White Paper

Introduction

Enterprises and government agencies are under repeated cyber attack. Attacks range in scope from distributed denial of service (DDoS) attacks, which are designed to shut down systems, to elaborate stealth efforts, which are designed to live undetected in the infrastructure and steal intellectual property or other sensitive data.

Critical gaps in existing security systems allow unauthorized traffic to enter and compromise the computing ecosystem. Managing the sophisticated and dynamic methodologies employed in attacks today requires an innovative approach that can co-exist transparently with deployed security and network architectures.

Invisinet Transport Access Control (TAC) provides innovative, proactive protection to network resources by preventing attackers from performing reconnaissance of high-value and mission-critical network assets and by denying them the ability to communicate anonymously.

TAC blocks unauthorized, anonymous traffic at the very first packet of TCP session, effectively disrupting an attacker's strategy by allowing only authorized and authenticated inbound and outbound network sessions.

Threat and Need

Relying on existing security technologies to defend computing infrastructure has proven to be an ineffective decision to stop a determined, sophisticated attacker.

Network reconnaissance, a key step in cyber attacks, uses vulnerability scanners to probe networks and the devices attached to them. Vulnerability scanners, also known as port scanners, attempt to establish TCP/IP connections to various network ports at various network addresses. Network-attached devices reveal information about their characteristics simply by responding to these TCP/IP connection requests.

Current state-of-the-art for securing network-connected devices includes the use of firewalls, VPNs, IPS, and encryption. Each technology accomplishes a specific mission within the security regime. The demarcation point at each security layer exposes information about services and network applications provided when communications protocols are not specifically designed to prevent such information leakage.

Information being leaked, even in the presence of firewalls, contains the existence and identity of servers and network applications. This information is exposed because each network-connected device must establish a TCP/IP connection before performing any client authentication. It is this design flaw of TCP/IP that enables vulnerability scanning tools to identify what network applications are present and, in many cases, develop signatures of the network-connected devices, which includes the operating system, network applications, and their release and patch levels. This information can then be used to develop strategies to attack the network-connected device. Requiring authentication before establishing a TCP/IP connection closes this security hole and denies attackers information.

Invisinet Transport Access Control (TAC)

Invisinet Transport Access Control (TAC) authenticates users and client applications on first packet receipt in a TCP/IP session. First Packet® Authentication (FPA) protects data and network applications by concealing network applications from port scans, network reconnaissance, and intrusion, while allowing authenticated users to access network applications normally.

