



Practical Network Defense

Master's degree in Cybersecurity 2024-25

Network hardening

Angelo Spognardi
[*spognardi@di.uniroma1.it*](mailto:spognardi@di.uniroma1.it)

Dipartimento di Informatica
Sapienza Università di Roma



Agenda

- Introduction
- Management plane protection
- Control plane protection
- Data plane protection



Network hardening, i.e. protecting network devices

- Computer networks are composed of different types of devices.
- If even one of them is breached, the entire infrastructure can be compromised.
- The use of a methodology to protect network devices makes it possible to reduce the risk of violations and to limit the impact of anomalous events, whether they are voluntary (attacks) or involuntary (human errors or failures).

Three scopes of action

- Management plane
 - The scope of network device management
 - It consists of an administrator's protocols and tools to configure, monitor, or access a network device (e.g., SSH, SNMP, NTP).
 - Breaches in this area can be caused by overly simple passwords or insecure protocols, resulting in unauthorized access or loss of access to the device.
- Control plane
 - The scope of support for the operation of network devices
 - It consists of the protocols and mechanisms devices use to perform their tasks (e.g., routing protocols).
 - Violations in this area are usually caused by unauthorized data exchange with the device, resulting in loss of performance (denial of service).
- Data plane
 - The scope of operation of network devices
 - It corresponds to the traffic forwarded by network devices (be they switches, routers, or firewalls) and the paths that appliances choose for individual packets.
 - Violations in this area are usually caused by external events (congestions), malicious interventions (spoofing, redirect, hijacking, etc.), and failures and can result in the alteration of packet paths and a block of network services.



Protection must occur at all scopes

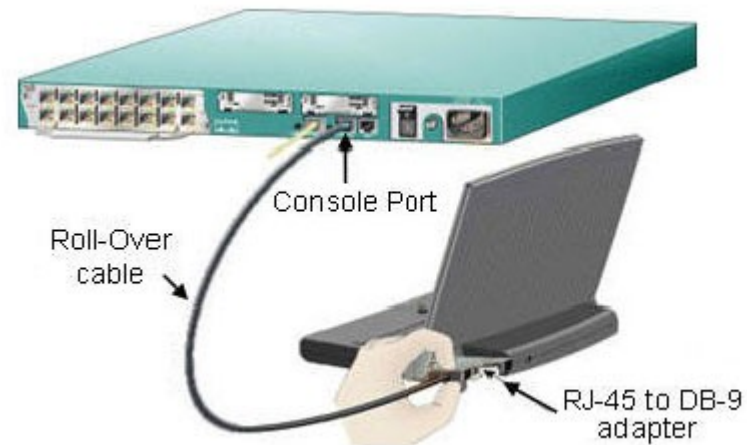
- In all the three areas of action of the network devices it is possible to have violations
- The three areas are closely linked, as anomalies in one can be reflected in the others.
- It is important, therefore, to adopt best practices to protect devices in all three areas.



Management plane protection

Appliance access protection

- Access to a device is the first step in configuring its operation and determining its behavior.
- Suppose the access occurs in person (with a serial terminal or a laptop connected to the console port). The risk is reduced since the access is usually restricted physically (access to the room where the device is).
- Suppose access can also be done remotely (through the network itself, using a virtual terminal, such as SSH or telnet). In that case, the risk is higher since anyone who can send traffic that reaches the device can claim to be a network administrator.
- Access to a device also allows access to other network devices' monitoring and status management functions, usually through the SNMP protocol.





Password policy

- Passwords are the simplest and most widely used form of authentication
- It is good to use passwords that are difficult to guess, for example, by employing:
 - passwords that are at least eight characters long
 - Devices can often force you to use a minimum number of characters for a password
 - passwords that are combinations of alphanumeric, upper and lower case characters, punctuation marks, and spaces are often used to create passphrases, i.e., passwords consisting of multiple words, usually not logically related
 - passwords that are changed frequently
 - passwords that are not overly complex, perhaps complicated to remember, requiring transcription to be used

