Hoofd1-8

Hoofdstuk : OSPF Features and Characteristics

OSPFv2 is used for IPv4 networks

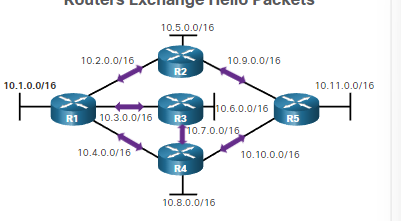
SPF has significant advantages over RIP in that it offers faster convergence and scales to much larger network implementations.rip kan niet werken in larger networks

A link is an interface on a router. A link is also a network segment that connects two routers, or a stub network such as an Ethernet LAN that is connected to a single router. Information about the state of a link is known as a link-state. All link-state information includes the network prefix, prefix length, and cost.

Components of OSPF :

* Routing protocol messages : hello packets,database description packet, linkstate request packet and link state update packet and link state acknowledge packet => doel neighbor discovery
* Database structure : ospf databases => adjency database : neighbor table, link state database : topology table , forwarding database : routing table
* Algoritm : he SPF algorithm is based on the cumulative cost to reach a destination, OSPF places the best routes into the forwarding database, which is used to make the routing table.

Link-State Operation

* he following are the link-state routing steps that are completed by a router:
* 
  + **Establish neighbor adjacensie** : hello packets => om tew eten of er neighbors zijn (ospf enabled routers) If a neighbor is present, the OSPF-enabled router attempts to establish a neighbor adjacency with that neighbor.
  + **Exchange link state advertisement** : Afbeelding met tekst, schermopname, diagram, lijn

    Automatisch gegenereerde beschrijving

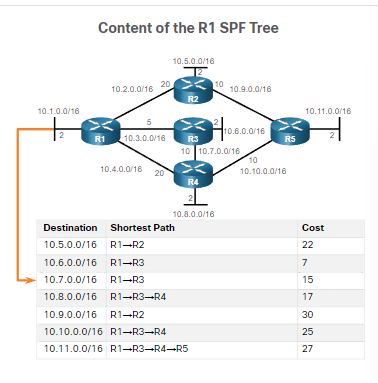
Na de adjecensie dan word er lsa’s gestuurd soor elke router. De ls geeft de state en de cost van elke connected link.

* + **Nadat de lsa is gedaan** dan gaat de router een topology table maken zodat ze weten hoe de netwerk in de ospf eruit ziet van die area
  + **Execute the spf algoritm** : spf algotritm word dan gebruikt om de spf tree te maken

Afbeelding met tekst, diagram, schermopname, ontwerp

Automatisch gegenereerde beschrijving

* **Choose best path** : maakt de beste pad naar waar je wilt gaan. Dit gebuerd naar de spf tree



**Single-Area OSPF** - All routers are in one area. Best practice is to use area 0.

**Multiarea OSPF -** OSPF is implemented using multiple areas, in a hierarchical fashion. All areas must connect to the backbone area (area 0). Routers interconnecting the areas are referred to as Area Border Routers (ABRs).

**Multiarea OSPF**

For instance, any time a router receives new information about a topology change within the area (including the addition, deletion, or modification of a link) the router must rerun the SPF algorithm, create a new SPF tree, and update the routing table. The SPF algorithm is CPU-intensive and the time it takes for calculation depends on the size of the area.

Als uw lsdb te groot is dan gaat de load of de cpu increasen : oplossing :

Afbeelding met tekst, Lettertype, schermopname, informatie

Automatisch gegenereerde beschrijving

Ospfv3 :

Gebruikt ipv6 addressen ,

OSPFv3 has the same functionality as OSPFv2, but uses IPv6 as the network layer transport, communicating with OSPFv3 peers and advertising IPv6 routes. OSPFv3 also uses the SPF algorithm as the computation engine to determine the best paths throughout the routing domain.

Ospfpackets :

Afbeelding met tekst, Lettertype, schermopname

Automatisch gegenereerde beschrijving

Linkstate update :

Lsu worden gebruikt wanneer er een lsr word gestuurd maar ze worden ook gebruikt wanneer de osf routing updates dan word er lsu’s gestuurd.

Een lsu contains one or more lsa’s

Lsa contains route information for the destination

Hello packkets :

Discover neighbors

Advertise parameters on which two routers must become neighbours

Elect dr,bdr on multiaccess networks

Point to point state do not require dr en bdr

Laat zien wat allemaak in de ospfpacket hello packet :

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

Ospf operation :

Ospf operational states

Afbeelding met tekst, schermopname, Lettertype, document

Automatisch gegenereerde beschrijving

Establish neighbor adjencensie

When OSPF is enabled on an interface, the router must determine if there is another OSPF neighbor on the link. To accomplish this, the router sends a Hello packet that contains its router ID out all OSPF-enabled interfaces. The Hello packet is sent to the reserved All OSPF Routers IPv4 multicast address 224.0.0.5. Only OSPFv2 routers will process these packet

router ID is a 32-bit number formatted like an IPv4 address and assigned to uniquely identify a router among OSPF peers.

When a neighboring OSPF-enabled router receives a Hello packet with a router ID that is not within its neighbor list, the receiving router attempts to establish an adjacency with the initiating router

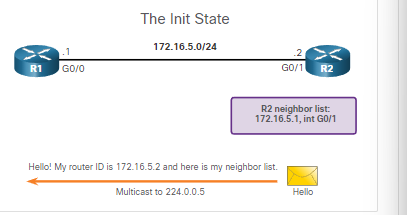
Down state to initstate =

Afbeelding met tekst, schermopname, diagram, lijn

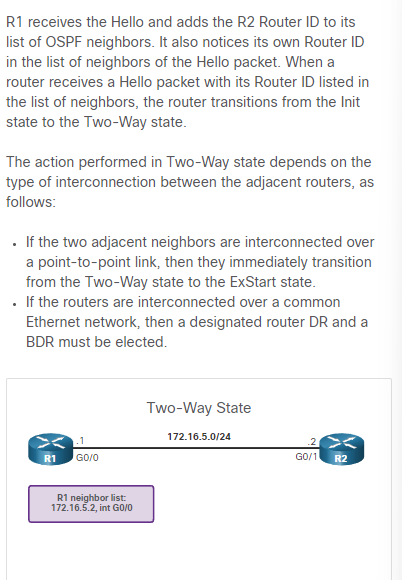
Automatisch gegenereerde beschrijving

The inti state =

Zet de router id van r1 in de neighbor table en dan stuurt een hello terug naar r1



Two way state = In the "Two-Way" state, routers have received Hello packets from each other, and they have confirmed that they can reach each other. However, they have not yet agreed to form a full neighbor relationship.



Elect the d rand bdr :

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Synchronizing OSPF Databases :

After the Two-Way state, routers transition to database synchronization states

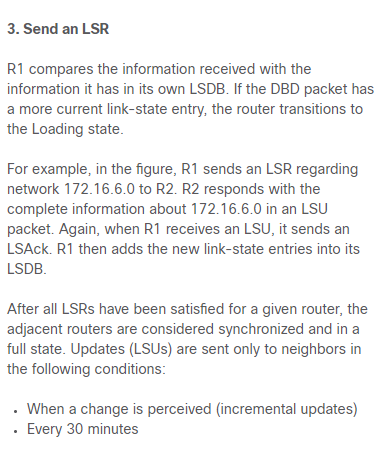
Decide first router = with higher router id die router suurt als eerst de dbd paketten in de exhchange state

Exchange dbd =

Afbeelding met tekst, schermopname, Lettertype, document

Automatisch gegenereerde beschrijving

Send a lsr =



Why is there a need for a DR:

Afbeelding met tekst, schermopname, Lettertype, document

Automatisch gegenereerde beschrijving

Afbeelding met tekst, Lettertype, schermopname, algebra

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, nummer

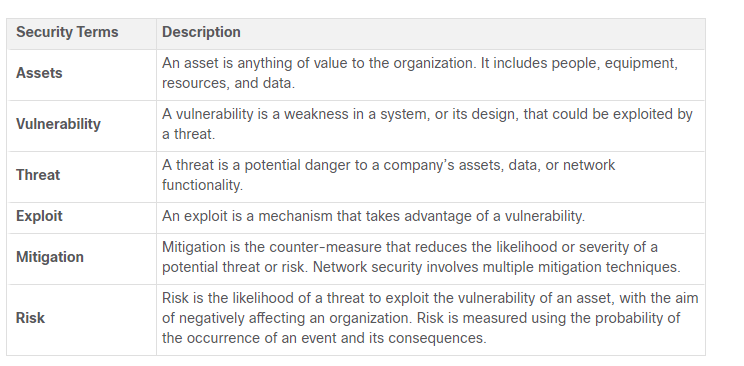
Automatisch gegenereerde beschrijving

Als je een dr hebt en bv router 1 is een dr en router 2 wilt een lsa sturen dan gaat de lsa naar de dr en de dr stuur de lsa naar iedereen.op dit mannier stuurt niet elke router een lsa maar alleen de dr

**Hoofdstuk : network security concepts :**

Current state of cyber security

Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people’s privacy, and compromise the integrity of information. These breaches can result in lost revenue for corporations, theft of intellectual property, lawsuits, and can even threaten public safety.