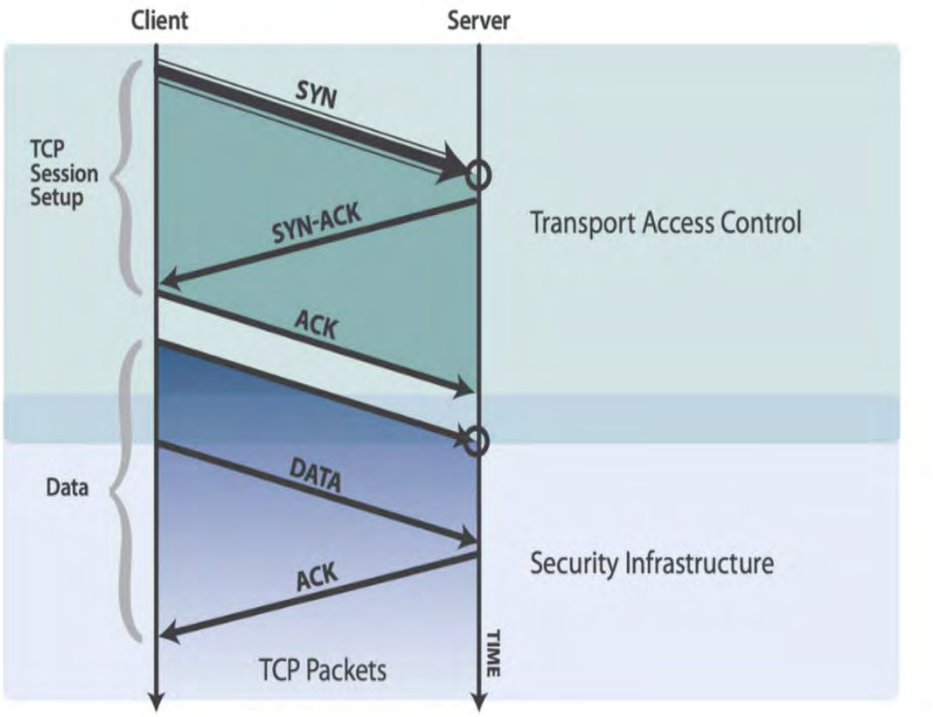


FIG. 2
First Packet Authentication occurs BEFORE connection is established.

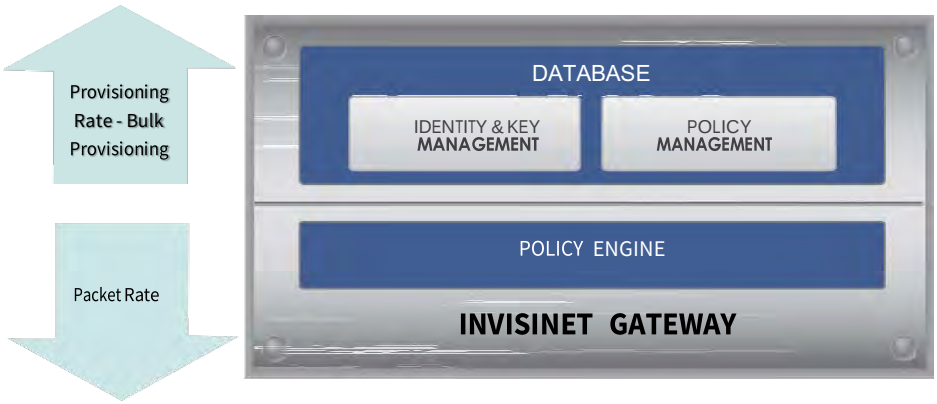
Managing a modern enterprise requires existing security technologies such as firewalls and intrusion prevention systems. But it is also clear that even with these systems, enterprises are being actively attacked and penetrated. Preventing attackers from anonymously gathering critical information, anonymously connecting to network resources, and anonymously removing intellectual property requires a different approach.

Invisinet TAC inserts an identity token into a TCP/IP connection request. TAC extracts, authenticates and applies policy to the received TCP/IP connection requests. TAC can provide both external and internal protection. Externally, TAC protects against unauthorized access, port scans, and network reconnaissance. Internally, TAC prevents viruses, malware, and rogue applications from calling home or contaminating adjacent networks. TAC is tolerant of network and port address translation and is designed to operate transparently, without introducing its own port or network translation complexity. TAC works with mobile

and other devices that use dynamic addressing without requiring administrative updates. All TAC activities can be logged, enabling IT and security personnel to quickly identify and respond to rogue applications and hosts that attempt to infiltrate their networks.

FIG. 3

The architecture components of TAC provide a robust network security solution.



TAC works by generating a single-use identity token for each TCP/IP session. TAC identity tokens are cryptographically generated tokens that communicate authentication information. TAC uses a steganographic overlay to insert the token into the first packet of a TCP/IP connection request. When TAC receives the connection request, it extracts and authenticates the inserted TAC identity token and then applies a security policy (forward, redirect, discard) for the connection request based on the received TAC identity.

TCP/IP session establishment does not allow users to send any user (non-protocol) data, including authentication information. By using a steganographic overlay, TAC can be used during TCP/IP session establishment to provide FPA. Additionally, the size of TCP/IP headers is not increased, enabling TAC to function without consuming any network bandwidth. Each TAC identity token is individually generated, cannot be re-used, and expires after a short period of time.