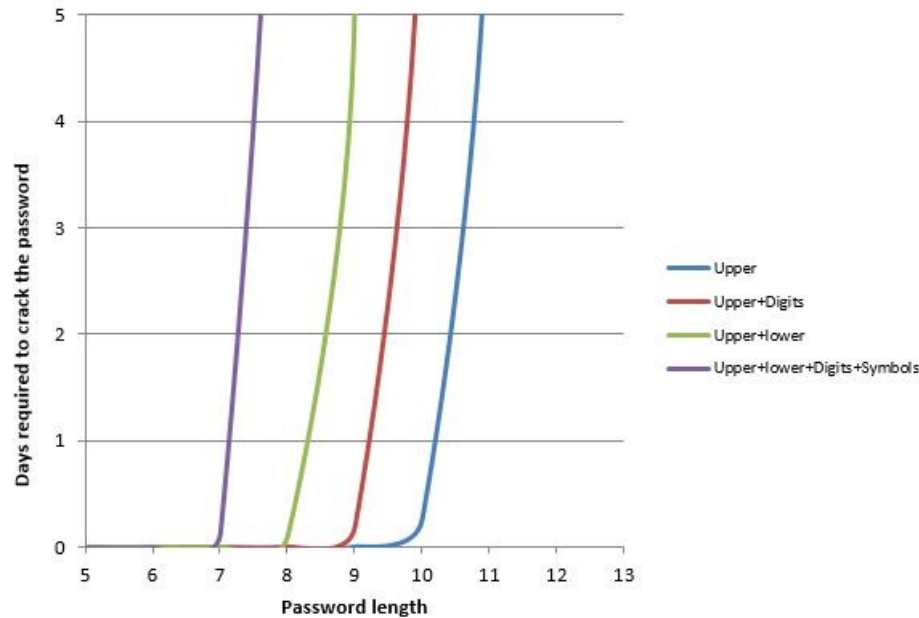


Brute force protection

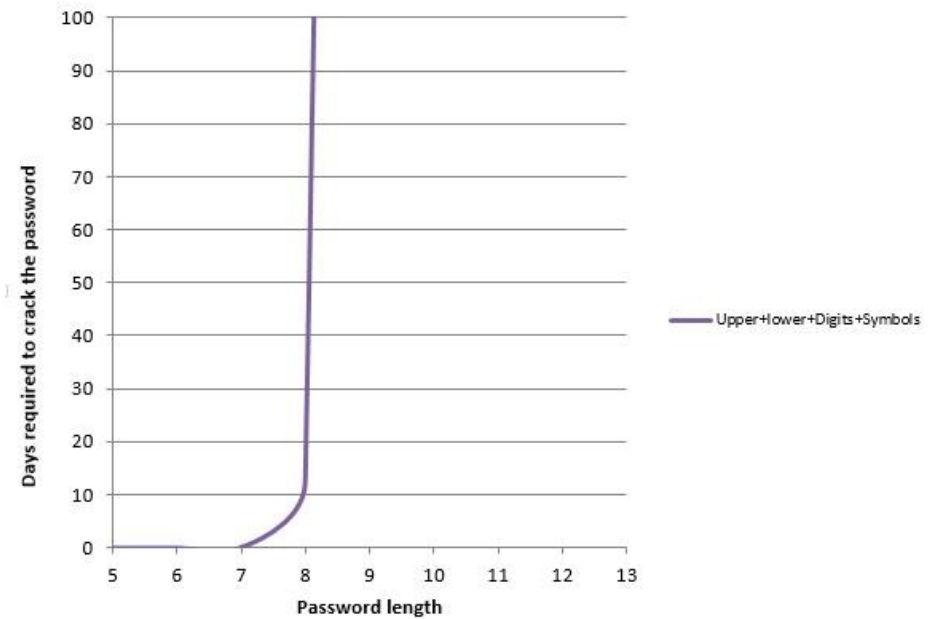
- The use of different character types and a minimum length ensures that the password search space is enormous and such that a brute force attack is challenging to accomplish
- An attacker will guess a password with only two lower case letters in $2^{12}=441$ attempts.
- With an eight-character password of upper and lower case letters, the attacker will guess numbers and symbols in $(21+21+10+36)^8=3.6*10^{15}$ attempts, or more than 3 million billion attempts.
- It is a good idea to configure the devices so that they can
 - store passwords in an encrypted way
 - temporarily block accounts for which the password is wrong three times in a row, notifying the incident in the logs

