WHITEPAPER

Network authentication with certificates

Use case: Network Authentication

EVERTRUST

Introduction to Network Authentication

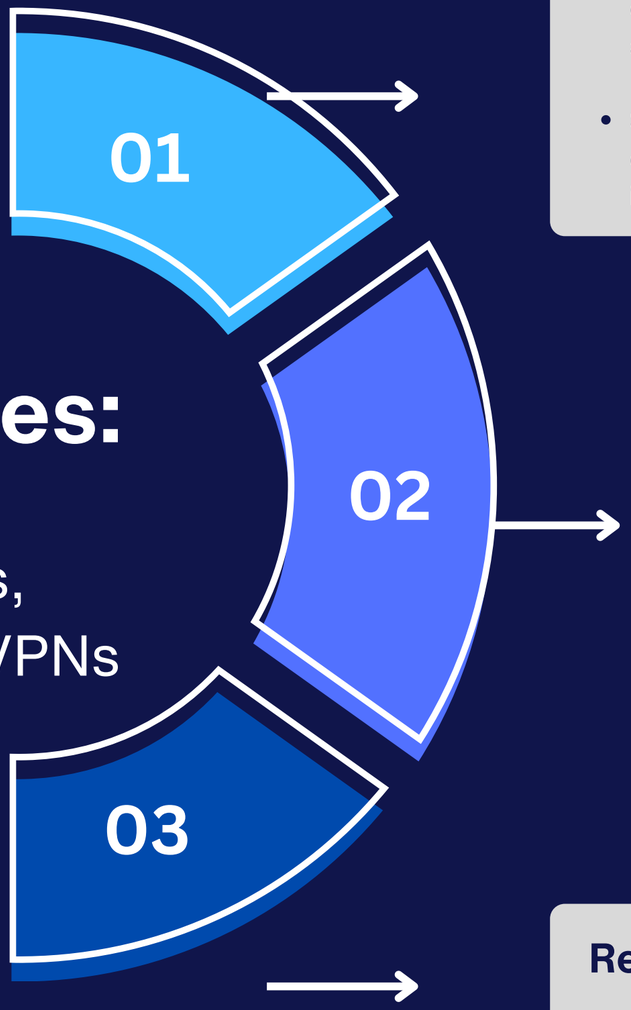
In today's interconnected world, where data breaches and cyber threats loom large, robust network authentication is paramount. It involves a series of protocols and mechanisms designed to verify the identities of users, devices, and applications before granting them access to network services, ensuring secure access and protecting sensitive information.

This comprehensive guide explores the critical role of certificates in VPNs, the nuances between IPSec and SSL protocols, and the superiority of EAP-TLS in network authentication. It underscores the importance of RADIUS and IEEE 802.1X in access management, highlighting their pivotal role in modern cybersecurity frameworks.

By understanding and implementing these advanced security measures, organizations can fortify their defenses, mitigate risks, and uphold operational integrity in an increasingly digital landscape.

VPN Technologies:

IPSec vs SSL,
Site-to-Site VPNs,
Remote Access VPNs



VPN Encryption: IPSec vs SSL

- IPSec: Operates at the network layer (OSI Layer 3), encrypts and authenticates traffic using L2TP, IKEv2, and SSTP.
- SSL/TLS: Works at the application layer (OSI Layer 7), commonly through OpenVPN and OpenSSL, often used in browser-based VPNs.

Site-to-Site VPNs

- Networking technology enabling businesses to securely connect geographically distant offices and networks.
- Establishes a secure communication channel over the internet, facilitating seamless data exchange between different physical locations.
- 2 main types: intranet-based (connects multiple sites within the same organization) and extranet-based (connects different organizations for secure data transfer).

Remote Access VPNs

- Allows secure connections to a private network from remote locations over the internet, encrypting data transmission to protect against unauthorized access.

Use case: Network Authentication

EVERTRUST

Use case: Network Authentication

WiFi ⟶ Security

PKS (Pre-Shared Key)

Concept: Shared secret or password that must be entered into all devices that wish to connect to the network.

Ease of Distribution: Anyone with the PSK can join the network, making it less secure in environments where the key might be shared widely or where many devices are connected.

- **Loss or theft of the device storing the PSK:** the security of the entire network is compromised, so the PSK must be changed and updated on all devices, which is time-consuming and disruptive to the operation of the network.
- **Shared key vulnerability:** A single PSK shared among multiple users means that compromise of one user's device can lead to compromise of the entire network
- **Limited scalability:** PSK-based security is not well suited to environments with a large number of devices or users, as the process of distributing and updating the PSK is impractical.

EAP-TLS

Concept: Is an IETF standard, essential in WPA2-Enterprise networks for robust authentication.
It employs X.509 digital certificates to achieve mutual authentication between clients and servers, ensuring data confidentiality and integrity.

Types:

- EAP-TLS (previously tested)
- EAP-TTLS/MSCHAPv2 (April 2005)
- PEAPv0/EAP-MSCHAPv2 (April 2005)
- PEAPv1/EAP-GTC (April 2005)
- PEAP-TLS
- EAP-SIM (April 2005)
- EAP-AKA (April 2009[35])
- EAP-FAST (April 2009)

Benefits:

01 MUTUAL AUTHENTICATION

EAP-TLS provides mutual authentication between the client and the server, ensuring that both parties are legitimate. Involves a secure exchange where both: the *client* and *server* present and verify each other's certificates.

02 CERTIFICATE-BASED SECURITY

Each device has a unique certificate, which enhances security by reducing the risk of unauthorized access. This certificate-based approach simplifies password management and leverages advanced cryptography to further secure communications.