Assets must be identified and protected. Vulnerabilities must be addressed before they become a threat and are exploited. Mitigation techniques are required before, during, and after an attack.

Vectors of Network Attacks

An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network, as shown in the figure. For example, threat actors may target a network through the internet, to disrupt network operations and create a denial of service (DoS) attack.

Afbeelding met tekst, diagram, schermopname, ontwerp

Automatisch gegenereerde beschrijving

DoS attack occurs when a network device or application is incapacitated and no longer capable of supporting requests from legitimate users.

An internal user, such as an employee, can accidentally or intentionally:

* Steal and copy confidential data to removable media, email, messaging software, and other media.
* Compromise internal servers or network infrastructure devices.
* Disconnect a critical network connection and cause a network outage.
* Connect an infected USB drive into a corporate computer system.

Internal threats zijn gevaarlijker dan external threats want die internal heeft direct acces to de building and its infrastructure decvices.

Data Loss

Data is de belangrijkste asset van een organisatie.

Data loss is wanneer de data perongeluk of express word verloren of gestolen of geleaked naar de buiten wereld.

Gevolgen van data loss:

* Brand dammage of loss reputation
* Loss of competitive advandatage
* Klanten kwijt
* Loss of revenu
* Litigation/legal action resulting in fines and civil penalties
* Significant cost and effort to notify affected parties and recover from the breach

Hoe data loss kan gebueren

* Email/social networking : email of im messages opvangen en revalen van confidential information
* Unencrypted devices : de dief kan makkelijk aan de confindetial info als er geen encrytion op is
* Cloud storage devices : Sensitive data can be lost if access to the cloud is compromised due to weak security settings.
* Removable media : One risk is that an employee could perform an unauthorized transfer of data to a USB drive. Another risk is that a USB drive containing valuable corporate data could be lost
* Hard copy : confidential data should be shredded when no longer needed
* Improper access control : password of zwakke password is gecomprimes waardoor de threat actor makkelijk aan de corporate data kan.

Network security professionals must protect the organization’s data. Various Data Loss Prevention (DLP) controls must be implemented which combine strategic, operational and tactical measures.

Threat actors

The hacker

Originally the term referred to someone who was a skilled computer expert such as a programmer and a hack was a clever solution.

White hat hackers : these hackers users their programming skills voor legak purposes. Zoekt security vulnerabilities and reports to developers for them to fix before the vulnerabilities can be exploited.

Gray hat hacker : These are individuals **who commit crimes and do arguably unethical things**, **but not** for personal gain or to cause damage. Gray hat hackers may **disclose a vulnerability to the affected organization after having compromised their network.**

**Black hat hacker :** These are unethical criminals who compromise computer and network **security for personal gain, or for malicious reasons, such as attacking network**

In this course, we will not use the term hacker outside of this module. We will use the term threat actor. The term threat actor includes hackers. But threat actor also includes any device, person, group, or nation state that is, intentionally or unintentionally, the source of an attack.

Evolution of hackers :

Modern hacking terms :

**Script kiddies** : gebruikt een **exisitening script** to cause harm. Not for profit

**Vulnerability broker** : gray hat hacker => **discover exploit** and report to vendors soms voor geld

**Hacktitvis :** gray hat hacker => **publicly protest organizations** or governments by posting articles, videos, leaking sensitive information, and performing network attacks.

**Cyber criminals** : black hat hackers => **self employed** of werken voor een **groote cyber crime organisation**

**State-sponsored** : white hat hacker of black hat hacker => who **steal government secrets**, gather intelligence, and sabotage networks. **Their targets** **are foreign governments**, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking.

Cyber Criminals

It is estimated that cyber criminals steal **billions of dollars from consumers and businesses**. Cyber criminals operate in an **underground economy where they buy, sell, and trade attack toolkits**, zero day exploit code, botnet services, banking Trojans, keyloggers, and much more. They also **buy and sell** the **private information and intellectual property they steal**. Cyber criminals target small businesses and consumers, as well as large enterprises and entire industries.

Hacktivists

Two examples of hacktivist groups are Anonymous and the Syrian Electronic Army. **Although most hacktivist groups are not well organized,** they can cause significant problems for governments and businesses. Hacktivists tend to rely on fairly basic, freely available tools

State-Sponsored Hackers

State-sponsored hackers create advanced, customized attack code, often using previously **undiscovered software vulnerabilitie**s called zero-day vulnerabilities. An example of a state-sponsored attack involves the Stuxnet malware that was created to damage Iran’s nuclear enrichment capabilities.

Threat actor tools :

Evolution of Security Tools

Penetration testing tool :

**Password crackers** : crack or recover password. Password **repeadetly make geusses** until it cracks the password. John the ripper

**Wireless hacking tools** : hack into a wireless network **to detect security vulnerabilities**. Vb kismet

**Network scanning and hacking tools** : probe network devices, servers, and hosts for open TCP or UDP ports**. Vb nmap**

**Packet crafting tool : robe** and test a firewall’s robustness using **specially crafted forged packets**.vb Hping

**Packet sniffers : capture** and **analyze packets within** traditional Ethernet LANs or WLANs.wireshark

**Rootkit detectors :** his is a directory and **file integrity checker** used **by white hats to** detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter. White hacker

**Fuzzers to search** vulnerabilities : **discover computer security vulnerabilities** vb skipfish

**Forensic tools** : white hackers => **sniff any trace of evidence of a existing computer** vb HELIX

**Debuggers :** black hat hacker : **reverse engineer binaru files** when **writing exploits**.word ook gebruikt bij white hat **hackers om malware te anylazinge.vb** winDbg

**Hacking operarting systems** : os made for hacking vb kali linux. **Pre installed hacking tools in os**

Encryption tools : **openssh, openssl**

**Vulnerability exploitation tools** : identify whether **a remote host is vulnerable to a security attack**. Vb metaspoit

**Vulnerability scanners** : scan a network system to identify open ports . kan ook gescanned worden voor known vulnerability and scan vm’s vb NIPPER

Many of these tools are UNIX or Linux based; therefore, a security professional should have a strong UNIX and Linux background.

Attack Types

**Eavesdropping attack :** listen to network traffic => andere naam is sniffing of snooping

**Data modification attack :** If threat **actors have captured enterprise traffic**, they can alter the data in the packet without the knowledge of the sender or receiver.

**Ip address spoofing attack** : A threat actor **constructs an IP packet** that appears to originate from a valid address inside the corporate intranet

**Password based attack** : if threat actors **discover a valid user account**, the threat actors have the **same rights as the real user.** Threat actors could use that valid account to obtain lists of other users, network information, change server and network configurations**, and modify, reroute, or delete data.**

**Denial of service attack (dos) :** A DoS attack prevents normal use of a computer or network by valid users. A DoS attack can **flood a computer or the entire network with traffic** until a shutdown occurs because of **the overload**. A DoS attack can also block traffic, which results in a loss of access to network resources by authorized users.

**Man in the middle attack** : this attack occurs when threat actors have positioned themselves **between a source and destination.** They can now actively monitor, capture, and control the communication transparently.

**Compromised key attack** : threat **actor obtiain secrect key.** That key becomes a **compromised key**. A compromised key can be used to gain **access to a secured communication** without the sender or receiver being aware of the attack.

**Sniffer attack** : sniffer is an application or device that can **read, monitor, and capture network data** exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet.

Malware

Viruss and trojan horsa

Virus

The first and most common type of computer malware is a virus. **Viruses require human action to propagate and infect other computers**. For example, a virus can infect a computer when a victim opens an email attachment, opens a file on a USB drive, or downloads a file.

Viruses can:

* Alter, corrupt, **delete files**, or erase entire drives.
* Cause computer **booting issues**, and corrupt applications.
* Capture and **send sensitive information** to threat actors.
* Access and use **email accounts** to spread.
* Lay dormant until summoned by the threat actor

**Boot sector virus** : attacks boot sector,file partion, file system

**Firmware viruss** : attacks device firmware

**Macro virus** : Virus uses the MS Office or other applications macro feature maliciously.

**Program virus** : Virus inserts itself in another executable program.

**Scritp viru**s : Virus attacks the OS interpreter which is used to execute scripts.

Trojan horse :

Threat actors use Trojan horses to compromise hosts. **A Trojan horse is a program that looks useful** but also carries malicious code. Trojan horses are often provided with free online programs such as computer games. Unsuspecting users download and install the game, along with the Trojan horse.