Password complexity

Example 2 - Modifying the Charset



Example 3 - Enforcing Password Length



<https://www.coresecurity.com/blog/the-exponential-nature-of-password-cracking-costs>



Use the AAA principle

- AAA is the principle of reducing unauthorized access to resources.
- It provides for identifying users and allowing them access only to those components for which they are authorized, keeping a record of their actions.
- **Authentication:** verifying the identity of a user
 - By user name and password, by token or similar
- **Authorization:** verify if a user is authorized to act on a system
 - The association between users and permissions can be done in different ways. The best known is RBAC, Role-Based Access Control, which considers the presence of different roles in the system, or groups of users with the same permissions (e.g., administrator, junior administrator, controller, and so on)
 - In RBAC, each user is associated with one or more roles, and each role has a set of permissions on system objects
- **Accounting/auditing:** store the details (e.g., time, duration, command used, and so on) of each action taken by each user in a permanent, unalterable log
 - Usually, network devices can send information to different destinations, such as a terminal, an SNMP server, or a Syslog server.

Use centralized solutions

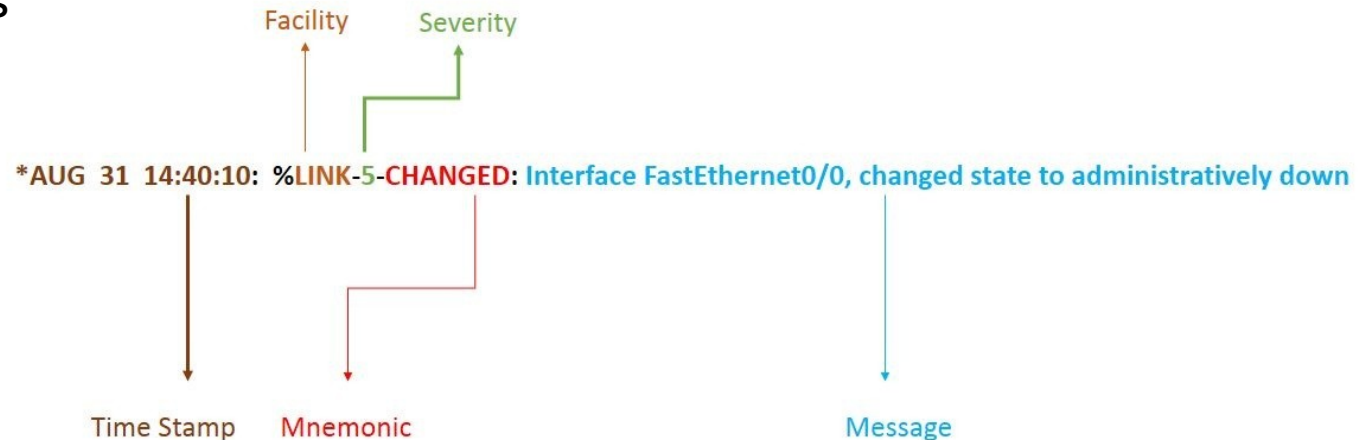
- Often, it is possible to configure solutions that concentrate AAA functions in a single point in network devices, for example, an ACS, Access Control Server.
- This allows you to have a centralized point from which to manage all the devices on the network.
 - The network devices (switches or routers) connect to the server and interact with it every time they need to verify the identity of a user trying to access it, the user's permissions, and record the actions it performs.
- Usually, these functions use specific protocols for managing users, passwords, permissions, authentication and authorization checks, and so on.
 - Examples are RADIUS for user access and TACACS+ for administrator access.
- The alternative to centralized solutions is the local solution, where each device has its own set of users, passwords, and permissions.
 - This solution is often used to overcome the problems that would arise if the authentication server was temporarily unavailable.

