Firewalls and network security measures

- Firewalls and network security measures
- Virtual private networks (VPNs)
- Security zones
- Subnetting and CIDR
- Proxy servers
- Virtual networks and privacy
- Glossary terms from week 2
- Course 3 resources and citations

Firewalls and network security measures

In this video, you'll
learn about different types of firewalls.
These include hardware,
software, and cloud-based firewalls.
You'll also learn the difference between
a stateless and stateful firewall and
cover some of the basic operations
that a firewall performs.
Finally, you will explore how
proxy servers are used to
add a layer of security to the network.

A firewall is a network security device that
monitors traffic to and from your network.
It either allows traffic or it blocks
it based on a defined set of security rules.
A firewall can use port filtering,
which blocks or allows
certain port numbers to limit unwanted communication.
For example, it could have a rule
that only allows communications on port
443 for HTTPS or port
25 for email and blocks everything else.
These firewall settings will be determined by
the organization's security policy.

Let's talk about a few different kinds of firewalls.
A hardware firewall is considered the most
basic way to defend against threats to a network.
A hardware firewall inspects
each data packet before it's
allowed to enter the network.
A software firewall performs
the same functions as a hardware firewall,
but it's not a physical device.
Instead, it's a software program
installed on a computer or on a server.
If the software firewall is installed on a computer,
it will analyze all the traffic

received by that computer.
If the software firewall is installed on a server,
it will protect all the devices connected to the server.
A software firewall typically costs
less than purchasing a separate physical device,
and it doesn't take up any extra space.
But because it is a software program,
it will add some processing burden
to the individual devices.

Organizations may choose to use a cloud-based firewall.
Cloud service providers offer firewalls as
a service, or FaaS, for organizations.
Cloud-based firewalls are software firewalls
hosted by a cloud service provider.
Organizations can configure the firewall rules
on the cloud service provider's interface,
and the firewall will perform security operations on
all incoming traffic before
it reaches the organization’s onsite network.
Cloud-based firewalls also protect any assets or
processes that an organization
might be using in the cloud.

All the firewalls we have discussed can be
either stateful or stateless.
The terms "stateful" and "stateless"
refer to how the firewall operates.
Stateful refers to a class
of firewall that keeps track of
information passing through it
and proactively filters out threats.
A stateful firewall analyzes
network traffic for characteristics and
behavior that appear suspicious
and stops them from entering the network.
Stateless refers to a class
of firewall that operates based on
predefined rules and does not
keep track of information from data packets.
A stateless firewall only acts according to
preconfigured rules set by the firewall administrator.
The rules programmed by the firewall administrator tell
the device what to accept and what to reject.
A stateless firewall doesn't store analyzed information.
It also doesn't discover
suspicious trends like a stateful firewall does.

For this reason, stateless firewalls are considered
less secure than stateful firewalls.

A next generation firewall, or NGFW,
provides even more security than a stateful firewall.
Not only does an NGFW provide
stateful inspection of incoming and outgoing traffic,
but it also performs more
in-depth security functions like
deep packet inspection and intrusion protection.
Some NGFWs connect to
cloud-based threat intelligence services
so they can quickly update to
protect against emerging cyber threats.

Now you have a basic understanding
of firewalls and how they work.
We learned that firewalls can be hardware or software.
We also discussed the difference between
a stateless and stateful firewall
and the security benefits of a stateful firewall.
Finally, we discussed next generation firewalls
and the security benefits they provide.
Coming up, we'll learn more about virtual networks.

Virtual private networks (VPNs)

In this video, we're going to
discuss how virtual private networks,
or VPNs, add security to your network.
When you connect to the internet,
your internet service provider receives
your network's requests and
forwards it to the correct destination server.
But your internet requests
include your private information.
That means if the traffic gets intercepted,
someone could potentially connect your internet activity
with your physical location
and your personal information.
This includes some information
that you want to keep private,
like bank accounts and credit card numbers.
A virtual private network,
also known as a VPN,
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 also encrypt your data as it
travels across the internet to preserve confidentiality.
A VPN service performs
encapsulation on your data in transit.
Encapsulation is a process performed
by a VPN service that protects
your data by wrapping
sensitive data in other data packets.
Previously, you learned how the MAC and IP address of
the destination device is contained
in the header and footer of a data packet.
This is a security threat because it shows
the IP and virtual location of your private network.
You could secure a data packet by encrypting
it to make sure your information can't be deciphered,
but then network routers won't be able to read
the IP and MAC address to know where to send it to.
This means you won't be able to connect to