**Several types of trojan horses :**

* **Remote access** : Trojan horse enables unauthorized remote access.
* **Data-sending** : trojan horse provides , the threat actor with sensitive data, such as passwords.
* **Destructive : c**orrupts or deletes files
* **Proxy :** use a victim device as a source device to attack and preform illegal activities
* **ftp :** enables unauthorized file transfer services on end devices
* **security software disabler** : stops antivirus programs or firewalls
* **dos** : slows or halts network activity
* **keylogger :** steal confidential info such as credit card

Viruses and Trojan horses are only two types of malware that threat actors use. There are many other types of malware that have been designed for specific purposes.

Other types of malware :

**Adware** : usually distributed **by downloading online software**., **Pop-up windows** may be difficult to control as new windows can pop-up faster than the user can close them

**Ransomware** : **denies user access to their files bc of encryption** by the threat actor and ask for ransom for the key , users without up to date backups must pay ransom, payment usually crypto

**Rootkit** : **admin level access to a computer, difficult to detect** , They can provide a backdoor to threat actors giving them access to the PC, and allowing them to upload files, and install new software to be used in a DDoS attac,

**Spyware** : similar to **addware, but used to gather information about the user and send to** threat actors without the user’s consent., Spyware can be a low threat, gathering browsing data, or it can be a high threat capturing personal and financial information.

Worm : worm is a self-replicating program that propagates automatically without user actions by exploiting vulnerabilities in legitimate software**. The intent of a worm is usually to slow or disrupt network operations.**

Common network attacks :

Reconnaissance attack :

Reconnaissance = means gather info about the enemy doel om de zwakheden te vinden

Threat actors use reconnaissance (or recon) attacks to **do unauthorized discovery and mapping of systems, services, or vulnerabilities. Recon attacks precede access attacks or DoS attacks.**

Some of the techniques used by malicious threat actors to conduct reconnaissance attacks are described in the table:

**Preform an info query of a target :** initial info about the target vb tool googlesearch

**Initate a ping sweep of the target network** : reveals target network address . with ping sweep you can know which ip address is active

**Intitate a port scan of active ip addresses** : to deteminis which port or sercices are available ; vb netscan

**Run vulnerability scannners** : to determine the type and version of the application and operating system that is running on the host. vb Nipper

**Run exploitation tools** : discover vulnerable services that can be exploited. Vb metaspoit

Access attacks :

Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services.

**Doel =**> retrieve data, gain access, or to escalate access privileges to administrator status.

**Password Attacks** : hreat actor attempts to discover critical system passwords using various methods. Password attacks are very common and can be launched using a variety of password cracking tools.

**Spoofing attacks :** , the threat actor device **attempts to pose as another device by falsifying** data. Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing. These spoofing attacks will be discussed in more detail later in this module

**Other Access attacks include:**

* **Trust exploitations** : threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target.
* **Port redirections :** In a port redirection attack, a threat actor uses a compromised system as a base for attacks against other targets. The example in the figure shows a threat actor using SSH (port 22) to connect to a compromised Host A
* **Man-in-the-middle attacks : is al uitgelegd**
* **Buffer overflow attacks :** In a buffer overflow attack, the threat actor exploits the buffer memory and overwhelms it with unexpected values. This usually renders the system inoperable, creating a DoS attac

Social engineering attack :

Social engineering is an access attack that attempts **to manipulate individuals** into performing actions or divulging confidential information. Some social engineering techniques are **performed in-person while others may use the telephone or internet.**

**Social engineers often rely on people’s willingness to be helpful. They also prey on people’s weaknesses.**

**social engineers techniek :**

**pretexting** : A threat actor **pretends to need personal** or financial data to confirm the identity of the recipient

**phishing** : A threat actor sends fraudulent email **which is disguised as being from a legitimate**, trusted source to trick the recipient into installing malware on their device

**spear phising** : A threat actor creates a targeted phishing attack tailored **for a specific individual** or organization.

**Spam :** Also **known as junk mail**, this is unsolicited email which often contains harmful links, malware, or deceptive content.

**Baiting :** A threat actor leaves a **malware infected flash drive in a public location.** A victim finds the drive and unsuspectingly inserts it into their laptop, unintentionally installing malware

**Impersonation :** This type of attack is where a **threat actor pretends to be someone they are** not to gain the trust of a victim

**Tailgating :** This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area.

**Shoulder surfing :** This is where a threat actor **inconspicuously looks over someone’s shoulder to steal their passwords or other information.**

**Dumpster diving** : This is where a threat actor rummages through **trash bins to discover confidential** documents.

**he Social Engineering Toolkit (SET) was designed to help white hat hackers and other network security professionals create social engineering attacks to test their own networks.**

**DoS and DDoS Attacks**

Afbeelding met tekst, Lettertype, lijn, schermopname

Automatisch gegenereerde beschrijving

DoS attacks are a major risk because they interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled threat actor.

A Distributed DoS Attack (DDoS) : s **similar to a DoS attack, but it originates from multiple, coordinated sources**. making it a zombie that can communicate with the CnC system. The collection of zombies is called a botnet. **When ready, the threat actor instructs the CnC system to make the botnet of zombies carry out a DDoS attack.**

**IP Vulnerabilities and Threats**

IPv4 and IPv6

IP does not validate whether t**he source IP address contained in a packet actually came from that source**. For this reason, threat actors can send packets using a spoofed source IP address.

**Icmp attacks** : Threat actors use Internet Control Message **Protocol (ICMP)** echo packets (pings) to **discover subnets and hosts on a protected network**, to generate DoS flood attacks, and to alter host routing tables.

**Amplification and reflection attacks** : Threat actors attempt **to prevent legitimate users** from **accessing information or services using DoS** and DDoS attacks.

**Address spoofing attacks :** Threat actors spoof the source IP address in an IP packet to perform blind **spoofing or non-blind spoofing**.

**Man in the middle attack** :  or alter packets and forward them to their original destination.

**Session hijacking** : Threat actors gain access to the physical network, and then use an MITM attack to hijack a session.

**ICMP Attacks**

Threat actors use ICMP for **reconnaissance an**d scanning attacks. They can launch information-**gathering attacks to map out a network topology,** discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall. Threat actors also **use ICMP for DoS attacks.**

**Networks should have strict ICMP access control list (ACL) filtering on the network edge to avoid ICMP probing from the interne**

Common ICMP messages of interest to threat actors are listed in the table:

**CMP echo request and echo reply :** This is used to **perform host verification** and DoS attacks.

**ICMP unreachable** : This is used to perform network reconnaissance and scanning attacks.

**ICMP mask reply** : This is used to map an internal IP network.

**ICMP redirects :** This is used to lure a target host into sending all traffic through a compromised device and create a MITM attack.

**ICMP router discovery :** This is used to inject bogus route entries into the routing table of a target host.

Amplification and Reflection Attacks

Threat actors often use amplification and reflection techniques to create DoS attacks. The example in the figure illustrates how an amplification and reflection technique called a Smurf attack is used to overwhelm a target host.

Afbeelding met tekst, schermopname, diagram, lijn

Automatisch gegenereerde beschrijving

: Newer forms of amplification and reflection attacks such as DNS-based reflection and amplification attacks and Network Time Protocol (NTP) amplification attacks are now being used.

Address Spoofing Attacks

IP address spoofing attacks occur when a threat actor **creates packets with false source IP address** information to either hide the identity of the sender, or to pose as another legitimate user. The threat actor can then gain access to otherwise inaccessible data or circumvent security configurations. Spoofing is usually incorporated into another attack such as a Smurf attack.

**Non-blind spoofing** : can see the traffic between the host and the target. the threat actor uses non-blind spoofing **to inspect the reply packet from the target victim**. Non-blind spoofing determines the **state of a firewall and sequence-number prediction.** It can also hijack an authorized session.(has some knowledge about the target system)

**Blind spoofing** : The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks**.(has no knowledge of the targer system**)

In both cases, the term "spoofing" generally refers to the act of pretending to be someone or something else to gain unauthorized access or deceive a system. Common examples include IP spoofing, email spoofing, or MAC address spoofing.

TCP and UDP Vulnerabilities

TCP Services

**Reliable delivery : TCP** incorporates acknowledgments to guarantee delivery, instead of relying on upper-layer protocols to detect and resolve errors. If a timely acknowledgment is not received, the sender retransmits the data.

**Flow control** : TCP implements flow control to address this issue. Rather than acknowledge one segment at a time, multiple segments can be acknowledged with a single acknowledgment segment.

**Stateful communication :** TCP stateful communication between two parties occurs during the TCP **three-way handshake**. Before data can be transferred using TCP, a three-way handshake opens the TCP connection, as shown in the figure. **If both sides agree to the TCP connection, data can be sent and received by both parties using TCP.**

**Afbeelding met tekst, schermopname, diagram, lijn

Automatisch gegenereerde beschrijving**

TCP Attacks

TCP SYN Flood Attack : The TCP SYN Flood attack exploits **the TCP three-way handshake.** The figure shows a threat actor continually **sending TCP SYN session** request packets with **a randomly spoofed source IP address to a targe**t. The target device **replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet**. Those responses never arrive. Eventually the target host is overwhelmed with half-open TCP connections, and **TCP services are denied to legitimate users**.

