RADIUS Conference 2025, 13th of March 2025, Tampere, Finland

RADIUS in Action: Securing, Monitoring and Protecting Network Infrastructure

Karri Huhtanen (Radiator Software)

Radiator

Contents

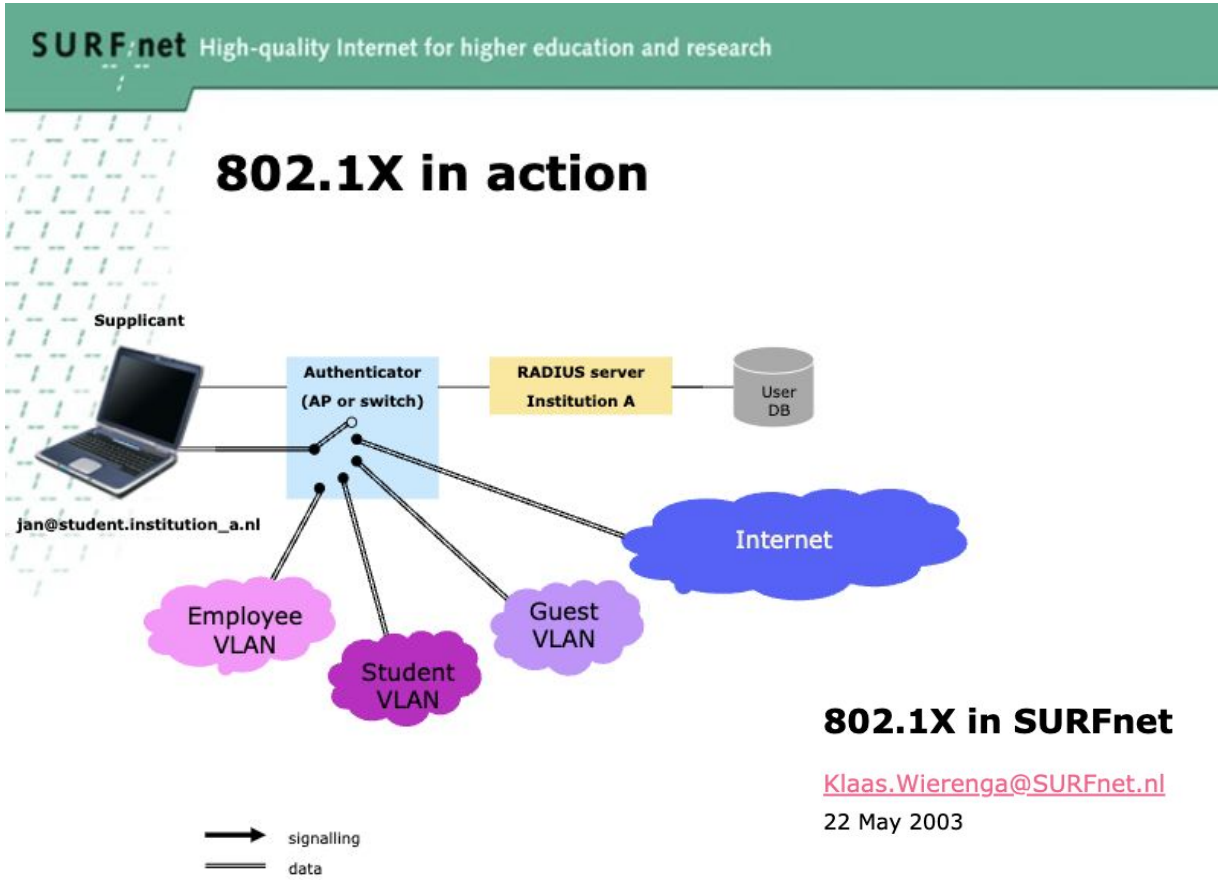
Introduction

- Usernames and passwords are getting harder to secure and harder to use – for the better or worse.
- Non-authenticated ports and non-segmented networks enable attackers to both gain access and move laterally in the network with minimal resistance and risk of detection.
- Unprotected RADIUS traffic can be captured, modified and tracked.
- Multi-Factor Authentication (MFA) and RADIUS/Tacacs+ Authorisation helps to secure network device access, but what happens when your MFA service or Active Directory is down?
- In addition to control, RADIUS can also provide information to monitor network better, detect and locate anomalies.

