From Zero Trust to Adaptive Cyber Defense

Invisinet Identity Based Zero Trust Network Access

Solution Brief

INVISINET
Where Zero Trust Begins

Introduction

Enterprises and service providers need to deliver more secure and resilient business services in today’s rapidly evolving technology, computing and cyber threat environments.

Adaptive Cyber Defense

This need can be addressed by implementing adaptive security models that prevent known and unknown attacks, rather than simply detecting and reacting to attacks once networks and sensitive data have already been breached. Developed for the U.S. Department of Defense, Invisinet provides an adaptive cyber defense solution that proactively isolates cloud services, cloaks and protects IoT devices, and segments IT and OT networks. This new level of real-time protection blocks or redirects unidentified and unauthorized traffic to stop cyber-attacks and unauthorized access, port scanning, and reconnaissance. This greatly reduces risk, simplifies compliance, and increases operational efficiency by eliminating unauthorized traffic from networks and servers.

End-to-End Trust Solution

The Invisinet identity-based, adaptive trust model for network security operates end-to-end across network and cloud boundaries with multiple policy enforcement points, without impacting network compatibility. This provides high throughput and low latency network security that operates pre-session, in real time, before next generation firewall and application security defenses engage. Invisinet uses a highly scalable, non-interactive authentication protocol that does not rely on signatures, sandboxing, or deep packet inspection.

Operating at the transport layer, Invisinet is compatible with existing network and security technologies and middle boxes.

How it Works

Invisinet uses a patented approach to authenticate network sessions, called First Packet Authentication. Transport Control Protocol (TCP), the internet protocol used to connect, does not allow identity credentials to be exchanged until after a network session is fully established. This widely exploited flaw in networks exposes critical resources to attack from the Internet and insider threats. You can’t know whom your network device is “talking to” until the conversation is underway. Invisinet TransportAccess Control (TAC) enhances TCP by closing this vulnerability with cryptographic single-use identity secure tokens to authenticate TCP/IP requests before a session is established. No session is established until TAC software authenticates the identity token and applies a security policy. In this way, TAC cloaks and protects network resources from network reconnaissance, port scans, and many other forms of unauthorized access. After Invisinet is deployed, your network is a “black hole” that will not emit any information (not even a SYN/ACK packet) until the right to communicate with network resources is established. Log records are generated for each policy action, providing real-time information on unidentified and unauthorized access to event management systems for early detection of insider or third-party incidents and for compliance reporting

Key Deployment Use Cases

Micro-Segmentation

Network or micro-segmentation is a security and compliance best practice that is difficult and costly to implement with traditional approaches of maintaining ACLs and firewall rules. Firewalls have high administrative overhead, as well as network topology dependencies, and when used in data center interior network segmentation can be resource-intensive and can impact application performance. Invisinet provides a new software-based approach to segmentation with identity-based access controls to block or allow network connections. This provides granular security zones on shared networks or clouds.

Cloak and Protect Servers & Cloud Services

Invisinet TAC provides a new level of cyber defense to isolate and protect critical services and provide access attribution across enterprises and hybrid clouds. As shown in Fig 1, the virtual InvisiGate can be placed between an access network or campus, and the servers, enclaves, or data centers to be segmented and protected. Similarly, IT networks can be isolated from OT networks and devices.

Protect Management & Control Networks

Management and control networks are the foundation upon which business systems are built. They need to be further protected from cyber-attacks and insider threats, including privileged account and third-party risks. Invisinet TAC isolates

and protects IT management networks, control planes, and management systems from unauthorized users and devices. This additional layer of protection lowers risks of IT or Operation Technology (OT) management systems being attacked and provides identity attribution information for each network session.

Software Defined Perimeter

Private Network (VPN) and network boundaries applies policy at multiple enforcement points. This end-to-end security architecture reduces risks from remote and branch office access into corporate networks or to cloud services, while increasing your security and compliance posture. Distributed cloud services like blockchain can be protected from unauthorized access and DDoS attacks.