Afbeelding met tekst, schermopname, diagram, ontwerp

Automatisch gegenereerde beschrijving

**TCP Reset Attack** : TCP reset attack can be **used to terminate TCP communications** between two hosts. TCP can terminate a connection in a civilized (i.e., normal) manner and uncivilized (i.e., abrupt) manner.

**TCP Session Hijackin : TCP session hijacking is another TCP vulnerability. Although difficult to conduct, a threat actor takes over an already-authenticated host as it communicates with the target. The threat actor must spoof the IP address of one host, predict the next sequence number, and send an ACK to the other host. If successful, the threat actor could send, but not receive, data from the target device.**

**UDP Segment Header and Operation**

UDP is commonly used by DNS, TFTP, NFS, and SNMP. UDP is a connectionless transport layer protocol. It has much lower overhead than TCP because **it is not connection-oriented** and does not offer the sophisticated retransmission, sequencing, and flow control mechanisms that provide reliability. The UDP segment structure, shown in the figure, is much smaller than TCP’s segment structure.

Overhead means extra data

UDP Attacks :

UDP is not protected by any encryption. he lack of encryption means that anyone can see the traffic, , and send it on to its destination. Changing the data in the traffic will alter the 16-bit checksum, , but the checksum is optional and is not always used. When the checksum is used, the threat actor can create a new checksum based on the new data payload, and then record it in the header as a new checksum. The destination device will find that the checksum matches the data without knowing that the data has been altered. This type of attack is not widely used.

**UDP Flood Attacks** :

A program sends a flood of UDP packets from a spoofed host to a server on the subnet sweeping through all the known UDP ports looking for closed ports. This will cause the server to reply with an ICMP port unreachable message

IP Services

ARP Vulnerabilities

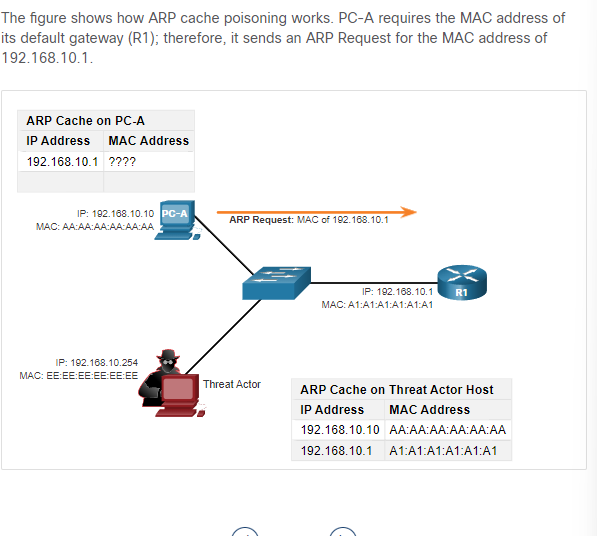
Earlier in this module you learned about vulnerabilities with IP, TCP and UDP. **The TCP/IP protocol suite was never built for security**. Therefore, **the services that IP** uses for addressing functions such as ARP, DNS, and DHCP, are **also not secure**, as you will learn in this topic.

**Hosts broadcast an ARP Request** to other hosts on the segment to determine the MAC address of a host with a particular IP address. All hosts on the subnet receive and process the ARP Request. The host with the matching IP address in the ARP Request sends an ARP Reply.

Any client can send an **unsolicited ARP Reply called a “gratuitous ARP**.” This is often done when a device **first boots up** to inform all other devices on the local network of the new device’s MAC address. When a host sends a gratuitous ARP, other hosts on the subnet store the MAC address and IP address contained in the gratuitous ARP in their ARP tables.

This feature of ARP also **means that any host can claim to be the owner of** any IP or MAC. **A threat actor** **can poison the ARP cache** of devices on the local network, **creating an MITM attack** to redirect traffic. The goal is to target a victim host, and have it change its default gateway to the threat actor’s device. This positions the threat actor in between the victim and all other systems outside of the local subnet.

ARP Cache Poisoning



Extra info : De router is Meestal altijd de default gateway van een switch

De pc vraag de mac van r1 en r1 doet een arp reply naar de pc maar de threat actror stuur 2 spoofen gratuitous arp replies en gebruikt zijn eigen mac address op de indicated destination ip address. Hierdoor krijgt de pc een arp update en dan word default gate van pc de address van de threat actor. R1 updates zijn arp tabel waardoor r1 de mac addres van de pc de mac addres van threat actor word

Afbeelding met tekst, schermopname, diagram, ontwerp

Automatisch gegenereerde beschrijving

**Passive ARP poisoning** is where threat actors steal confidential information. **Active ARP poisoning** is where threat actors modify data in transit, or inject malicious data.

Dns attack :

**The Domain Name System** (DNS) protocol defines an automated service that matches resource names, such as www.cisco.com, with the required numeric network address, such as the IPv4 or IPv6 address. It includes the format for queries, responses, and data and uses resource records (RR) to identify the type of DNS response.

DNS attacks include the following:

* DNS open resolver attacks
* DNS stealth attacks
* DNS domain shadowing attacks
* DNS tunneling attacks

DNS Open Resolver Attacks :

Many organizations use the services of publicly open DNS servers such as GoogleDNS (8.8.8.8) to provide responses to queries. This type of DNS server is called an open resolver. **A DNS open resolver answers queries from clients outside of its administrative domain**. DNS open resolvers are vulnerable to multiple malicious activities described in the table

Extra info : spoofed mean to a situation where something is manipulated or falsified to deceive someone

**DNS Resolver Vulnerabilities :**

* **DNS cache poisoning attacks** : Threat actors send spoofed, falsified record resource (RR) information to a DNS resolver to redirect users from legitimate sites to malicious sites
* **DNS amplification and reflection attacks** : Threat actors **use DoS or DDoS attacks** on DNS open resolvers to increase the volume of attacks and to hide the true source of an attack
* **DNS resource utilization attacks** : A DoS attack that **consumes the resources of the DNS open resolvers**. This DoS attack consumes all the available resources to negatively affect the operations of the DNS open resolver. The impact of this DoS attack may require the DNS open resolver to **be rebooted or services to be stopped and restarted.**

**DNS Stealth Attacks**

**Extra info ip address mapping:** Here's a simple analogy: think of IP addresses like phone numbers, and IP address mapping is like having a contact list that associates each phone number with a person's name. When you want to communicate with someone, you look up their name (IP address) in your contact list to find their phone number (physical location on the network).

To hide their identity, threat actors also use the DNS stealth techniques :

* **Fast Flux :** Threat actors use this technique to hide their phishing and malware delivery sites behind a quickly-changing network of compromised DNS hosts.
* **Double IP Flux : Threat actors use this technique to rapidly change the hostname to IP address mappings** and to also change the authoritative name server. This increases the difficulty of identifying the source of the attack.
* **Domain Generation Algorithms : Thr**eat actors use this technique in malware to randomly generate domain names that can then be **used as rendezvous points** to their command and control (C&C) servers.

**DNS Domain Shadowing Attacks :** Domain shadowing involves the threat actor gathering domain account credentials in order to silently create multiple sub-domains to be used during the attacks. These subdomains typically point to malicious servers without alerting the actual owner of the parent domain.

DNS Tunneling

**Certainly! DNS tunneling is a technique used to encode non-DNS traffic within DNS queries and responses. In simpler terms, it's a method of sending data covertly by hiding it within the DNS protocol.**

In essence, DNS tunneling is a method of using the DNS protocol to carry information beyond its intended use of domain name resolution, and it can be both a legitimate and a security concern depending on the context in which it is used.

**To stop DNS tunneling**, the network administrator must **use a filter that inspects DNS traffic**. Pay close attention to DNS queries that are longer than average, or those that have a suspicious domain name. DNS solutions, like Cisco OpenDNS, block much of the DNS tunneling traffic by identifying suspicious domains.

DHCP

Afbeelding met tekst, schermopname, software, Webpagina

Automatisch gegenereerde beschrijving

DHCP Attacks

**DHCP Spoofing Attack :** rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. A rogue server can provide a variety of misleading information:

Wrong default gateway, wrong dns server, wrong ip address

Afbeelding met tekst, Lettertype, Elektrisch blauw, schermopname

Automatisch gegenereerde beschrijving

De client kiest voor de rogue dhcp over de echte dhcp server omdat de rogue dhcp offer als eerste aankwam.

Network Security Best Practices

Confidentiality, Integrity, and Availability => cia

**Confidentiality** - **Only authorized individuals**, entities, or processes can access sensitive information. It may require using cryptographic encryption algorithms such as AES to encrypt and decrypt data.