Certificate-Based Authentication: Replacing Usernames and Passwords

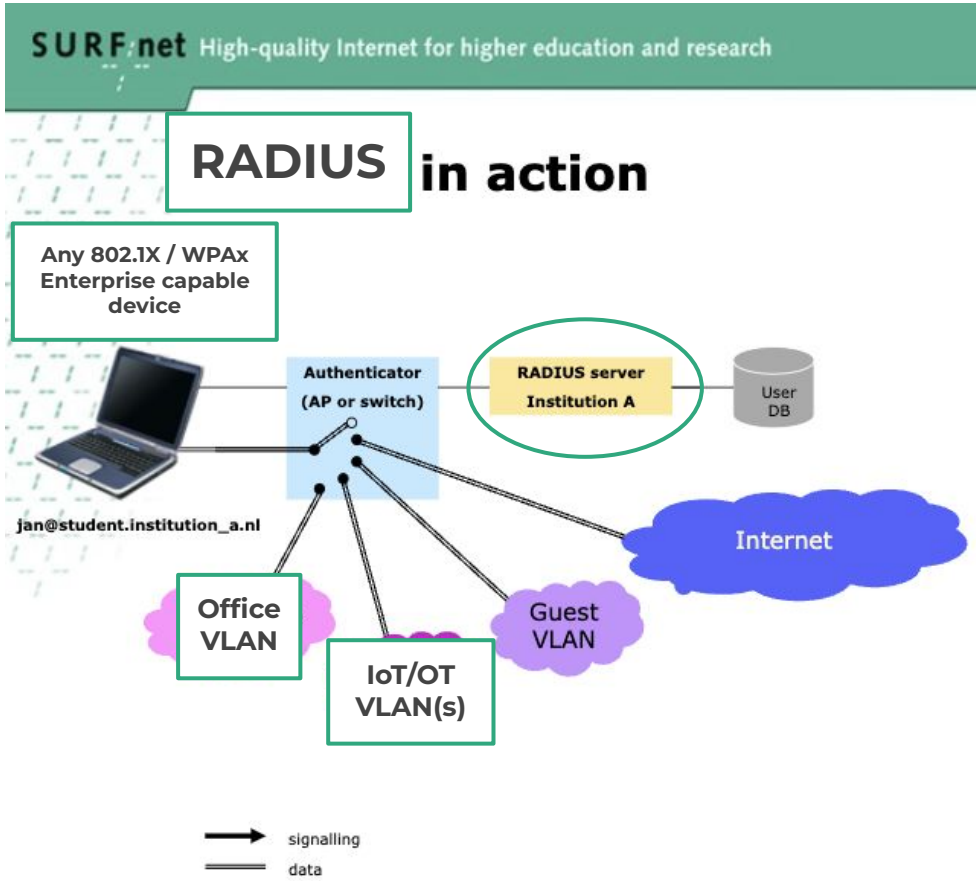
- Usernames and passwords can be guessed, phished, copied or stolen.
- MFA adds some protection, but the user can be tricked to bypass it. It is not also very useful for repeating network authentications.
- Certificate-Based Authentication (EAP-TLS) has been around since 1999 and updated several times (2008, 2022) on include new TLS versions and other enhancements.
- With EAP-TLS and trusted platform modules (TPMs) in modern devices, both the credentials and the network access in wired and wireless networks can be secured.
- For provisioning of the certificates there are multiple services and solutions available especially for managed devices, but for non-managed devices the certificate and configuration provisioning is still harder.

Securing Network Port Access with 802.1X and VLANs



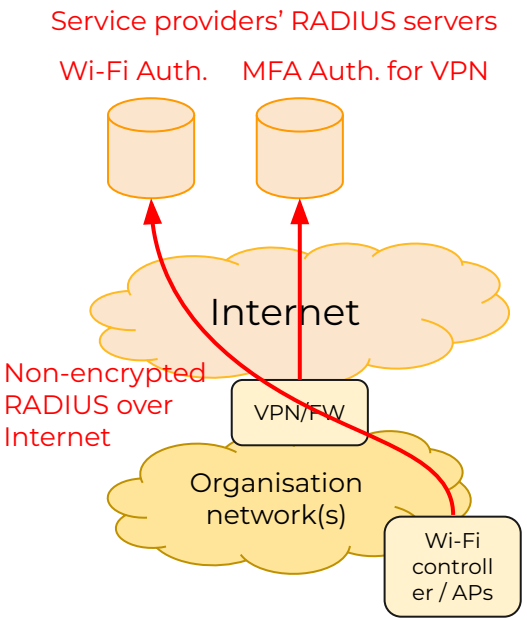
So in 2003 in Terena Networking Conference in Zagreb (Croatia) was this guy from Netherlands presenting 802.1X, dynamic VLAN allocation and roaming ...