the internet site or the service that you want.
Encapsulation solves this problem
while still maintaining your privacy.
VPN services encrypt your data packets and
encapsulate them in other data packets
that the routers can read.
This allows your network requests
to reach their destination,
but still encrypts your personal data
so it's unreadable while in transit.
A VPN also uses an encrypted tunnel
between your device and the VPN server.
The encryption is unhackable without a cryptographic key,
so no one can access your data.

VPN services are simple and offer
significant protection while you're on the internet.
With a VPN,
you have the added assurance that your data is encrypted, and
your IP address and
virtual location are unreadable to malicious actors.

Security zones

In this section, we'll discuss a type of
network security feature called a security zone.
Security zones are a segment of a network
that protects the internal network from the internet.
They are a part of a security technique
called network segmentation
that divides the network into segments.
Each network segment has
its own access permissions and security rules.
Security zones control who can
access different segments of a network.
Security zones act as a barrier to internal networks,
maintain privacy within corporate groups,
and prevent issues from spreading to the whole network.
One example of network segmentation is
a hotel that offers free public Wi-Fi.
The unsecured guest network is kept separate from
another encrypted network used by the hotel staff.

Additionally, an organization's
network can be divided into
subnetworks, or subnets, to
maintain privacy for each department in a organization.
For instance, at a university,
there may be a faculty subnet
and a separate students subnet.
If there is contamination on the student's subnet,
network administrators can isolate it and
keep the rest of the network free from contamination.

An organization's network is classified into
two types of security zones. First,
there's the uncontrolled zone,
which is any network outside of
the organization's control, like the internet.
Then, there's the controlled zone,
which is a subnet that protects
the internal network from the uncontrolled zone.
There are several types of
networks within the controlled zone.
On the outer layer is the demilitarized zone,
or DMZ, which contains

public-facing services that can access the internet.
This includes web servers,
proxy servers that host websites for the public,
and DNS servers that provide
IP addresses for internet users.
It also includes email and file
servers that handle external communications.
The DMZ acts as
a network perimeter to the internal network.
The internal network contains private servers and
data that the organization needs to protect.
Inside the internal network is
another zone called the restricted zone.
The restricted zone protects
highly confidential information that is only
accessible to employees with certain privileges.

Now, let's try to picture these security zones.
Ideally, the DMZ is situated between
two firewalls. One of them
filters traffic outside the DMZ,
and one of them filters traffic
entering the internal network.
This protects the internal network
with several lines of defense.
If there's a restricted zone,
that too would be protected with
another firewall. This way,
attacks that penetrate into
the DMZ network cannot spread to the internal network,
and attacks that penetrate
the internal network cannot access the restricted zone.
As a security analyst,
you may be responsible for regulating
access control policies on these firewalls.
Security teams can control traffic reaching
the DMZ and the internal network
by restricting IPs and ports.
For example, an analyst may ensure that
only HTTPS traffic is
allowed to access web servers in the DMZ.

Security zones are
an important part of securing networks,
especially in large organizations.
Understanding how they are used is
essential for all security analysts.

Coming up, we'll learn about securing internal networks.

Subnetting and CIDR

Earlier in this course, you learned about network segmentation, a security technique that divides networks into sections. A private network can be segmented to protect portions of the network from the internet, which is an unsecured global network.

For example, you learned about the uncontrolled zone, the controlled zone, the demilitarized zone, and the restricted zone. Feel free to review the video about security zones

for a refresher on how network segmentation can be used to add a layer of security to your organization's network operations. Creating security zones is one example of a networking strategy called subnetting.

Overview of subnetting

Subnetting is the subdivision of a network into logical groups called subnets. It works like a network inside a network. Subnetting divides up a network address range into smaller subnets within the network. These smaller subnets form based on the IP addresses and network mask of the devices on the network. Subnetting creates a network of devices to function as their own network. This makes the network more efficient and can also be used to create security zones. If devices on the same subnet communicate with each other, the switch changes the transmissions to stay on the same subnet, improving speed and efficiency of the communications.