**Integrity - R**efers to **protecting data from unauthorized alteration**. It requires the use of cryptographic hashing algorithms such as SHA.

**Availability** - **Authorized users must have uninterrupted access to important resources and data**. It requires implementing redundant services, gateways, and links

The Defense-in-Depth Approach

To ensure **secure communications across** **both public and private networks**, you must secure devices including routers, switches, servers, and hosts. Most organizations employ **a defense-in-depth approach to security.** This is also known as a layered approach. It requires a combination of networking devices and services working together. Consider the network in the figure.

Afbeelding met tekst, diagram, schermopname, lijn

Automatisch gegenereerde beschrijving

Vpn : secure encrypted tunnels

Asa firewall : internal traffic can go out and come back but external traffic cannot initiate connection to inside hosts

Ips : intrusion prevention system : monitors incoming and outgoing traffic looking for malware. If its recognized it will stop it immediately

Esa/wsa : email security appliance => filters spams ans suspicious mails, web security appliance=> filters suspicious internet malware sites

Aaa server : secure database of who is authorized to access ans manage network devices

Firewalls

**A firewall is a system, or group of systems, that enforces an access control policy between networks.** Click Play in the figure to view an animation of how a firewall operates.

**All firewalls share some common properties:**

* Firewalls are resistant to network attacks.
* Firewalls are the only transit points between internal corporate networks and external networks because all traffic flows through the firewall.
* Firewalls enforce the access control policy.

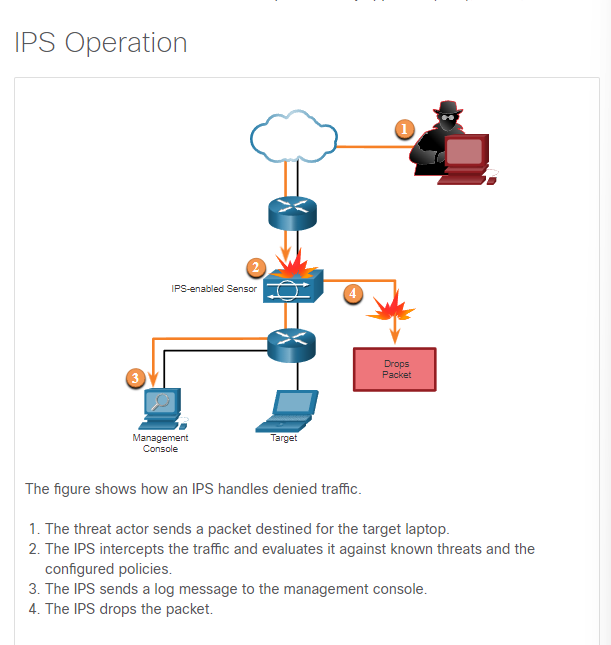
**There are several benefits of using a firewall in a network:**

* **They prevent the exposure of sensitive hosts, resources, and applications to untrusted users.**

**Afbeelding met tekst, schermopname, Lettertype, document

Automatisch gegenereerde beschrijving**

IPS



IDS and IPS technologies detect patterns in network traffic **using signatures**. A signature is a set of rules that an IDS or IPS uses to detect malicious activity. Signatures can be used to detect severe breaches of security, **to detect common network attacks, and to gather information.** IDS and IPS technologies can detect atomic **signature patterns (single-packet) or composite signature patterns (multi-packet).**

**Content Security Appliances :**

**Esa : The Cisco Email Security Appliance (ESA) is a special device designed to monitor Simple Mail Transfer Protocol (SMTP)** Cisco ESA is constantly updated by real-time feeds from the Cisco Talos, which detects and correlates threats and solutions by using a worldwide database monitoring system. This threat intelligence data is pulled by the Cisco ESA every three to five minutes.

Afbeelding met tekst, schermopname

Automatisch gegenereerde beschrijving

WsA :

**t helps organizations address the challenges of securing and controlling web traffic. The Cisco** WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, and reporting

**Cisco WSA provides complete control over how users access the internet**. Certain features and applications, such as chat, messaging, video and audio, can be allowed, restricted with time and bandwidth limits, or blocked, according to the organization’s requirements. The WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, web application filtering, and encryption and decryption of web traffic.

Afbeelding met tekst, schermopname

Automatisch gegenereerde beschrijving

Cryptography

Securing Communications

These are the four elements of secure communications:

* **Data Integrity -** Guarantees that the message was not altered
* **Origin Authentication** - Guarantees that the message is not a forgery and does actually come from whom it states
* **Data Confidentiality** - Guarantees that only authorized users can read the message.
* **Data Non-Repudiation** - Guarantees that the sender cannot repudiate, or refute, the validity of a message sent.

Data Integrity

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Hash Functions

**MD5 with 128-bit Digest** : D5 is a one-way function that produces a 128-bit hashed message**.MD5 should be avoided . sha-2 en 3 zijn aangeraden**

**SHA Hashing Algorithm : HA-1** creates a 160-bit hashed message and is slightly slower than MD5. SHA-1 has known flaws and is a legacy algorithm.

**SHA-2** : It includes SHA-224 (224 bit), SHA-256 (256 bit), SHA-384 (384 bit), and SHA-512 (512 bit). If you are using SHA-2, then the SHA-256, SHA-384, and SHA-512 algorithms should be used whenever possible.

**SHA-3 : SHA-3 includes SHA3-224 (224 bit), SHA3-256 (256 bit), SHA3-384 (384 bit), and SHA3-512 (512 bit**). it cannot be used to guard against deliberate changes that are made by a threat actor. hashing is vulnerable to man-in-the-middle attacks and does not provide security to transmitted data. To provide integrity and origin authentication, something more is required.want mitm kan de hash veranderen

: Hashing algorithms only protect against accidental changes and does not protect the data from changes deliberately made by a threat actor.

Origin Authentication

HMAC uses an additional secret key as input to the hash function.

Afbeelding met tekst, schermopname

Automatisch gegenereerde beschrijving

Hmac is Calculated using any cryptographic algorithm that combines a cryptographic hash function with a secret key.this defeats man in the middle attack

Data Confidentiality

There **are two classes of encryption used to provide data confidentiality.** These two classes differ in how they use keys.

**Symmetric encryption algorithms** such as **Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES)** are based on the premise that each communicating party knows **the pre-shared key**. Data confidentiality can also be ensured using **asymmetric algorithms, including Rivest, Shamir, and Adleman (RSA) and the public key infrastructure (PKI).**

**Gebruik aes in de plaats van des en 3des**

Symmetric Encryption

**Gebruikt dezelfde key** om te openen of encrypeten.

Symmetric encryption algorithms fall into two categories, block ciphers and stream ciphers.

**Block ciphers** encrypt data in **fixed-sized blocks**. . Examples of block ciphers include DES, and AES.

**Stream ciphers encrypt** data one bit or byte at a time in a continuous string.

Examples of stream ciphers includes RC4 and SEAL.

today, symmetric encryption algorithms are commonly used with VPN traffic

like any other type of encryption, the longer the key, the longer it will take for someone to discover the key.

Most encryption keys are between 112 and 256 bits

Afbeelding met tekst, schermopname, Lettertype, document

Automatisch gegenereerde beschrijving

Asymmetric Encryption

Asymmetric algorithms, also called public-key algorithms, a**re designed so that the key that is used for encryption is different from the key that is used for decryption,**

**Public key to encrypt and private key to decrypt**

Afbeelding met tekst, schermopname, diagram, ontwerp

Automatisch gegenereerde beschrijving

Asymmetric encryption can use key lengths between 512 to 4,096 bits.

Afbeelding met tekst, Lettertype, schermopname, algebra

Automatisch gegenereerde beschrijving

Asymmetric encryption duurd langer dan symmetric encryption

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

Diffie-Hellman

**Diffie-Hellman (DH) is an asymmetric mathematical algorithm. where two computers generate an identical shared secret key without having communicated before.**

Here are three examples of instances when DH is commonly used:

* **Data is exchanged using an IPsec VPN.**
* **Used when data is exchanged using an SSL or TLS VPN.**
* **SSH data is exchanged.**

**Afbeelding met tekst, schermopname, sap, ontwerp

Automatisch gegenereerde beschrijving**

Hoofdstuk : acl concepts

What is an ACL?

**Routers make routing decisions** based on information in the **packet header.** Traffic entering a router interface is **routed solely based on information within the routing table**. The router compares the destination IP address with routes in the routing table **to find the best match** and then forwards the packet based on the best match route. **That same process can be used to filter traffic using an access control list (ACL).**

An ACL is a series of IOS commands that **are used to filter packets based on information** found in the packet header. By default, **a router does not have any ACLs configured**. However, when an ACL is applied to an interface, the router performs the additional task of evaluating all network packets as they pass through the interface **to determine if the packet can be forwarded**

An ACL uses **a sequential list of permit or deny statements**, known as access control entries (ACEs).