Securing Network Port Access with 802.1X and VLANs



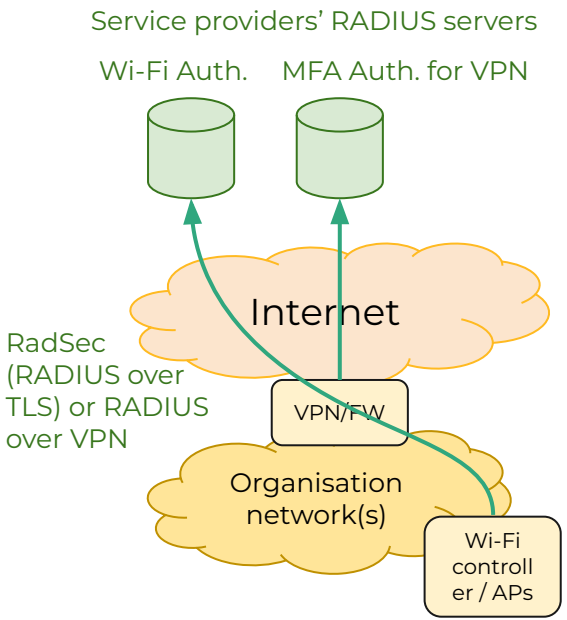
- 802.1X and dynamic VLAN selection worked then and works now – both in wired and wireless networks.
- VLANs are used for network/device segmentation, 802.1X is used for port/VLAN authentication.
- Single port or single Wi-Fi network, but what VLAN is selected for the device, is determined by RADIUS.
- RADIUS can utilise and combine multiple sources of information for the decision, for example:
  - Device registry / directory services
  - Device identification/classification by network devices (e.g. Wi-Fi controllers)
  - Device security assessment information
  - Even AI if not now, then probably in the future

Enhancing Management Traffic Security with RadSec (RADIUS over TLS)