TAC uses an innovative identity token cache to provide high scalability and low, deterministic latency. The token cache is tolerant of packet loss and enables TAC deployments in low bandwidth and high packet loss environments. The algorithms used in TAC are highly parallelizable, enabling high scalability to take advantage of today's multi-core and multi-processor systems. TAC clients and policy engines can be hosted on a wide variety of platforms, including network appliances, router blades, security blades, laptops, end point payment systems, PDAs, and cell phones. TAC works with IPv4 and IPv6, as well as a variety of network architectures, including client-server, server-server, cloud, and mesh networks.

Identity and Key Management

TAC is designed to integrate smoothly with existing identity and key management systems and requires no modification to existing network applications or servers. TAC is compatible with and complimentary to existing security and authentication technologies, including IPsec, SSL/TLS, and firewalls, providing additional protection not found in these solutions.

Policy Management

In addition to enforcing policy for TAC-authenticated traffic, TAC can also enforce policy to allow unauthenticated traffic to be forwarded, redirected, or discarded. These actions, like all actions performed by TAC, start with the first packet and are performed in real time, giving downstream remediation, analytic, and responsive systems the earliest possible access to live data streams.

Value Proposition

TAC provides significant value to improve security, scalability and performance including:

- Reduced network traffic load

  TAC is complementary to existing network and security topologies. It is lightweight, transparent, and does not add significantly to system latency. Using TAC can remove 99.999% of unauthenticated TCP/IP traffic, which in some cases can comprise 70% or more of all sessions being processed by a firewall. TAC also reduces the load on information protection and detection systems by reducing the amount of data that these systems are required to process and store, while still maintaining log data for evidence gathering.

- Reduced System Cost

  TAC reduces equipment acquisition costs by reducing the use of deep packet inspection and the expensive hardware deep packet inspection requires. Securing the transport layer with TAC results in the reduction of unauthenticated traffic and provides an additional security layer against malware, DDoS attacks, and unauthenticated users.

  TAC can greatly reduce the spread of malware and, most importantly, prevent data exfiltration through perimeter protection. TAC provides an additional layer of security to protect mission-critical and business-critical data and intellectual property.

- Reduced compliance cost

  TAC provides improved compliance to organizations. All requests can be logged. These logs can provide the data needed to support regulatory requirements and requirements associated with internal compliance audits. In addition, TAC authentication can be transparently added to devices and network applications that do not have the ability to perform authentication. The ability to add authentication and logging capabilities to legacy

network applications enables corporations and agencies to meet their compliance and regulatory requirements. Legacy applications continue to operate as normal with TAC being transparently added to the security posture.

Many compliance rules require that complete packet traces of all suspect traffic be maintained for a period of time. By using FPA security tagging, the amount of traffic being stored is greatly reduced, significantly decreasing the storage costs of compliance.

Summary

Cyber war is happening. Cyber-attacks are ever present. The rate at which the advanced persistent threat is escalating is surpassing all estimates. Adversaries are progressing much faster in their ability to successfully attack cyber infrastructure than has been forecast—faster than the prepared defense of today's approaches and technologies.

Firewalls, VPNs, and encryption methodologies are not keeping pace with the barrage of attacks that are being launched on a daily basis. Deep packet inspection-based solutions employed by most firewalls require too much processing power to keep up with the advances in offensive network attack capabilities that are available. Increases in network bandwidth only exacerbate this problem.

Invisinet TAC is a new cyber security technology that blocks network scans and other unauthenticated traffic. TAC compliments existing security with a strong value proposition that can reduce both capital and operational costs.

TAC protects servers, critical assets, and network applications from unauthorized users, attackers, and malware. TAC can also be used for protection against data exfiltration, botnets, and other malware. Specifically, TAC:

- **Authenticates the first packet of a session**
- **Filters and controls network access to resources while preserving existing investments in cyber security**
- **Blocks network scans (by cloaking TAC-protected systems from unauthorized users)**
- **Provides low, deterministic latency with highly scalable throughput**

Security must go beyond host-based and network-based information—and far beyond simple anti-virus and network intrusion detection to stop reconnaissance and anonymous unauthorized connections. Enterprises must focus security resources to look inside the right packets, files, and email instead of ineffectively mulling through all data streams, including anonymous and unauthorized traffic.