03 SCALABILITY

It eliminates the need to manually distribute and update PSKs, making it a more efficient solution for multi-device environments. *EverTrust* streamlines certificate issuance and management with its solutions, ensuring compliance and operational efficiency.

04 ENHANCED SECURITY

TLS provides strong encryption and integrity protection for the authentication process. Makes it much more difficult for attackers to intercept with communications and the authentication process, ensuring that both parties are authenticated and session keys are generated for encrypted communication.

05 REVOCATION AND MANAGEMENT

Certificates can be easily revoked if a device is lost or compromised, without affecting the rest of the network. This feature improves network management and device recognition, enhancing overall security and making it easier to manage devices within the network.

EVERTRUST

The Use of Certificates for Authentication on VPNs and WiFi and the Importance of Strong Authentication

Whether you choose to use a VPN or a Wi-Fi connection, strong authentication is essential to ensure network security and data integrity. Certificates are an excellent option and play a crucial role in this process, providing a strong and secure method of verifying user and device identities.
The main purpose of using certificates is to ensure that only authorized users can establish a VPN connection, while maintaining the integrity and confidentiality of the network.

But, what are certificates in the context of WiFi and VPN Authentication?

They are digital documents that use PKI principles to associate a user's identity with a public key. They are issued by a trusted certificate authority and contain information such as: the user's public key, the identity of the user or device and the digital signature of the CA, which verifies the authenticity of the certificate.

That is why in both VPN and Wi-Fi scenarios, strong authentication methods are essential for Wi-Fi networks to prevent unauthorised access and protect the confidentiality and integrity of transmitted data. Without these mechanisms, Wi-Fi networks are vulnerable to various attacks. And with the use of certificates, you ensure that only legitimate users can connect to the network, providing a secure environment for communication.

Keys elements of strong authentication

1. Multi-Factor Authentication (MFA)

Involves providing 2 or more verification factors to access a VPN. It includes:

- Password
- Digital certificate or hardware token
- Biometric verification such as fingerprint or facial recognition

2. Digital Certificates

Provide a secure means to verify user identities.

EverTrust Stream facilitates their issuance, validation, and revocation, ensuring compliance with regulatory standards like eIDAS and offering deployment flexibility (on-premises or cloud).

3. Public Key Infrastructure (PKI)

Supports certificate-based authentication, managing public-private key pairs securely to validate and encrypt VPN communications effectively.

EverTrust Horizon streamlines CLM, automating processes to enhance efficiency and minimize operational disruptions across diverse IT environments.

4. Regular Updates and Revocation

To maintain robust security, certificates must be regularly updated and revoked as necessary.

EverTrust Stream supports these tasks by automating certificate management processes, including the generation of Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responses.

Use case: Email Encryption

EVERTRUST

Integration with EverTrust Solutions:

Our Solutions, including **Stream** and **Horizon**, optimize VPN certificate and cryptographic key management for robust network security and operational efficiency.

- **Stream** simplifies secure certificate issuance, validation, and revocation with flexible deployment options, ensuring compliance with eIDAS regulations and continuous operational integrity.

- **Horizon** automates Certificate Lifecycle Management (CLM) with adaptable workflows, integrating smoothly into existing IT systems. It supports diverse device environments and enhances data security through streamlined lifecycle processes and robust authentication measures.

By integrating these principles, **Horizon effectively deploys certificates, ensuring robust security for both VPN authentication** and general device management through UEM solutions like Windows autoenrollment and **MDM like Microsoft Intune.**

Together, these solutions fortify VPN security against evolving cyber threats.

Conclusion

In today's digital world, network security relies on strong authentication and strategic protocol choices. Certificates enhance VPN security through PKI and multi-factor authentication, preventing credential theft.

Choosing VPN protocols like IKEv2/IPSec and OpenVPN/SSL balances performance and ease of use.

Network authentication, especially EAP-TLS, uses digital certificates and cryptography for high security. Protocols like RADIUS and IEEE 802.1X ensure centralized security. Advanced methods like EAP-TLS and RADIUS are crucial for modern cybersecurity.

EVERTRUST solutions streamline these processes: EVERTRUST Stream simplifies certificate issuance and eIDAS compliance, while EVERTRUST Horizon automates Certificate Lifecycle Management (CLM).

These solutions ensure robust VPN authentication and device management through UEM systems like Windows auto-enrollment and MDM such as Microsoft Intune. Prioritizing strong authentication and protocol integration helps protect data and maintain operational integrity.

GET RID OF CERTIFICATE OUTAGES AND REDUCE PKI OPERATING COST WITH EVERTRUST

WE CREATE...

- Operational, secure and high-performance solutions that articulate IT security and control the lifecycle of electronic certificates.
- Integrated in a non-intrusive, simple and effective way into our customers' existing ecosystems.
- Designed to meet the needs of trusted service delivery, automation and continuity.

Stream

- Hold your own Keys without Captivity
- Issuance and revocation of certificates
- Issuance of CRLs, OCSP responses and timestamping
- eIDAS ready and compliant
- Designed to be deployed on premises or in the cloud

Horizon

- Streamlined integration within the information system
- Process certificate lifecycle requests using comprehensive workflows and machine identity management tools
- Take care of the issuance, renewal, and revocation of certificates hosted on:
  - Servers, mobiles and workstations
  - Appliances and IoT
  - On premises or in the Cloud

Use case: TLS Server Certificates

EVERTRUST

EVERTRUST

Use case: Network Authentication

Discover more !

evertrust.io

Use case: TLS Server Certificates

EVERTRUST