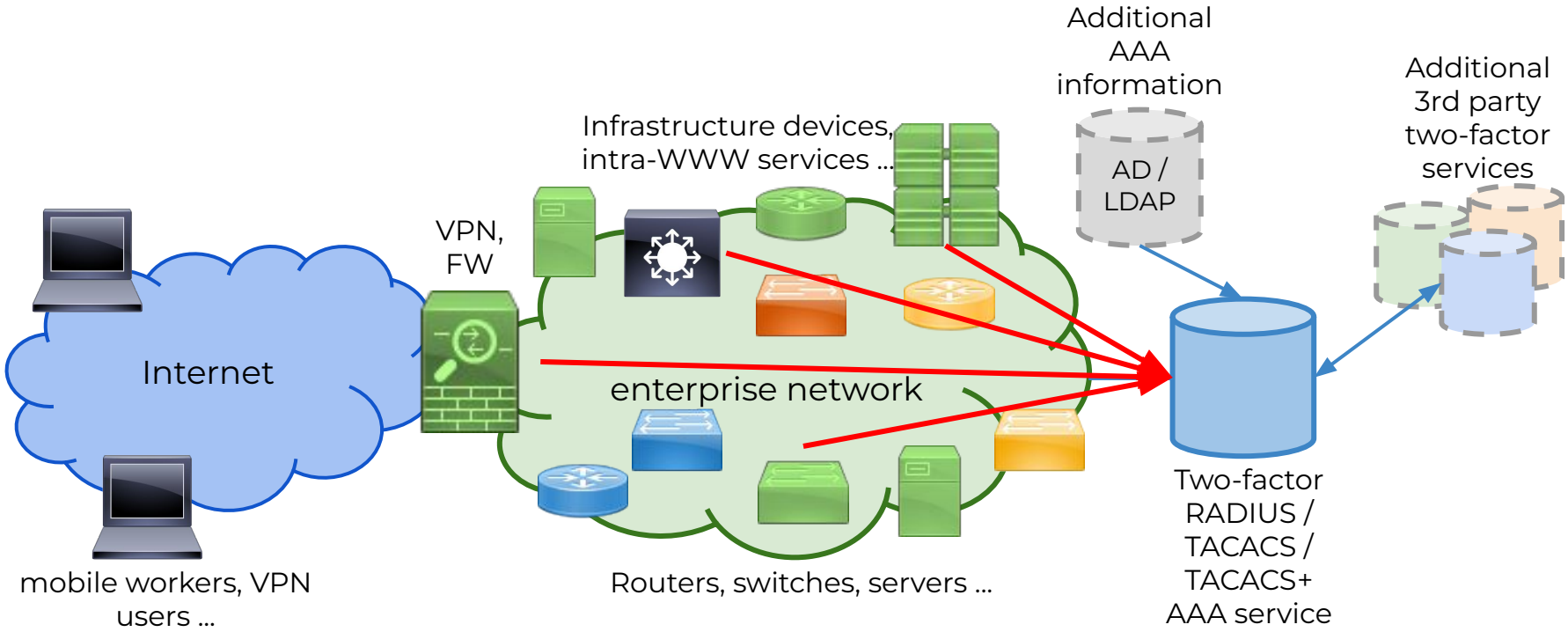
- Sending non-encrypted RADIUS traffic over untrusted networks without a VPN or TLS is nowadays even worse idea because of BlastRADIUS vulnerability.
- Both RADIUS authentication and accounting requests have by default in them plain-text attributes, which may contain sensitive information about the users, devices and even organisation network settings.
- The larger the distance between RADIUS clients and servers is, the larger is the risk of leaking information or to be vulnerable to BlastRADIUS.

Enhancing Management Traffic Security with RadSec (RADIUS over TLS)



- With RadSec not only the RADIUS traffic is secured but also the RADIUS clients are more securely identified with certificates.
- The service providers' RADIUS server can now better verify multiple RadSec clients even behind Network Address Translation (NAT) and dynamic addresses.
- We have even measured better authentication/accounting throughput with RadSec than with RADIUS over UDP with our RADIUS servers.

Protecting Network Infrastructure Access with RADIUS, TACACS+, and Multi-Factor Authentication

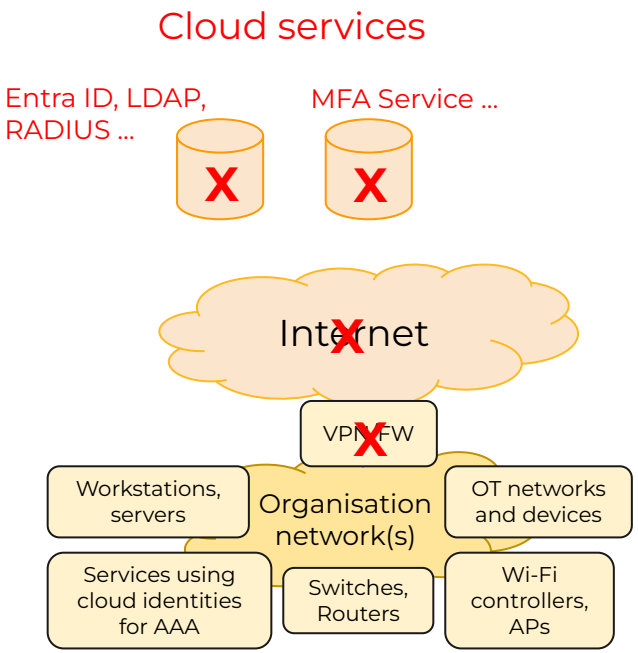


Radiator

Protecting Network Infrastructure Access with RADIUS, TACACS+, and Multi-Factor Authentication

- The network devices authenticate and authorise the users accessing them via RADIUS or TACACS+ server => no common user accounts
- The Multi-Factor Authentication replaces passwords with more secure authentication => no weak passwords
- The RADIUS/TACACS+ server can then combine information from multiple sources (e.g. LDAP, Active Directory, Entra Id, SQL, 3rd party services) to authenticate and authorise particular user to access the network device.
- All this works with most enterprise, operator and even operational technology (OT) network devices.
- There is also increasing support for securing also these connections with TLS for added security.