Note: ACEs are also commonly called ACL statements(ace is a individual rule in the acl)

An ACE is an individual rule within an ACL. Each ACE specifies a particular set of conditions that must be met for the rule to be applied, along with an action to be taken if those conditions are met. The two most common actions are "permit" (allow the traffic) and "deny" (block the traffic).

Several tasks performed by routers require the use of ACLs to identify traffic . hier zijn de voorbeelden :

* Limit network traffic to increase network performance **vb prohibit video traffic**
* Provide traffic flow control **vb routing protocol traffic be limited to certain links only**
* Provide a basic level of security for network access v**b authorized users only**
* Filter traffic based on traffic type vb **acls to filter traffic by type**
* Screen hosts to permit or deny access to network **services vb acls to filter user access to services**
* Provide priority to certain classes of network traffic **vb voice traffic be forwarded as fast as possible to avoid any interruption.**

Packet Filtering

Packet filtering controls access to a network by analyzing the incoming and/or outgoing packets and forwarding them or discarding them based on given criteria. Packet filtering can occur at Layer 3 or Layer 4, as shown in the figure.

Afbeelding met tekst, schermopname, lijn, Rechthoek

Automatisch gegenereerde beschrijving

**Standard ACLs** - ACLs **only filter at Layer 3 using** the source IPv4 address only.

**Extended ACLs - ACLs filter at Layer 3 using the source and / or destination IPv4 address**. They can also filter at Layer 4 using TCP, UDP ports, and optional protocol type information for finer control.

ACL Operation

ACLs define the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router, and packets that exit outbound interfaces of the router.

Afbeelding met schermopname, tekst, Lettertype, logo

Automatisch gegenereerde beschrijving

: **ACLs do not act on packets that originate from the router itself.**

An **inbound ACL filters packets before they are routed to the outbound interface**. An inbound ACL is efficient because **it saves the overhead of routing lookups if the packet is discarded**. If the packet is **permitted b**y the ACL, **it is then processed for routing**. Inbound ACLs are best used to filter packets when the network attached to an inbound interface is the only source of packets that need to be examined.

**An outbound ACL** **filters packets after being routed**, regardless of the inbound interface. **Incoming packets are routed to the outbound interface a**nd then they are processed through the outbound ACL. **Outbound ACLs are best used when the same filter** will be applied to packets coming from **multiple inbound interfaces** before exiting the same outbound interface.

**here are the operational steps used when traffic has entered a router interface with an inbound standard IPv4 ACL configured.**

* The router extracts the source IPv4 address from the packet header.
* The router starts at the top of the ACL and **compares the source IPv4 address to each ACE** in a sequential order.
* **When a match is made**, the router carries out the instruction, either **permitting or denying** the packet, and the remaining ACEs in the ACL, if any, are not analyzed.
* If the source **IPv4 address does not match** any ACEs in the ACL, **the packet is discarded** because there is an implicit deny ACE automatically applied to all ACLs.

In het kort er word gekeken naar het pakket of het match met de ace rules van acl en als het match dat word er gekeken of het word permitted of denied. Als het niet match dan word het direct discarded.

**The last ACE statement of an ACL is always an implicit deny** that blocks all traffic. By default, this statement is automatically implied at the end of an ACL even though it is hidden and not displayed in the configuration.

Wildcard Masks in ACLs

This topic explains how ACL uses wildcard masks. **an IPv4 ACE uses a 32-bit wildcard mask to determine which bits of the address to examine for a match. Het word ook bij ospf gebruikt**

Wildcard masks use the following rules to match binary 1s and 0s:

* Wildcard mask bit 0 - Match the corresponding bit value in the address
* Wildcard mask bit 1 - Ignore the corresponding bit value in the address

Afbeelding met tekst, schermopname, nummer, Lettertype

Automatisch gegenereerde beschrijving

**De nullen is de match en de 1 is een ignore . dus 0.0.0.63. dan weet je de eerste 3 is een match en dat zet je de laatste getal om in binair en weet je dat 63 = 00111111 . in hier zie ook nullen dus de twee linksen nulles is een match de 1’en zijn een ignore.**

Wildcard Mask Types

**Using wildcard masks will take some practice. Refer to the examples to learn how the wildcard mask is used to filter traffic for one host, one subnet, and a range IPv4 addresses**

ACE that only permits the host with IPv4 address 192.168.1.1. Recall that “0” equals a match and “1” equals ignore. To match a specific host IPv4 address, a wildcard mask consisting of all zeroes (i.e., 0.0.0.0) is required.

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

he resulting ACE in ACL 10 would be access-list 10 permit 192.168.1.1 0.0.0.0.

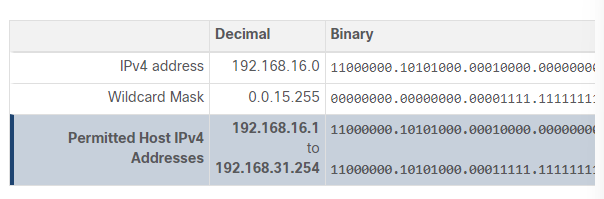
In this example, ACL 10 needs an ACE that permits all hosts in the 192.168.1.0/24 network. The wildcard mask 0.0.0.255

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

**access-list 10 permit 192.168.1.0 0.0.0.255.**

**In this example, ACL 10 needs an ACE that permits all hosts in the 192.168.16.0/24, 192.168.17.0/24, …, 192.168.31.0/24 networks. The wildcard mask 0.0.15.255 would correctly filter that range of addresses.**



access-list 10 permit 192.168.16.0 0.0.15.255.hiermee laat je de eerste 2 octet van de netwerk 192.168.16.0 toe en de voorlaatse alleen vanaf 16 begint toe

Wildcard Mask Calculation

Calculating wildcard masks can be challenging. One shortcut method is **to subtract the subnet mask from 255.255.255.255**

**Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving**

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

**192.168.3.32 /28 dan is wildcard mask : 0.0.0.15**

**Wildcard Mask Keywords**

**Keywords reduce ACL keystrokes and make it easier to read the ACE.**

* **host -** This keyword substitutes for **the 0.0.0.0 mask.** This mask states that all IPv4 address bits must match to filter just one host address.
* **any** - This keyword substitutes **for the 255.255.255.255** mask. This mask says to ignore the entire IPv4 address or to accept any addresses.

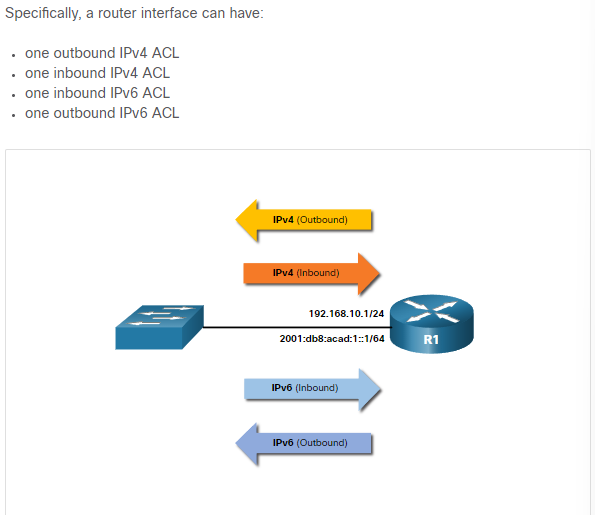
Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

Guidelines for ACL Creation

Limited Number of ACLs per Interface

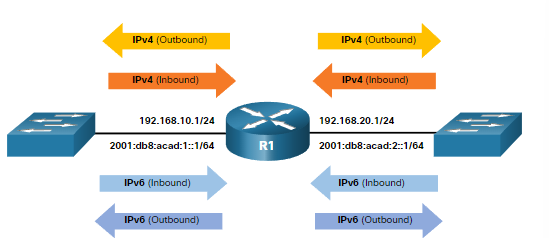
In a previous topic, you learned about how wildcard masks are used in ACLs. This topic will focus on the guidelines for ACL creation. There is a **limit on the number of ACLs that** can be applied on a router interface. For example, **a dual-stacked** (i.e., IPv4 and IPv6) router interface can **have up to four ACLs applied, as shown in the figure.**

****

Assume R1 has two dual-stacked interfaces that require inbound and outbound IPv4 and IPv6 ACLs applied. As shown in the figure, R1 could have up to 8 ACLs configured and applied to interfaces. Each interface would have four ACLs; two ACLs for IPv4 and two ACLs for IPv6. For each protocol, one ACL is for inbound traffic and one for outbound traffic.

**Assume R1 has two dual-stacked interfaces** that require inbound and outbound IPv4 and IPv6 ACLs applied. As shown in the figure**, R1 could have up to 8 ACLs** configured and applied to interfaces. Each **interface would have four ACLs**; two ACLs for IPv4 and two ACLs for IPv6. For each protocol, one ACL is for inbound traffic and one for outbound traffic.

