INVISINET
Where Zero Trust Begins

TAC and VPNs
Extending Identity Beyond a VPN

WHITEPAPER

INVISINET
Where Zero Trust Begins

Introduction

INVISINET Transport Access Control

INVISINET Transport Access Control (TAC) mutually identifies and authenticates users and devices on first packet receipt of a TCP/IP session. This First Packet Authentication (FPA) protects applications and network resources from unauthorised access by concealing network services from unidentified and unauthenticated users and devices. Authenticated access control provided by TAC is so complete that it even stops port scans and network reconnaissance, rendering protected resources invisible to attackers and intruders.

Secured Identity Communication

TAC operates by communicating the identity of the user or device requesting resource access to a TAC Gateway located along the communications path. TAC identity is securely communicated using a stream of cryptographic tokens that are embedded in the TCP header during the establishment of the TCP session. These cryptographic tokens are ephemeral; they expire if not used. The cryptographic tokens are protected against replay. The entire token system employed by TAC consumes no additional bandwidth and is tolerant of packet loss. TAC is tolerant of network address translation and port address translation, enabling the use of dynamic and mobile addressing without being dependent on any particular network topology

Why INVISINET TAC?

TAC authenticates network sessions starting with the first packet. When a session is established in a TCP/IP network, information about that network application and server is exposed due to security weaknesses in the TCP protocol. This exposed information illuminates additional attack vectors for cyber attackers.

TAC closes this security gap by authenticating session requests on the first packet and by not responding to unauthenticated requests. TAC is the only solution that truly mitigates this vulnerability. By employing INVISINET's patented FPA technology, TAC ensures that information about the network environment is prevented from leaking to unauthorized parties during the initial establishment of the TCP session, effectively disabling the use of network reconnaissance tools. As a result, only authenticated and authorized users and devices are allowed access. All TAC-protected assets and resources effectively disappear from attacker view as they are cloaked by the TAC technology. The bad guys can't target and attack what they can't see.

VPNs

A virtual private network (VPN) is a private data network that makes use of the public Internet, maintaining privacy through the use of a tunneling protocol and accompanying security procedures. A virtual private network can be compared with a system of owned or leased lines that can only be used by one company. The main purpose of a VPN is to give a company the same capabilities as private leased lines at a much lower cost by using shared public infrastructure. Companies and organizations construct VPNs for both extranets and wide-area intranets.

There are two standardized technologies for VPNs: IPsec and SSL (TLS). Both of these technologies utilize similar encryption protocols.

https://www.armis.com/analyst-reports/2023-forrester-top-trends-in-operational-technology-security/