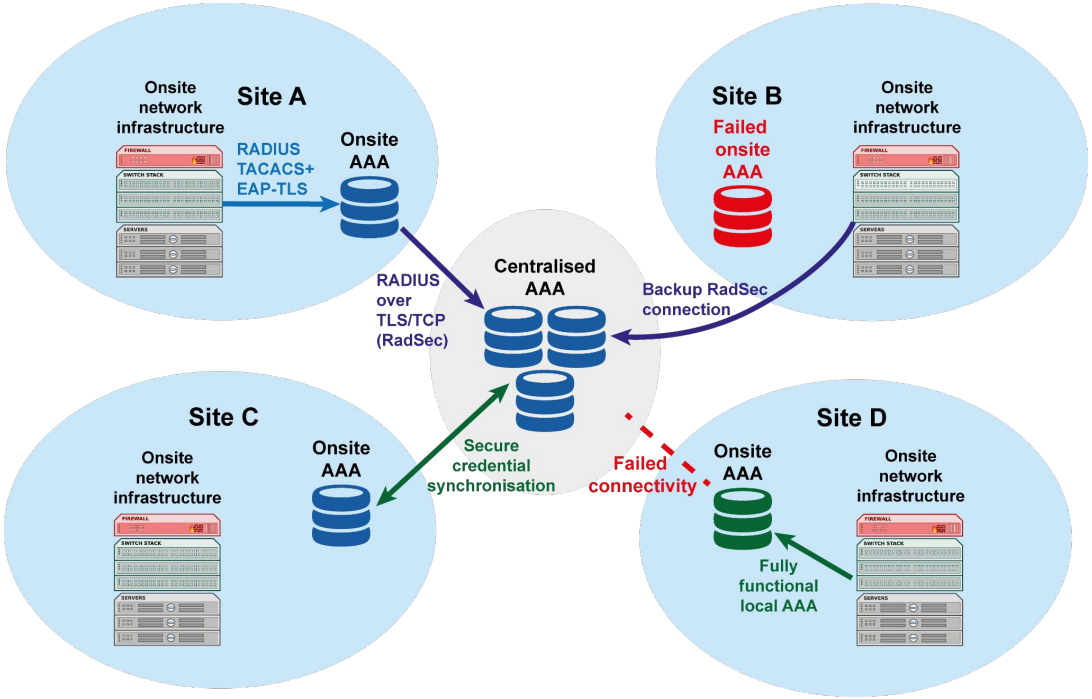
But what happens to your network when your Internet connection(s) or cloud services are down?



- Are you able to access your wired and wireless network?
- Can you log into your workstations, servers and network devices to do diagnostics?
- Do you have sealed emergency support accounts written down, stored securely and configured into network devices?
- What happens if ransomware or faulty updates hit your directory and other servers?

Radiator

Adding local or hybrid AAA improves resiliency



- Redundant local AAA ensures that the site continues to function.
- Cloud services can be used as primary or backup option for local AAA.
- By using technologies such as EAP-TLS, which do not require a constant access to outside services, services such as network connectivity can be ensured.
- MFA can also be implemented without cloud services with a local or hybrid AAA model.

Fault-Tolerant Distributed AAA Architecture Supporting Connectivity Disruption
https://urn.fi/URN:NBN:fi:tuni-202209197126