Use a reliable NTP server

- To have reliable Accounting and Auditing, all devices must know the current time correctly.
- For this purpose, the Network Time Protocol (NTP) is used.
- Usually, one of the devices on the network is designated as the reference NTP server, and all the other devices interact with it to synchronize with its time.
 - This device, in turn, can refer to another trusted NTP server, perhaps one that can be reached on the Internet, to receive the current time accurately.
- This ensures that all logs from all devices can be compared temporally.
- NTP version 3 is preferred since, unlike previous versions, it makes use of authentication and integrity verification mechanisms

Syslog

- syslog is a standard mechanism for generating log messages.
- Its structure allows you to efficiently separate the applications that generate logs from those that need to store them and those that need to consult them.
- The syslog server is critical to centrally collecting and managing logs
- One or more servers receive log messages from network devices representing noteworthy events



Correctly configure Syslog

- In Syslog, there are eight levels of criticality (severity) for individual log messages, ordered in such a way that levels with low values have higher criticality than those with high values:
 - 0 Emergencies, 1 Alert, 2 Critical, 3 Errors, 4 Warnings, 5 Notifications, 6 Informational, 7 Debugging
- Devices send log messages with a level less than or equal to the set criticality level.
 - This implies that a high level of lower criticality (such as 7, Debugging) will generate many more messages than a low level of higher criticality (such as 3, Errors).
- It is therefore essential:
 - to choose the appropriate level of criticality
 - For example, limit the use of Debugging only to the time required to solve a sudden anomaly
 - that the syslog server has an adequate log storage capacity, both in terms of space and computing capacity.
 - This is because the messages are transmitted and stored in plain text, with a timestamp (synchronized thanks to NTP) and with a text message



Remotely access using encryption

- Remotely accessing network devices must be done securely, i.e., using encryption protocols.
- For devices that require command-line configuration (CLI), avoid telnet, which is an unencrypted protocol since it involves sending a username and password without any protection.
 - Any intermediate node that separates the administrator and the remote device can potentially intercept the traffic and learn the credentials to access the device's configuration.
 - Administrators should only use telnet on an isolated channel (not intercepted) or within an encrypted tunnel (such as a VPN).
 - SSH should always be preferred, as it offers the same functionality as telnet but encrypts every packet exchanged between the device and the administrator. SSH version 2 is more secure than version 1.
- For devices that provide configuration through a graphical interface (GUI), similarly, should always be avoided the use of the HTTP protocol (clear) and prefer the use of HTTPS (encrypted).



Control plane protection



Protect control data

- It is essential to protect network devices to prevent them from using non-genuine information.
- This is done both to avoid unauthorized changes to the way traffic moves through the network and avoid overloading devices (denial of service attacks).
- For this purpose, we use
 - Control Plane Policing and Control Plane Protection, namely a series of measures that can limit the packets addressed directly to the devices and that require the use of their CPUs
 - routing protocols with authentication reduce the risk of using information for non-genuine traffic routing.



DoS protection

- The primary purpose of routers is to forward packets, so routers are very optimized.
 - Packet forwarding, based on routing table information, is almost always done from the cache, with zero impact on the CPU.
- Process packets directed to a router, instead, involve the CPU, possibly considerably.
 - E.g., routing table updates, management traffic (telnet, ssh, SNMP), service traffic (IGMP, DHCP), IP options that require processing by routers.
- Therefore, flooding routers with packets for processing can impact their performance and cause a DoS attack.
- The specific protections for the control plane limit this kind of traffic, setting up thresholds for the reception.
 - For example, x packets per second for protocol y, z traffic only from interface k, ignore protocol w, etc.

Manage dangerous ICMP packets

- The ICMP protocol can also have adverse effects on the CPUs of network devices.
 - For example, when there are particular topologies that, according to ICMP specifications, cause the systematic generation of such packets.
 - E.g., ICMP redirects in multi-point ethernet networks (with multiple routers connected) or in point-to-point ethernet networks.
- Considering that the ICMP packets are informative, some types of packets can be disabled in the devices without altering the functionality of the network.
- To limit the impact on the CPU of network devices, it is good practice to use the ICMP packet filtering mechanism to block the following ICMP packets:
 - **ICMP redirects**, which suggest an alternate route if the destination can be reached through another router in the same network
 - They can be used to indicate a different gateway and, thus, exposed to a man-in-the-middle.
 - **ICMP unreachable**, which informs the sender of a packet that the final destination is unavailable (e.g., not responding to ARPs or no route to that destination)
 - The unreachable ICMPs, besides overloading the CPU of the routers, can be used to know the internal topology of a network.