: **ACLs do not have to be configured in both directions**. The number of ACLs and their direction applied to the interface will **depend on the security policy** of the organization

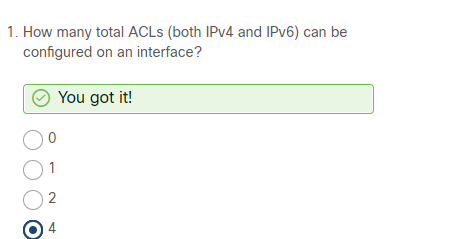


ACL Best Practices

Using **ACLs requires attention to detail** and great care. **Mistakes can be costly in** terms of downtime, troubleshooting efforts, and poor network service. Basic planning is required before configuring an ACL..

**The table presents guidelines that form the basis of an ACL best practices list**

* Base ACLs on the organizational security policies.
* Write out what you want the ACL to do.
* Use a text editor to create, edit, and save all of your ACLs
* Document the ACLs using the remark command.
* Test the ACLs on a development network before implementing them on a production network.



Standard and Extended ACLs

**Standard ACL (Standaard Toegangscontrolelijst):**

**Wat het doet**: Standard ACLs controleren het verkeer op basis van **de bron-IP-adressen** van **pakketten.**

**Waar het zich op rich**t: Standard ACLs kijken alleen naar **de bron-IP-adressen van de pakketten**.

**Gebruiksscenario:** Ze zijn vaak handig als je alleen verkeer wilt toestaan of blokkeren op basis van de bron-IP-adressen, zonder veel gedetailleerde criteria.

**Extended ACL (Uitgebreide Toegangscontrolelijst):**

**Wat het doet:** Extended ACLs controleren het verkeer **op basis van verschillende criteria, zoals bron- en doel-IP-adressen, poortnummers en het type protocol.**

**Waar het zich op richt**: Extended ACLs **kunnen specifieker zijn** en toestaan ​​of blokkeren op basis van verschillende kenmerken van het pakket, **zoals het type applicatie (dankzij poortnummers) naast de IP-adressen.**

**Gebruiksscenario**: Ze zijn handig als je gedetailleerdere controle wilt over welk verkeer wordt toegestaan ​​of geblokkeerd op basis van verschillende kenmerken van het pakket.

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

Numbered and Named ACLs

ACLs **number 1 to 99, or 1300 to 1999 are standard ACLs** while ACLs **number 100 to 199, or 2000 to 2699 are extended ACLs**, as shown in the output.

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

**Als je access-list ? => dan kun je zien voor welke nummer voor welke acl is.**

**Named ACLs**

Named ACLs is the preferred method to use when configuring ACLs. Specifically, standard and extended **ACLs can be named to provide information about the purpose of the ACL**. For example, naming an extended ACL FTP-FILTER is far better than having a numbered ACL 100.

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

**Guidelines voor named acls**

* Assign a name to identify the **purpose of the ACL**.
* Names can contain **alphanumeric characters**.
* Names **cannot c**ontain spaces or punctuation.
* It is suggested that the name be written in **CAPITAL LETTERS**.
* Entries can be added or deleted within the ACL.

Where to Place ACLs

The figure illustrates where standard and extended ACLs should be located in an enterprise network. Assume the objective to prevent traffic originating in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network.

Afbeelding met schermopname, diagram, tekst, lijn

Automatisch gegenereerde beschrijving

Dus de extended moet bij zo dicht mogelijk bij de source of traffic komen dus bij dit vb moet je ervoor zorgen dat de source netwerk 192.168.10.0 niet kan komen aan de 192.168.30.0. hier zie je dat je standard acl kan gebruiken want je filter alleen de source addres. En de extended acls plaats je waar de destination is . de extende moet je plaatsen zo dicht mogelijk bij de source

**Als je de standard bij de source zet dan gaat alle pakketen gedropped worden maakt niet uit waar het naartoe moet want de standard weet alleen dat de source address 192.168.10.0 moet gedropped worden daarom zet je het best bij de destination zodat pakketen van 192.168.10.0 nog naar een andere netwerk kan gaan.**

**Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving**

Standard ACL Placement Example

**In the figure, the administrator wants to prevent traffic originating in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network.**

Afbeelding met tekst, schermopname, diagram, lijn

Automatisch gegenereerde beschrijving

**De acl op de seriele link s0/1/1 staat fout want de doel is om ervoor te zorgen dat 192.168.10.0 netwerk niet aan de 192.168.30.0 netwerk kan. Maar als je de standard acl op de s0/1/1 zet dan gaat het ook niet naar de 192.168.31.0 netwerk toe. En dat is fout**

**Je zet de standard acl het best op de g0/0/0 netwerk waardoor je het netwerk van 192.168.10.0 niet toe laat op de 192.168.31 netwerk maar de 192.168.10.0 kan wel nog naar de 192.168.31.0 toe.en dat is juist**

Extended ACL Placement Example

Extended ACL should be located as **close to the source as possible**. This prevents unwanted traffic from being sent across multiple networks only to be denied when it reaches its destination.

However, the organization can **only place ACLs on devices that they control**. Therefore, the extended ACL placement must be determined in the context of where organizational control extends.

In the figure, for example, **Company A wants to deny Telnet and FTP traffic to Company B’s 192.168.30.0/24 network from their 192.168.11.0/24 network while permitting all other traffic**

Afbeelding met tekst, schermopname, diagram, lijn

Automatisch gegenereerde beschrijving

Tip ; icon acl ziet er uit als een zeef

**R1 S0/1/0 interface (outbound**) - The extended ACL can be applied outbound on the S0/1/0 interface. However, **this solution will process all packets leaving R1 including packets from 192.168.10.0/24.slecht idee het is beter dat je deze weg doet**

**R1 G0/0/1 interface (inbound**) - The extended ACL can be applied inbound on **the G0/0/1 and only packets from the 192.168.11.0/24 network are subject to ACL processing on R1**. Because the filter is to **be limited to only those packets leaving the 192.168.11.0/24 network**, applying the extended ACL to G0/1 **is the best solution.**

Hoofstuk : nat for ipv4

NAT Characteristics

IPv4 Private Address Space

As you know, there are not **enough public IPv4 addresses to assign a unique address** to each device connected to the internet. **Networks are commonly implemented** **using private IPv4 addresses**, as defined **in RFC 1918. The** range of addresses included in RFC 1918 are included in the following table. It is very likely that the computer that you use to view this course is assigned a private address.

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

**These private addresses are used within an organization or site to allow devices to communicate locally.** However, because these addresses do not identify any single company or organization, private IPv4 addresses cannot be routed over the internet. To allow a device with a private IPv4 address to access devices and resources outside of the local network, **the private address must first be translated to a public address.**

NAT provides the translation of private addresses to public addresses, as shown in the figure. This **allows a device with a private IPv4 address to access resources outside of their private network**, **such as those found on the internet. N**AT, combined with private IPv4 addresses, has been the primary method of preserving public IPv4 addresses. A **single, public IPv4 address can be shared by hundreds, even thousands of devices, each configured with a unique private IPv4 address**

Afbeelding met tekst, schermopname, Lettertype, diagram

Automatisch gegenereerde beschrijving

Nat alleen nodig wanneer internal netwerk naar de internet gaat.dus het word toegepast op een router die tussen de internal netwerk en de internet staat

What is NAT

NAT has many uses, but its primary use is **to conserve public IPv4 addresses**. It does this by allowing networks to use **private IPv4 addresses internally and providing translation to a public address only when needed.** NAT has a perceived benefit of adding a degree of **privacy and security to a network,** because it hides internal IPv4 addresses from outside networks.

NAT-enabled routers can be configured with **one or more valid public IPv4 addresses**. These public addresses are known as the NAT pool. When an internal **device sends traffic out of the network,** the NAT-enabled router translates **the internal IPv4 address of the device to a public address from the NAT pool**. To outside devices, all traffic entering and exiting the network appears to have a public IPv4 address from the provided pool of addresses.

A NAT router typically operates at the border of a stub network. **A stub network is one or more networks with a single connection to its neighboring network**, one way in and one way out of the network. In the example in the figure, R2 is a border router. As seen from the ISP, R2 forms a stub network.

Afbeelding met tekst, schermopname, diagram, ontwerp

Automatisch gegenereerde beschrijving

When a device inside the stub network wants to communicate with a device outside of its network, the packet is **forwarded to the border router**. The border router performs **the NAT process, translating the internal private address of the device to a public, outside, routable address**.

**! A stub network is a network that has only one route in or out, meaning it has only one connection to another network. In networking terms**

How NAT Works

Afbeelding met tekst, schermopname, diagram

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, diagram, ontwerp

Automatisch gegenereerde beschrijving

From private to public and from puclic to private

NAT Terminology

In NAT terminology, the inside network is the set of networks that is subject to translation. The outside network refers to all other networks.