Two subnets for two networks connected to one router.

Classless Inter-Domain Routing notation for subnetting

Classless Inter-Domain Routing (CIDR) is a method of assigning subnet masks to IP addresses to create a subnet. Classless addressing replaces classful addressing. Classful addressing was used in the 1980s as a system of grouping IP addresses into classes (Class A to Class E). Each class included a limited number of IP addresses, which were depleted as the number of devices connecting to the internet outgrew the classful range in the 1990s. Classless CIDR addressing expanded the number of available IPv4 addresses.

CIDR allows cybersecurity professionals to segment classful networks into smaller chunks. CIDR IP addresses are formatted like IPv4 addresses, but they include a slash ("/"") followed by a number at the end of the address, This extra number is called the IP network prefix. For example, a regular

IPv4 address uses the 198.51.100.0 format, whereas a CIDR IP address would include the IP network prefix at the end of the address, 198.51.100.0/24. This CIDR address encompasses all IP addresses between 198.51.100.0 and 198.51.100.255. The system of CIDR addressing reduces the number of entries in routing tables and provides more available IP addresses within networks. You can try converting CIDR to IPv4 addresses and vice versa through an online conversion tool, like IPAddressGuide

, for practice and to better understand this concept.

Note: You may learn more about CIDR during your career, but it won't be covered in any additional depth in this certificate program. For now, you only need a basic understanding of this concept.

Security benefits of subnetting

Subnetting allows network professionals and analysts to create a network within their own network without requesting another network IP address from their internet service provider. This process uses network bandwidth more efficiently and improves network performance. Subnetting is one component of creating isolated subnetworks through physical isolation, routing configuration, and firewalls.

Key takeaways

Subnetting is a common security strategy used by organizations. Subnetting allows organizations to create smaller networks within their private network. This improves the efficiency of the network and can be used to create security zones.

Proxy servers

Previously, we discussed how firewalls, VPNs, and
security zones help to secure networks.
Next, we'll cover how to secure internal networks with proxy servers.

Proxy servers are another system that helps secure networks.
The definition of a proxy server is a server that fulfills the request of
a client by forwarding them on to other servers.
The proxy server is a dedicated server that sits between the internet and
the rest of the network.
When a request to connect to the network comes in from the internet,
the proxy server will determine if the connection request is safe.
The proxy server is a public IP address that is different from the rest
of the private network.
This hides the private network's IP address from malicious actors on the internet and
adds a layer of security.

Let's examine how this will work with an example.
When a client receives an HTTPS response, they will notice a distorted IP address or
no IP address rather than the real IP address of the organization's web server.
A proxy server can also be used to block unsafe websites that users aren't allowed
to access on an organization's network.
A proxy server uses temporary memory to store data that's
regularly requested by external servers.
This way, it doesn't have to fetch data from an organization's internal
servers every time.
This enhances security by reducing contact with the internal server.

There are different types of proxy servers that support network security.
This is important for security analysts who monitor
traffic from various proxy servers and may need to know what purpose they serve.
Let's explore some different types of proxy servers.
A forward proxy server regulates and
restricts a person with access to the internet.
The goal is to hide a user's IP address and approve all outgoing requests.
In the context of an organization,
a forward proxy server receives outgoing traffic from an employee, approves it, and
then forwards it on to the destination on the internet.
A reverse proxy server regulates and
restricts the internet access to an internal server.
The goal is to accept traffic from external parties, approve it, and
forward it to the internal servers.
This setup is useful for protecting internal web servers containing

confidential data from exposing their IP address to external parties.
An email proxy server is another valuable security tool.
It filters spam email by verifying whether a sender's address was forged.
This reduces the risk of phishing attacks that impersonate people known to the organization.

Let's talk about a real world example of an email proxy.
Several years ago when I was working at a large U.S. broadband ISP,
we used a proxy server to implement multiple layers of anti-spam filtering
before a message was allowed in for delivery.
It ended up tagging around 95% of messages as spam.
The proxy servers would've allowed us to filter and
then scale those filters without impacting the underlying email platform.

Proxy servers play an important part in network security by filtering incoming and outgoing traffic and staying alert to network attacks.
These devices add a layer of protection from the unsecured public network that we call the internet.