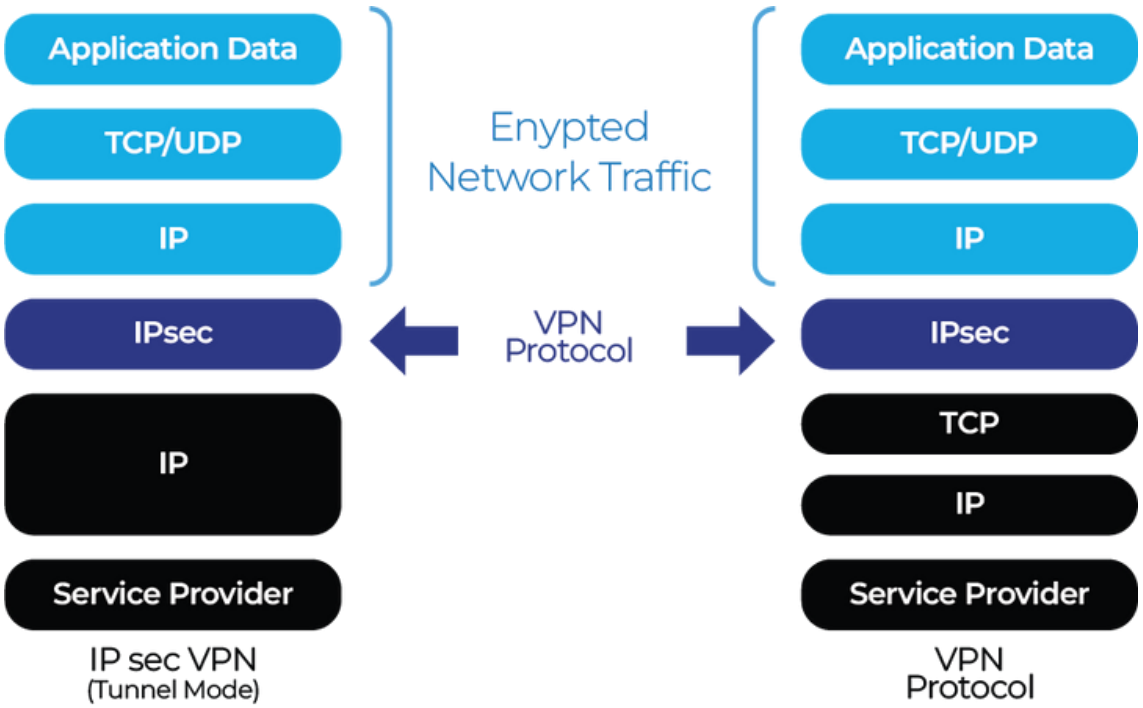


Fig 1

IPsec

IPsec is an IP-based packet encryption protocol that operates in tunnel and transport modes. IPsec requires that security associations be established using Internet Key Exchange (IKE) with either certificates or pre-shared secrets. Security associations can be established manually as well, but this is usually unfeasible for enterprise deployments. IPsec is standardized by the Internet Engineering Task Force (IETF) and is described in several Request For Comments (RFCs).

Secure Socket Layer VPNs

SSL VPNs use SSL or Transport Layer Security (TLS, the successor to SSL) to provide an encrypted IPlayer tunnel between endpoints. SSL VPN security associations are established during SSL session establishment and use certificates or other user-supplied credentials. SSL and TLS are standardized by the IETF and are described in several RFCs.

While providing privacy for network traffic, a VPN is still just a network tunnel, connecting a remote device to a network or connecting two networks. To ensure security, the traffic traversing VPNs should still pass through firewalls, IPS's, and other security devices before it should be trusted.

https://www.armis.com/analyst-reports/2023-forrester-top-trends-in-operational-technology-security/

Identity Boundaries

A client's identity within a VPN is provided by the certificate or other credential used to establish the client's security association. This identity is used by the security association to decrypt VPN traffic at the termination of the VPN.

Once the traffic is outside of the VPN tunnel and has been decrypted, there is no ability to authenticate the sender at the networking layers, because there is no secured identity to communicate. Outside the VPN tunnel, client traffic is identified solely by the client IP address. Unless the VPN termination occurs directly on the device providing the desired network resources, client traffic has crossed a boundary where the sender's identity is no longer securely and explicitly described. VPN traffic must be decrypted so additional value-add network infrastructure can operate. This additional infrastructure—firewalls, IPS's, load balancers, and traffic shapers—provide various functions for security, authentication, application routing, and service delivery. Complete access to the network payload, including TCP and application headers and data, is needed, thereby requiring decryption by the VPN termination device.

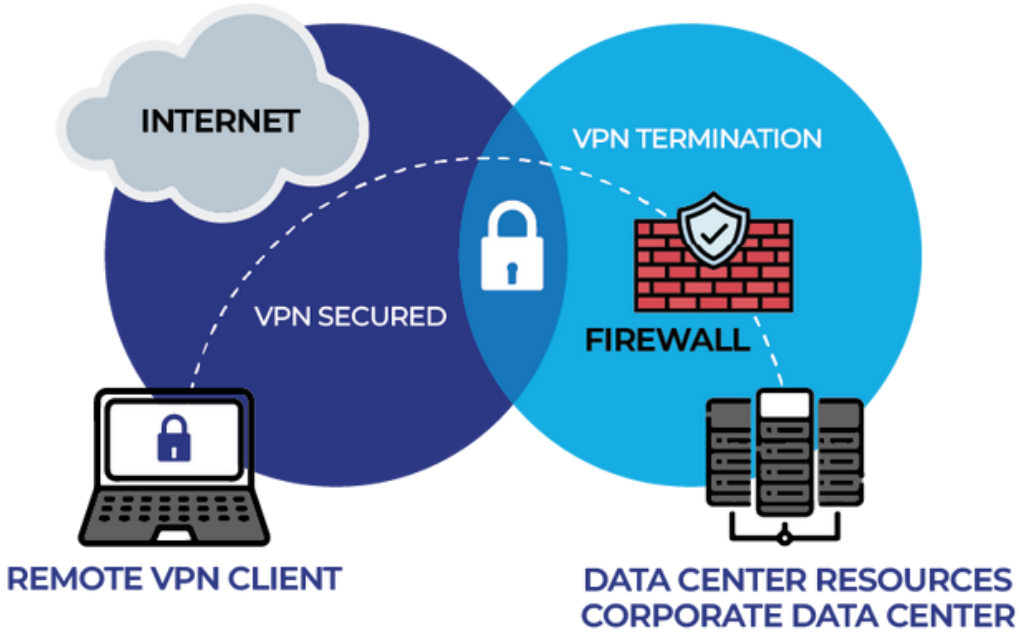


Fig 2

INVISINET TAC and VPNs

Complementary Technology

TAC is complementary to VPNs, both IPsec and SSL VPNs. Specifically, TAC does not provide data encryption and relies on VPNs or TLSs for this service. For VPN environments, the existing VPN infrastructure is used. For non-VPN environments, where data encryption is required, TAC can be combined with other technologies to provide encryption services.