Radiator

Improving Network Monitoring with RADIUS Authentication and Accounting Logs


```
{
  "Backend-Server": [
    "fi-proxy-1.auth.fi"
  ],
  "Called-Station-Id": "D8-B1-90-DB-F8-C0:eduroam",
  "Calling-Station-Id": "BE-57-64-BA-85-CA",
  "Chargeable-User-Identity-Request": "00",
  "Client-IP-Address": "10.255.255.247",
  "Client-Identifier": "CLIENT-IPV4-CISCO-WLC-MGMT",
  "Context-Id": "5f89b13fc9affb50",
  "Elapsed-Time": 0.170439395,
  "Framed-IP-Address": "192.168.172.252",
  "Handler": "proxy_to_eduroam",
  "NAS-IP-Address": "10.255.255.247",
  "NAS-Identifier": "172.16.172.52:D8-B1-90-DB-F8-C0:eduroam",
  "Policy": "default",
  "Result": "accept",
  "Service-Type": "framed-user",
  "Timestamp": "2025-03-11T18:55:15.809544+00:00",
  "User-Name": "anonymous@radiatorsoftware.fi",
  "cisco-avpair": [
    "service-type=Framed",
    "audit-session-id=F7FFFF0A000121A5845714C3",
    "method=dot1x",
    "addrv6=fe80::c8d:cc5:9f1:ae86",
    "client-iif-id=2550141079",
    "vlan-id=145",
    "cisco-wlan-ssid=eduroam",
    "wlan-profile-name=eduroam"
  ],
}
```


- Network devices can provide detailed information about the devices connecting to the network via RADIUS.
- This information is often included in the RADIUS authentication and accounting requests, and can then be utilised for AAA decisions or logged for further analysis.
- SIEMs, XDR solutions and AI analysis can benefit from this complementing information provided by RADIUS clients and servers.

Radiator

Improving Network Monitoring with RADIUS Authentication and Accounting Logs

```
e86bff00 Thu Feb 23 14:50:10 2023 594131: DEBUG: Packet dump:
e86bff00 *** Received from 10.255.255.245 port 61503 ....
e86bff00 Code:       Accounting-Request
e86bff00 Identifier: 1
e86bff00 Authentic:  <167>[<8>i+<250><208><242><12>A<179><226>d<183><183>S
e86bff00 Attributes:
e86bff00       Acct-Status-Type = Start
e86bff00       NAS-IP-Address = 10.255.255.245
e86bff00       User-Name = "0001012014020013@wlan.mnc001.mcc001.3gppnetwork.org"
e86bff00       NAS-Port = 0
e86bff00       NAS-Port-Type = Wireless-IEEE-802-11
e86bff00       Calling-Station-Id = "aa2b0b553528"
e86bff00       Called-Station-Id = "6026efcdcdc4"
e86bff00       Framed-IP-Address = 172.16.145.111
e86bff00       Acct-Multi-Session-Id = "AA2B0B553528-1677156607"
e86bff00       Acct-Session-Id = "6026EF5CDC55-AA2B0B553528-63F76102-8F448"
e86bff00       Acct-Delay-Time = 0
e86bff00       Aruba-Essid-Name = "RS-TEST"
e86bff00       Aruba-Location-Id = "rs-aruba-ap-1"
e86bff00       Aruba-User-Vlan = 145
e86bff00       Aruba-User-Role = "RS-TEST"
e86bff00       Aruba-Device-Type = "NOFP"
e86bff00       Acct-Authentic = RADIUS
e86bff00       Service-Type = Login-User
e86bff00       NAS-Identifier = "rs-aruba-ap-1"
e86bff00
```

- For RADIUS Authentication and Accounting data to be useful, its quality from different vendors needs to be assured and attributes to be standardised.
- Including the useful data within vendor specific RADIUS attributes hinders their general use across vendors.
- Protecting privacy makes even legitimate tracking of sessions harder (e.g. MAC address randomisation and anonymous identities)
- Solutions such as Chargeable-User-Identity are needed to combine RADIUS authentication and accounting requests into sessions.
- IPv4 and IPv6 address information from DHCP or network devices needs to be combined with RADIUS authentication and accounting for improved network monitoring and auditing.

Conclusion: RADIUS in Action

1. **Stronger Authentication**: Replacing passwords with certificate-based authentication enhances security and usability.
2. **Network Access Control**: 802.1X and VLANs effectively segment and secure network access, preventing unauthorized lateral movement.
3. **Management Traffic Security**: RadSec (RADIUS over TLS) protects sensitive RADIUS communications from interception and modification.
4. **Infrastructure Protection**: Combining RADIUS, TACACS+, and Multi-Factor Authentication ensures secure and accountable access to critical network devices.
5. **Resilient Network Operations**: Local and hybrid AAA solutions help maintain network access even when cloud services or Internet connectivity fail.
6. **Improved Monitoring & Visibility**: Leveraging RADIUS authentication and accounting logs enhances network monitoring, security insights, and anomaly detection.