Only use authenticated routing protocols

- Routing information is critical to forwarding packets according to the correct routes.
- It is essential to ensure that packets with routing information from other routers are authentic.
- For this reason, it is best to use the authenticated version of the routing protocols wherever possible.
 - This ensures that unauthorized routers cannot distribute false information.



Data plane protection



Data plane protection

- The purpose of network devices is to move packets through the network according to the security policies established by governance.
- Without proper protections, attacks can be made to alter packet forwarding rules, potentially causing security policy violations.
- In addition, because network devices operate with virtually no administrator intervention once configured, it is challenging to observe security policy violations without proper monitoring.
- Therefore, data plane protection must be as thorough as possible.



Operate at all protocol stack layers

- To protect the data plan, it is necessary to intervene in several protocol stack layers.
- At level 2, you have to protect devices from possible MAC-IP association changes.
- At layer 3, you must protect devices from IP packets with dangerous configurations that attempt to map the network.
- At layer 4, you must protect devices from ICMP packets that may alter the normal flow of packets within the network.



Level 2 protection (switch configuration)

- Disable gratuitous ARP packets.
 - To avoid ARP spoofing attacks (MAC address theft), typical of man-in-the-middle attacks.
- Enable dynamic ARP inspection (DAI) mechanism
 - To protect against ARP spoofing and ARP poisoning, typical of man-in-the-middle attacks
- Disable ARP Proxy IP if not needed
 - IP proxy ARP allows ARP packets to traverse routers when a logical network is physically divided by routers and not just switches. This can be exploited for man-in-the-middle attacks.
- Enable port security mechanism
 - Allows only a limited number of MAC addresses to be exchanged, preventing attacks such as CAM table overflow, DHCP depletion, or misuse of a switch port.
- Enable DHCP snooping mechanism
 - This allows DHCP response packets to be forwarded only from authorized ports connected to a trusted DHCP server.
- Enabling the IP source guard mechanism
 - To allow blockomg all traffic with an abnormal IP-MAC address association, typical of IP spoofing.



Level 3 and 4 protection

- The main tools to protect networks at layers 3 and 4 are Access Control Lists (ACLs) used for packet filtering functions.
- ACLs are the rules that routers follow to identify the type of traffic of the packets they forward.
- ACLs are the rules that routers follow to identify the type of packet traffic that they are forwarding.
- They can identify packets by considering only IP addresses (standard ACL) or IP addresses and Layer 4 header information (extended ACL).
- Depending on the specified policy, routers can transform packets (e.g., blocked, subjected to NAT, forwarded in a VPN, etc.).
- For the protection of networks, the primary use is to filter packets (packet filtering) according to the network's security policy.
 - They are also used for NAT, Quality of service (QoS), VPN traffic selection, policy-based routing, or routing information.



Use rules (ACL in routers) for traffic filtering

- Block packets with IP address spoofing
 - Through ACLs, it is possible to block all packets used as source IP addresses IPs that are not consistent with the network topology.
 - For example, a host in a 10.0.0.0/8 network that uses IP 11.0.0.1
- Block packets that can lead to network mapping (scanning)
 - For example, taking care not to block functional features in the network, you can use ACLs to block UDP or ICMP packets from outside the web that may reveal information about the internal structure.
- It's a good idea to allow only packets that correspond to the traffic expected on the network.
 - According to the principle of least permission, blocking everything that is not explicitly expected to be exchanged in the network would be good.

Use rules (ACL in routers) to authorize only trusted sources



- Routers can use ACLs to limit the type of traffic of supporting protocols
- Examples
 - an ACL allowing NTP traffic from the trusted server only
 - an ACL allowing SSH access only from administrator hosts.
 - an ACL allowing ICMP or SNMP diagnostic packets from the administrator's hosts only.