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), virtual local area networks (VLANs), proxy servers, firewalls, tunneling, 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 encrypted data in an unencrypted 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 connecting to servers or virtual machines that host business applications. VPNs can also be used for personal use to increase personal privacy. They allow the user to access the internet without anyone being able to read their personal information or access their private IP address. 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.

Glossary terms from week 2

Glossary terms from week 2

Terms and definitions from Course 3, Week 2

Address Resolution Protocol (ARP): A network protocol used to determine the MAC address of the next router or device on the path

Cloud-based firewalls: Software firewalls that are hosted by the cloud service provider

Controlled zone: A subnet that protects the internal network from the uncontrolled zone

Domain Name System (DNS): A networking protocol that translates internet domain names into IP addresses

Encapsulation: A process performed by a VPN service that protects your data by wrapping sensitive data in other data packets

Firewall: A network security device that monitors traffic to or from your network

Forward proxy server: A server that regulates and restricts a person’s access to the internet

Hypertext Transfer Protocol (HTTP): An application layer protocol that provides a method of communication between clients and website servers

Hypertext Transfer Protocol Secure (HTTPS): A network protocol that provides a secure method of communication between clients and servers

IEEE 802.11 (Wi-Fi): A set of standards that define communication for wireless LANs

Network protocols: A set of rules used by two or more devices on a network to describe the order of delivery of data and the structure of data

Network segmentation: A security technique that divides the network into segments

Port filtering: A firewall function that blocks or allows certain port numbers to limit unwanted communication

Proxy server: A server that fulfills the requests of its clients by forwarding them to other servers

Reverse proxy server: A server that regulates and restricts the internet's access to an internal server

Secure File Transfer Protocol (SFTP): A secure protocol used to transfer files from one device to another over a network

Secure shell (SSH): A security protocol used to create a shell with a remote system

Security zone: A segment of a company’s network that protects the internal network from the internet

Simple Network Management Protocol (SNMP): A network protocol used for monitoring and managing devices on a network

Stateful: A class of firewall that keeps track of information passing through it and proactively filters out threats

Stateless: A class of firewall that operates based on predefined rules and does not keep track of information from data packets

Transmission Control Protocol (TCP): An internet communication protocol that allows two devices to form a connection and stream data

Uncontrolled zone: The portion of the network outside the organization

Virtual private network (VPN): A network security service that changes your public IP address and masks your virtual location so that you can keep your data private when you are using a public network like the internet

Wi-Fi Protected Access (WPA): A wireless security protocol for devices to connect to the internet

Course 3 resources and citations

Week 1: Network architecture

Resources

Helpful resources to get started

- Coursera Code of Conduct
- Coursera Honor Code
- Coursera: Edit my profile
- Coursera: Learner Help Center
- Coursera’s Global Online Community
- Google: Common problems with labs
- Google Docs help
- Google Sheets help
- How to use Google Slides
- Microsoft Excel help and learning
- PowerPoint help and learning

- Word help and learning
-

Citations

Network components, devices, and diagrams

- Meyers, Mike, and Scott Jernigan. (2019) CompTIA A+ Certification All-in-One Exam Guide, (Exams 220-1001 & 220-1002).
- Oluwatosin, H.S. (2014). Client-server model. *IOSR Journal of Computer Engineering*, *16* (1), 67-71.
- Sulyman, Shakirat. (2014). Client-Server Model. IOSR Journal of Computer Engineering. 16. 57-71. 10.9790/0661-16195771.
- GeeksforGeeks. (2022, March 21). *Devices used in each layer of TCP/IP model*

.

-

Cloud computing and software-defined networks

- Rackspace Technology Colo Data Centers. (n.d.). *What is colocation?*
-
- Fortinet. (n.d.). *What is hybrid cloud?*
-

Learn more about the TCP/IP model

- Clarke, Glen E. (2018). CompTIA Network+ Certification Study Guide: Exam N10-007.
- International Business Machines. (2022, Nov 15). *User datagram protocol*
- .
- International Business Machines. (2022, Nov 15). *Transmission control protocol*
- .
- Oracle. (n.d.). *TCP/IP protocol architecture model*

- . System administration guide, volume 3.
- Study CCNA. (n.d.). *OSI & TCP/IP models*
- .