Extends Identity Beyond VPN Termination Boundary

TAC's ability to insert identity into the TCP header during TCP session establishment does not end at the VPN termination boundary. A TAC Gateway, which provides access control policy enforcement, may be placed before or after other network infrastructure and can protect a single application, server, cluster, or entire data center. A TAC Gateway can enforce access control, application routing, and service delivery policies based on user and/or device identity

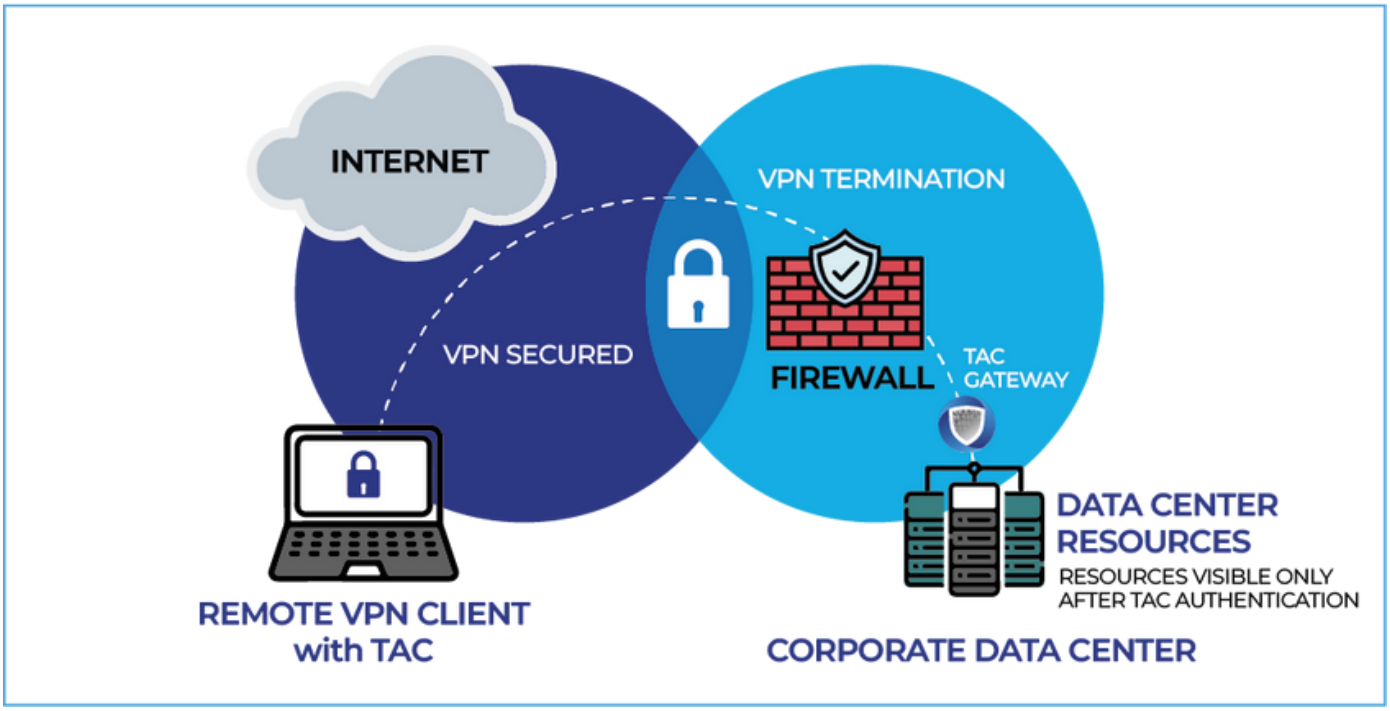
TAC protects network resources from port scans, network reconnaissance, and unauthorized access, even when all of the network resources are available (from a network perspective) to a VPN client. In the case of SSL VPNs, TAC can also protect the VPN infrastructure itself.

Identity-Based Policy

Since TAC's policy enforcement is based on the client's identity, the client's IP address is no longer part of the policy, eliminating the need for security policies to be tied to specific network addresses and topologies.

Moving from a client IP address-based policy to an identity-based policy also improves security, because addresses can be easily spoofed and impersonated, whereas identity, securely communicated by TAC, cannot. Identity based policy enables network and security administrators to make policy planning and enforcement easier and more secure.

Fig 3



Summary

INVISINET TAC mutually identifies and authenticates users and devices on first packet receipt of a TCP/IP session. This FPA protects applications and network resources from unauthorized access by concealing their network services from unidentified and unauthenticated access. TAC is complimentary to VPNs, both IPsec and SSL VPN. Specifically, TAC does not provide data encryption and relies on other technology for this service. INVISINET TAC extends identity beyond the VPN boundary. TAC enables identity-based policy, providing access control, application routing, and service delivery policies, all determined by the identity of the client. TAC protects assets and resources, effectively cloaking them from an attacker's view, even across a VPN.