**NAT includes four types of addresses:**

* Inside local address
* Inside global address
* Outside local address
* Outside global address

When determining which type of address is used, **it is important to remember that NAT terminology is always applied from the perspective of the device with the translated address**:

**Inside address** - The address of the **device which is being translated by NAT.**

**Outside address** - The address of the destination device.

**NAT also uses the concept of local or global with respect to addresses:**

* **Local address - A local** address is any address that appears on the inside portion of the network.
* **Global address** - A global address is any address that appears on the outside portion of the network

Afbeelding met tekst, schermopname, diagram, Lettertype

Automatisch gegenereerde beschrijving

**Inside local(IL) :** addres in internal network,en de device dat word vertaald

**Outside local (OL):** destination address en addres in internal portion of the network

**Inside global (IG):** address dat word vertaald , outside portion of the network

**Outside global (OG**): destination address , outside portion of the network

OEFENING :

**Van 192.168.10.10 naar de 209.165.201.1**

* **IL = 192.168.10.1**
* **OL = 209.165.201.1**
* **IG = 209.165.201.226**
* **OG = 209.165.201.1**

Types of NAT

Static NAT

Static NAT uses a one-to-one mapping of local and global addresses. These mappings are configured by the network administrator and remain constant.

In the figure, R2 is configured with static mappings for the inside local addresses of Svr1, PC2, and PC3. When these devices send traffic to the internet, **their inside local addresses are translated to the configured inside global addresses. To outside networks, these devices appear to have public IPv4 addresses.**

**Afbeelding met tekst, schermopname, diagram

Automatisch gegenereerde beschrijving**

**Static NAT is particularly useful for web servers or devices that must have a consistent address that is accessible from the internet, such as a company web server VB GOOGLE IS 8.8.8.8**

It is also useful for devices that must be accessible by authorized personnel when offsite, but not by the general public on the interne

**For example, a network administrator from PC4 can use SSH to gain access to the inside global address of Svr1 (209.165.200.226). R2 translates this inside global address to the inside local address 192.168.10.10 and connects the session to Svr1.**

Dynamic NAT

**Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis**

Afbeelding met tekst, schermopname, diagram

Automatisch gegenereerde beschrijving

Port Address Translation

**Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.**

**With PAT, multiple addresses can be mapped to one or to a few addresses, because each private address is also tracked by a port number**. When a device initiates a **TCP/IP session, it generates a TCP or UDP source port value**, or a specially assigned **query ID for ICMP, to uniquely identify the session.** When the NAT router receives a packet from the client, it uses its source port number to uniquely identify the specific NAT translation.

PAT ensures that devices use a **different TCP port number for each session with a server** on the internet. When a response **comes back from the server, the source port number, which becomes the destination port number on the return trip**, determines to which device the router forwards the packets. The PAT process also validates that the incoming packets were requested, thus adding a degree of security to the session

Afbeelding met tekst, diagram, schermopname, Lettertype

Automatisch gegenereerde beschrijving

**DE :155 is de poortnummer op die manier weet de server waar ze het moet terug sturen. De source ipaddress heef een vershillend poort nummer maar wnr de router de translation doet dan krijgt de public ip ook de sourcepoort nummer mee :**

**Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving**

Next Available Port

In the previous example, the **client port numbers, 1331 and 1555, did not change at the NAT-enabled** router. This is not a very likely scenario, because there is a good chance that these port numbers may have already been attached to other active sessions

**PAT attempts** to **preserve the original source por**t. However, if the original source port is already used, PAT assigns the first available port number starting from the beginning of the appropriate port group 0-511, 512-1,023, or 1,024-65,535. When there are no more ports available and there is more **than one external address in the address pool, PAT moves to the next address to try to allocate the original source port**. This process continues until there are no more available ports or external IPv4 addresses

**Dus als er geen source poort is dan gaat pat naar de volgende addres met source en skipt de vorige die geen source poort heeft.**

**Afbeelding met tekst, Lettertype, wit, ontvangst

Automatisch gegenereerde beschrijving**

**In de internal address mag de poortnummer hetzelfde zijn maar bij public address moet het anders zijn zodat het waar het pakket van komt als het moet terug sturen anders kan het naar de verkeerde device worden gestuurd.**

NAT and PAT Comparison

**Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving**

Packets without a Layer 4 Segment

What about IPv4 packets carrying data other than a TCP or UDP segment? These packets do not contain a Layer 4 port number. PAT translates most common protocols carried by IPv4 that do not use TCP or UDP as a transport layer protocol. The most common of these is ICMPv4. Each of these types of protocols is handled differently by PAT. For example, ICMPv4 query messages, echo requests, and echo replies include a Query ID. ICMPv4 uses the Query ID to identify an echo request with its corresponding echo reply. The Query ID is incremented with each echo request sent. PAT uses the Query ID instead of a Layer 4 port number.

NAT Advantages and Disadvantages

Advantages of NAT

* **pat**
* **NAT increases the flexibility of connections to the public network**
* **NAT provides consistency for internal network addressing schemes**
* **Using RFC 1918 IPv4 addresses, NAT hides the IPv4 addresses of users and other devices. Some people consider this a security feature; however, most experts agree**

**Nat does apply security features**

Disadvantages of NAT

* One disadvantage of using NAT is related to network performance, particularly for real time protocols such as VoIP. NAT increases forwarding delays because the translation of each IPv4 address within the packet headers takes time
* The forwarding delays caused by the NAT process becomes more of an issue as the pools of public IPv4 addresses for ISPs become depleted. this process of two layers of NAT translation is known as **Carrier Grade NAT (CGN)=> customer routre translate ip to network of isp and then the isp translate the ip again to a public ip**
* Another disadvantage of using NAT is that end-to-end addressing is lost.: some applications do not work with NAT. For example, some security applications, such as digital signatures, fail because the source IPv4 address changes before reaching the destination
* End-to-end IPv4 traceability is also lost.bc ip keeps changing
* **Using NAT also complicates the use of tunneling protocols**, such as IPsec, because NAT modifies values in the headers, causing integrity checks to fail.

Static nat configuration

Afbeelding met tekst, schermopname, diagram, lijn

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

De eerste stap bij de foto is de web internal netwerk en de extrenal is de internet met een client.Dus de webser geef je public ip en vervolgen doe je ook nat op de inbound en outboun interfacesen geef je ook de interfaces een ipaddres zoals bij routing. Je hebt alleen nat gedaan op de webserver. De rest van de config was routing zodat het weet waar het naartoe moet

Afbeelding met tekst, elektronica, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Dynamic NAT

Afbeelding met tekst, schermopname, diagram, lijn

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Je maakt public ipaddress en zet ze in de pool

Afbeelding met tekst, schermopname, Lettertype, ontwerp

Automatisch gegenereerde beschrijving

Afbeelding met tekst, Lettertype, schermopname, Graphics

Automatisch gegenereerde beschrijving

Voegt acl in de nat

Afbeelding met tekst, Lettertype, schermopname

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, ontwerp

Automatisch gegenereerde beschrijving

Vervolgen zeg je welke interface de outside is en welke inside is. En wnr je pakket stuur dan geeft het automatisch een public ip address .

PAT Scenario

Afbeelding met tekst, schermopname, Lettertype, diagram

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, scherm

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, document

Automatisch gegenereerde beschrijving

Bekijk de laatste delen van static nat,dynamic nat en pat opnieuw na op netacat

NAT64

Because many networks use both IPv4 and IPv6, **there needs to be a way to use IPv6 with NAT**. This topic discusses how IPv6 can be integrated with NAT. IPv6, with a 128-bit address, provides 340 undecillion addresses. **Therefore, address space is not an issue. IPv6** was developed with the intention of making NAT for IPv4 with translation between public and private IPv4 addresses unnecessary. **However, IPv6 does include its own IPv6 private address space, unique local addresses (ULAs).**

**Ipv6 doesn’t need nat**

**IPv6 unique local addresses (ULA) are similar to RFC 1918 private addresses in IPv4 but have a different purpose. ULA addresses are meant for only local communications within a site**

NAT for IPv6 is used in a much different context than NAT for IPv4. The varieties of NAT for IPv6 are used to transparently provide access between IPv6-only and IPv4-only networks,

**Dual-stack is** when the devices are running protocols associated with both IPv4 and IPv6. Tunneling for IPV6 is the **process of encapsulating an IPv6 packet inside an IPv4 packet**. This allows the IPv6 packet to be transmitted over an IPv4-only network.

NAT for IPv6 should not be used as a long-term strategy, but as a temporary mechanism to assist in the migration from IPv4 to IPv6

Pv6 including Network Address Translation-Protocol Translation (NAT-PT). NAT-PT has been deprecated by IETF in favor of its replacement, NAT64. NAT64 is beyond the scope of this curriculum.