Introduction

In many networks, once you're through the firewall, the internal network is relatively open. Users often move from system to system without checks or balances, and with relatively few security controls in place. This lack of controls not only permits authorized individuals to move freely but also enables unauthorized individuals and malicious software to do the same.

Associated Video:
Zero Trust - CompTIA Security+ SY0-701 - 1.2
https://youtu.be/zC_Pndpg8-c?si=1cK42vRMJdnsUIvQ

Transitioning to Zero Trust

To address these issues, many security administrators are adopting a zero trust architecture. Zero trust means that authentication or proof of identity is required each time access to a resource is requested. This principle applies to every device, process, and user on the network.

As the name implies, zero trust assumes that nothing is trusted by default. Multi-factor authentication, data encryption (both at rest and in transit), additional system permissions, firewalls, and various security policies and controls are implemented to enforce this environment.

Implementing Zero Trust

Functional Planes of Operation

A practical approach to implementing zero trust involves breaking security devices into smaller components, referred to as functional planes of operation. These planes include:

1. **Data Plane**
    - Handles the actual security processes.
    - Examples: switches, routers, and firewalls processing frames, packets, and network data in real time.
    - Functions: forwarding, network address translation (NAT), and routing processes.

2. **Control Plane**
    - Manages actions occurring in the data plane.
    - Functions: configuring policies and rules, managing routing tables, firewall rules, and NAT settings.

This separation applies to physical devices, virtual devices, and cloud-based security controls. For example, on a physical switch, the data plane manages traffic forwarding, while the control plane handles configuration settings.

Advanced Zero Trust Features

Adaptive Identity Verification

Adaptive identity technology enhances zero trust by applying security controls based on dynamic authentication variables, including:

- **Source Analysis**: Verifying the origin of requests (e.g., a U.S. user accessing resources via a Chinese IP address may trigger additional security checks).
- **User Relationship**: Differentiating between employees, contractors, or part-time workers.
- **Contextual Factors**: Physical location, connection type, and IP address.

These variables allow systems to create stronger authentication processes tailored to specific scenarios.

Limiting Entry Points

Zero trust also involves restricting network access points. For example, access may be limited to users within a building or those connecting via VPN, eliminating other methods of entry.

Security Zones

To manage trust within the network, security zones categorize connections and their associated trust levels. Examples include:

- **Untrusted Zone**: External networks.

- **Trusted Zone**: Internal corporate networks.
- **Internal Zone**: Data center environments.

Rules can define zone interactions, such as denying access from an untrusted zone to a trusted zone. Implicit trust can also be established within certain zones, such as between a corporate office (trusted zone) and a data center (internal zone).

Policy Enforcement and Decision Points

To enforce zero trust, networks use Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs):

1. **Policy Enforcement Point (PEP)**
    - Acts as a gatekeeper, evaluating all traffic.
    - Ensures all traffic complies with policies before allowing it to traverse the network.
2. **Policy Decision Point (PDP)**
    - Analyzes authentication requests and predefined security policies.
    - Determines whether access is granted, denied, or revoked.
3. **Policy Administrator**
    - Relays decisions from the PDP to the PEP.
    - Issues access tokens or credentials as needed.

Zero Trust in Practice

A complete zero trust model operates as follows:

1. Subjects and systems from an untrusted zone communicate through the data plane.
2. Traffic passes through the Policy Enforcement Point for evaluation.
3. The PEP forwards data to the Policy Administrator, which communicates with the Policy Decision Point.

4. The PDP examines requests against predefined policies and makes a decision.
5. The Policy Administrator relays this decision to the PEP.
6. If traffic is allowed, the PEP grants access to the trusted zone and the requested enterprise resource.

Conclusion

Zero trust transforms network security by requiring continuous authentication and verification. Through adaptive identity verification, functional planes of operation, security zones, and robust policy enforcement mechanisms, organizations can protect their resources and reduce the risk of unauthorized access. Adopting zero trust ensures a secure and well-controlled network environment.