Example of network hardening in the ACME network







Management plane protection

- Use strong passwords
 - Change the default password
- Use encrypted communication
 - Make sure to log in only using HTTPS
- Configure NTP service on internal interfaces
- Send logs to a syslog server
 - Configure opnsense to send logs to a centralized server

Opnsense management plane

- Change admin user password
 - Lobby: Password
 - Enter a password other than opnsense
 - Save the new password → 
- Make sure to log in only using HTTPS
 - System: Settings: Administration → Protocol HTTPS
 - Apply the new settings → 
 - Caution: it may be necessary to reload the page and authenticate in the firewall again for switching to encrypted communication

Management plane in Opnsense

- Configure NTP service on internal interfaces
 - Services: Network Time: General → select INTERNAL, DMZ, EXTERNAL
 - Save the new settings → 
- Send logs to a syslog server
 -  System: Settings: Logging / targets → add ()
 - Add as target the machine logserver.acme-XX.test, listening on port 514 via UDP.
 - To limit the number of logs, do NOT send messages for debug and info levels.
 - Save new settings → 
 - Apply changes → 




Control plane protection



- Protect against too many ICMP messages
 - Limit incoming ICMP traffic
- Block potentially malicious ICMP messages
 - Filter redirect and unreachable ICMP messages from external sources



Opnsense control plane: limit incoming ICMP traffic



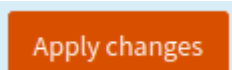
- Firewall: Shaper: Settings
 - In Pipes tab, add a limitation to 10 Kbit/s without selecting mask
 - In Rules tab, a rule for WAN about ICMP packets from each source and for each destination, using the limitation defined in Pipes tab as target
- Apply changes → 

Opnsense control plane: filter ICMP redirect messages

- Firewall: Rules: Floating → 
 - Add a Block rule in the first position, for ICMP redirect packets from any source and for any destination on the DMZ and EXTERNAL interfaces.
 - The rule must be of type "in" since packets enter the interface.
 - If necessary, to change the position of a rule, check the box next to the rule and click on the arrow icon () at the position where you want to move the rule



Opnsense control plane: filter outgoing *ICMP unreachable* messages

- Firewall: Rules: WAN → 
 - Add a Block rule in the first position, for ICMP packets of type Destination Unreachable with outbound direction from each source and to each destination
 - To change the position of a rule, check the box next to the rule and click on the arrow icon () at the position you want to move the rule to
 - The rule must be of type "out" since the packets we want to block go out of the interface to reach the network connected to it
- Apply the new rules → 



Data plane protection


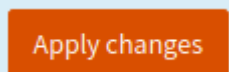
- Block packets with spoofed IP address
 - Filter packets with IP addresses not coming from local networks
- Allow only packets that match the traffic expected on the network
 - Allow access to the DMZ only to packets that require the services provided




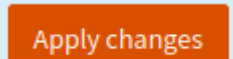
Opnsense data plane protection

- Like many other firewalls, the data plane protects itself by inserting traffic filtering rules.
- In Opnsense, rules are either interface-specific or floating.
- Floating rules are considered before any other interface rules.
 - A floating rule of type "pass" source any destination any overrides any other rule, making firewall rules quite useless.
- The rules for an interface are either "in" or "out":
 - "in", when packets are generated by the network to which the interface is connected, and they want to enter the interface (so "in" input) to reach a different network
 - "out", when another network generates packets, reach an interface, and want to exit the interface (thus "out") to enter the network to which the interface is connected

Opnsense data plane protection: block packets with spoofed address

- Filter packets with IP addresses **not** coming from local networks
 - Firewall: Rules: DMZ → 
- Add a pass rule for packets originating from the DMZ net, destined for any host and with any protocol.
 - The rules must be of type "in" since the packets enter the interface from the DMZ net network
- Create similar rules with the necessary modifications for the other internal interfaces, i.e. INTERNAL, EXTERNAL_CLIENT
- Apply the new rules → 

Opnsense data plane protection: accept packets for running services

- Allow access in the DMZ only to packets that require the services provided (web and proxy)
- Firewall: Rules: DMZ
 - To disable the rule that allows all IP packets coming from any source to reach any destination (it goes from a default pass to deny)
 - To disable a "pass" type rule you can click on the green icon
- Firewall: Rules: WAN → 
 - Add a "pass" rule for packets destined for the host with the webserver on port 80, coming from any source.
 - Add a "pass" rule for packets destined via tcp to the host with proxyserver on port 3128, coming from any source.
 - The rules must be of type "in" since the packets enter the interface from the WAN1 network.
- Create similar rules with the needed modifications for the other networks
- Apply the new rules → 





That's all for today?

Questions?

- References:
 - **CCNA Security 640-554 (Official Cert Guide)**