP addresses.
* Address Resolution Protocol (ARP). ARP is a network layer communication protocol that maps IP addresses to physical machines or a MAC address recognized on the local area network.

## ****Wi-Fi****

This section of the course also introduced various wireless security protocols, including WEP, WPA, WPA2, and WPA3. WPA3 encrypts traffic with the Advanced Encryption Standard (AES) cipher as it travels from your device to the wireless access point. WPA2 and WPA3 offer two modes: personal and enterprise. Personal mode is best suited for home networks while enterprise mode is generally utilized for business networks and applications.

## ****Network security tools and practices****

### ****Firewalls****

Previously, you learned that firewalls are network virtual appliances (NVAs) or hardware devices that inspect and can filter network traffic before it’s permitted to enter the private network. Traditional firewalls are configured with rules that tell it what types of data packets are allowed based on the port number and IP address of the data packet.

There are two main categories of firewalls.

* **Stateless:** A class of firewall that operates based on predefined rules and does not keep track of information from data packets
* **Stateful:** A class of firewall that keeps track of information passing through it and proactively filters out threats. Unlike stateless firewalls, which require rules to be configured in two directions, a stateful firewall only requires a rule in one direction. This is because it uses a "state table" to track connections, so it can match return traffic to an existing session

Next generation firewalls (NGFWs) are the most technologically advanced firewall protection. They exceed the security offered by stateful firewalls because they include deep packet inspection (a kind of packet sniffing that examines data packets and takes actions if threats exist) and intrusion prevention features that detect security threats and notify firewall administrators. NGFWs can inspect traffic at the application layer of the TCP/IP model and are typically application aware. Unlike traditional firewalls that block traffic based on IP address and ports, NGFWs rules can be configured to block or allow traffic based on the application. Some NGFWs have additional features like Malware Sandboxing, Network Anti-Virus, and URL and DNS Filtering.

### ****Proxy servers****

A proxy server is another way to add security to your private network. Proxy servers utilize network address translation (NAT) to serve as a barrier between clients on the network and external threats. Forward proxies handle queries from internal clients when they access resources external to the network. Reverse proxies function opposite of forward proxies; they handle requests from external systems to services on the internal network. Some proxy servers can also be configured with rules, like a firewall.  For example, you can create filters to block websites identified as containing malware.

### ****Virtual Private Networks (VPN)****

A VPN is a service that encrypts data in transit and disguises your IP address. VPNs use a process called encapsulation. Encapsulation wraps your unencrypted data in an encrypted data packet, which allows your data to be sent across the public network while remaining anonymous. Enterprises and other organizations use VPNs to help protect communications from users’ devices to corporate resources. Some of these resources include servers or virtual machines that host business applications. Individuals also use VPNs to increase personal privacy. VPNs protect user privacy by concealing personal information, including IP addresses, from external servers. A reputable VPN also minimizes its own access to user internet activity by using strong encryption and other security measures. Organizations are increasingly using a combination of VPN and SD-WAN capabilities to secure their networks. A software-defined wide area network (SD-WAN) is a virtual WAN service that allows organizations to securely connect users to applications across multiple locations and over large geographical distances.

### ****Key takeaways****

There are three main categories of network protocols: communication, management, and security protocols. In this reading, you learned the fundamentals of firewalls, proxy servers, and VPNs. More organizations are implementing a cloud-based approach to network security by incorporating a combination of VPN and SD-WAN capabilities as a service.

# VPN protocols: Wireguard and IPSec

A VPN, or virtual private network, is a network security service that changes your public IP address and hides your virtual location so that you can keep your data private when you’re using a public network like the internet. VPNs provide a server that acts as a gateway between a computer and the internet. This server creates a path similar to a virtual tunnel that hides the computer’s IP address and encrypts the data in transit to the internet. The main purpose of a VPN is to create a secure connection between a computer and a network. Additionally, a VPN allows trusted connections to be established on non-trusted networks. VPN protocols determine how the secure network tunnel is formed. Different VPN providers provide different VPN protocols.

This reading will cover the differences between remote access and site-to-site VPNs, and two VPN protocols: WireGuard VPN and IPSec VPN. A VPN protocol is similar to a network protocol: It’s a set of rules or instructions that will determine how data moves between endpoints. An endpoint is any device connected on a network. Some examples of endpoints include computers, mobile devices, and servers.

## Remote access and site-to-site VPNs

Individual users use remote access VPNs to establish a connection between a personal device and a VPN server. Remote access VPNs encrypt data sent or received through a personal device. The connection between the user and the remote access VPN is established through the internet.

Enterprises use site-to-site VPNs largely to extend their network to other networks and locations. This is particularly useful for organizations that have many offices across the globe. IPSec is commonly used in site-to-site VPNs to create an encrypted tunnel between the primary network and the remote network. One disadvantage of site-to-site VPNs is how complex they can be to configure and manage compared to remote VPNs.

## WireGuard VPN vs. IPSec VPN

WireGuard and IPSec are two different VPN protocols used to encrypt traffic over a secure network tunnel. The majority of VPN providers offer a variety of options for VPN protocols, such as WireGuard or IPSec. Ultimately, choosing between IPSec and WireGuard depends on many factors, including connection speeds, compatibility with existing network infrastructure, and business or individual needs.

### WireGuard VPN

WireGuard is a high-speed VPN protocol, with advanced encryption, to protect users when they are accessing the internet. It’s designed to be simple to set up and maintain. WireGuard can be used for both site-to-site connection and client-server connections. WireGuard is relatively newer than IPSec, and is used by many people due to the fact that its download speed is enhanced by using fewer lines of code. WireGuard is also open source, which makes it easier for users to deploy and debug. This protocol is useful for processes that require faster download speeds, such as streaming video content or downloading large files.

### IPSec VPN

IPSec is another VPN protocol that may be used to set up VPNs. Most VPN providers use IPSec to encrypt and authenticate data packets in order to establish secure, encrypted connections. Since IPSec is one of the earlier VPN protocols, many operating systems support IPSec from VPN providers.

Although IPSec and WireGuard are both VPN protocols, IPSec is older and more complex than WireGuard. Some clients may prefer IPSec due to its longer history of use, extensive security testing, and widespread adoption. However, others may prefer WireGuard because of its potential for better performance and simpler configuration.

## Key Takeaways

A VPN protocol is similar to a network protocol: It’s a set of rules or instructions that will determine how data moves between endpoints. There are two types of VPNs: remote access and site-to-site. Remote access VPNs establish a connection between a personal device and a VPN server and encrypt or decrypt data exchanged with a personal device. Enterprises use site-to-site VPNs largely to extend their network to different locations and networks. IPSec can be used to create site-to-site connections and WireGuard can be used for both site-to-site and remote access connections.