The OSI model

- Cloudflare. (n.d.). *What is the OSI model?*
-
- FreeCodeCamp. (2020, December 21). *The OSI Model – The 7 Layers of Networking Explained in Plain English*
- .
- Imperva. (n.d.). *OSI Model*
- . Application security.

Components of network layer communication

- Agnė Srėbaliūtė. (2022, Aug 2). *IPv4 packet header: Format and structure*
- . IPXO.
- Rajinder Kaur (2009) *IPv4 Header*
- . Advanced Internet Technologies.
- Gsephrioth. (2017). *The IP diagram*
- .
- Wright, Robert. (October 1998). *IP Routing Primer*. O'Reilly.

Week 2: Network operations

Citations

Network protocols

- National Institute of Standards and Technology. (n.d.). *Glossary*
- . Accessed December 2022.

Common network protocols

- Cloudflare. (n.d.). *What is a protocol? | Network protocol definition*
- .
- CompTIA. (n.d.). *What is a network protocol and how does it work?*
-
- Oracle. (n.d.). *TCP/IP protocol architecture model*
- . System administration guide, volume 3.

Additional network protocols

- IBM. (2022, Oct 17). *TCP/IP address and parameter assignment - Dynamic host configuration protocol*
- . IBM AIX documentation.
- Microsoft. (n.d.O). *What are IMAP and POP?*
- Microsoft Support.
- Microsoft. (2013, October 21). *SMTP*
- .

The evolution of wireless security protocols

- Asus. (2022, January 14). *[Wireless] What is WPA3? What are the advantages of using WPA3?*
- FAQ.
- Britannica, T. Editors of Encyclopaedia (2022, February 3). *Wi-Fi*
- . *Encyclopedia Britannica*.
- Cisco Press. (2010, April 9). *Moving to WPA/WPA2-Enterprise wi-fi encryption*
- .

Firewalls and network security measures

- Cisco. (n.d.). *What is a firewall?*
-

Subnetting and CIDR

- Cloudflare. (n.d.). *What is a subnet?*
-
- Techopedia. (2017, July 18). *Subnetting*
- . Dictionary.
- IP Address Guide. (n.d.). *CIDR to IPv4 Conversion*
- . IPV4 Tools.

Proxy servers

- National Institute of Standards and Technology. (n.d.). *Glossary*
- . Accessed December 2022.

Week 3: Secure against network intrusions

Resources

Analyze network attacks

- CompTIA

-

Citations

The case for securing networks

- Vinton, Kate. (2014, September 18). *With 56 million cards compromised, Home Depot's breach is bigger than Target's*
- . Forbes.

Analyze network layer communication

- Lager, Nathan. (2020, April 3). Network Troubleshooting with Packet Captures
- . Enable Sysadmin.
- Oracle. (n.d.) How the TCP/IP Protocols Handle Data Communications (System Administration Guide: IP Services
-).

Real-life DDoS attack

- Olenick, D. (2020, December 10) *Guilty plea in 2016 Dyn DDos attack*
- . Bank info security.
- Young, K (2022, January 10) *Cyber case study: The Mirai DDoS attack on Dyn*
- . Coverlink.

Overview of interception attacks

- Engebretson, P. (2013). *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier.

Week 4: Security hardening

Resources

Course 3 glossary

Apply OS hardening techniques

- Opensource.com
-
- Iana.org
-
- Geekflare
-
- Packet Pushers
-

Citations

OS hardening practices

- National Institute of Security Technology. (2018, October). *Guide to securing macOS 10.12 systems for IT professionals*
- . Special publication 800-179, revision 1. Accessed December 2022.

Apply OS hardening techniques

- Doropoulos, N. (n.d.). DNS Query Flood Attack.

- Linkedin.

Use the NIST Cybersecurity Framework to respond to a security

- Bhardwaj, P. (2023, January 2). How to detect an ICMP flood attack and protect your network.
-

Firch, J. (2023, February 28). How to prevent a ICMP flood attack.

Google, Android, Chronicle, Google Drive, Google Sites, and YARA are trademarks owned by Google LLC. All other trademarks belong to their respective owners and are not affiliated with Google LLC.