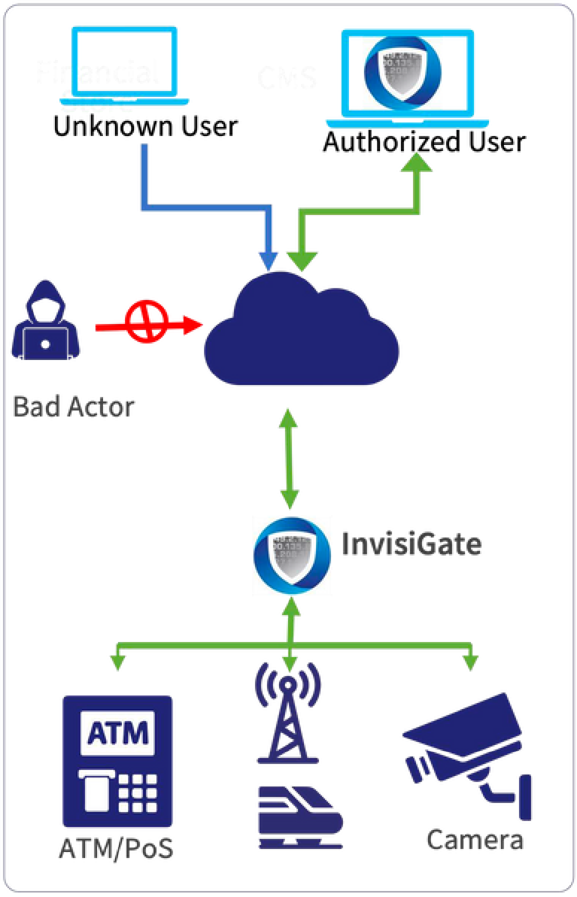


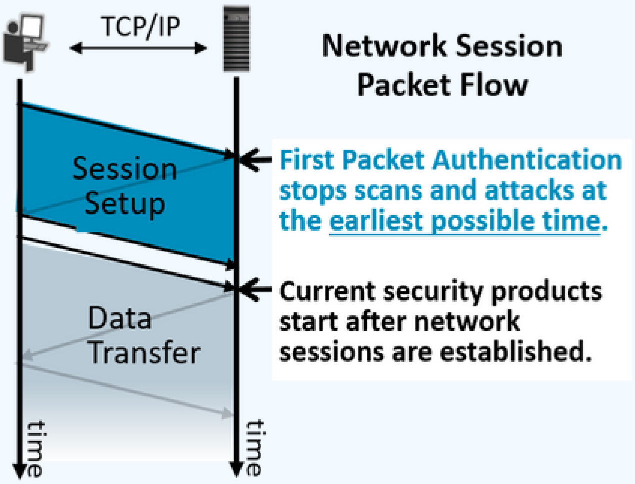
FIG 1 -

USE CASE: OPERATIONAL DEVICES AND CRITICAL INFRASTRUCTURE

Protect ICS and IIoT Systems

The Invisinet approach to micro-segmentation and isolation provides many advantages for Industrial Control Systems (ICS) and the Industrial Internet of Things (IIoT) including infrastructure and topology independence that is multi-vendor and heterogeneous. Invisinet TAC can be integrated into ICS controllers, compute, and edge devices, with support for legacy brownfield environments.

Unique Capabilities and Differentiators


TCP/IP
Network Session Packet Flow
Session Setup
Data Transfer
time
time
First Packet Authentication stops scans and attacks at the earliest possible time.
Current security products start after network sessions are established.

The Invisinet solution can be flexibly deployed as physical, virtual or cloud appliances and as software and hardware endpoints in corporate networks, in private and public clouds and for remote users over the Internet.

First Packet Authentication™

Invisinet TAC authenticates identityandapplies security policy on the first packet of network sessions. A cryptographic single-use identity token is inserted into the first packet of a TCP session. The token is then resolved to authenticate the identity of the TCP connection requestor and apply security policy — forward (with NAT or QOS classification) or drop — to the connection request. First Packet Authentication provides low and deterministic latency; no deep packet or content inspection is required.

Dynamic Identity Integration

Invisinet TAC integrates with Microsoft Active Directory, Cisco Identity Services Engine (ISE), and other identity systems to dynamically learn user and device identities and simplify configuration of policy for accessing resources. InvisiGate can also be configured with static identities and can map identity to certificate or an IP or MAC address.

Easy to Deploy and Maintain

Invisinet TAC operates in a “set it and forget it” mode. TAC gateways and endpoints securely distribute and transparently manage session keys for identity tokens. No additional management or action is required by IT or security staff. This simplifies management processes and eliminates the risk and complexity of maintaining stored keys.

Blocks Network Scanning

Invisinet TAC blocks network, server, and cloud port scanning and reconnaissance from unidentified and unauthorized users. Blocking port scanning effectively stops attackers in their tracks — you can't attack what you can't see — effectively cloaking the protected cloud or server resource. This includes "low and slow" scans that avoid traditional detection approaches. This greatly lowers the risk of key servers and network equipment being compromised

Identity Attribution

Authentication of TCP sessions enables TAC to log identity attribution with session information to security event management and analytics systems. This is the earliest possible time that attribution information can be provided, and it is higher quality than session information alone, since addresses can be easily spoofed and should not be used authoritatively for security policy.

End-to-End Protection

Invisinet provides a new level of network and cyber security protection from all access points throughout the enterprise or hybrid cloud. It works across LAN and router boundaries and automatically adjusts to changing network topologies, ensuring that systems are secure end-to-end.

Trust Level Feedback Policy

Invisinet enables external analytics systems and administrators to adaptively adjust the trust level of individual identities. Trust policies are defined on a system wide or per identity group basis. This additional level of adaptive security enhances protection in response to events to ensure resources remain protected.

InvisiGate Features

Key Features

- TCP Identity Token Insertion & Resolution
- First Packet Authentication
- Adjustable Confidence Thresholds
- Dynamic Identity for Users/Devices
- Static Identity for Users/Devices
- Microsoft Active Directory Integration
- Protected Resource Groups
- Unprotected Resource Table
- Traffic Policy - Forward (with NAT or QOSclassification) or Drop
- Traffic Policy – Granular Filter Rules
- Trust Level Policy
- Trust Feedback API
- TCP Session ID (SID) Tagging
- Policy Logging with Identity Attribution
- Adaptive Nulling / Dynamic Blacklisting
- Syslog messages for SIEM integrations
- VLAN support
- FIPS 140-2 Level 1 Validation

Platforms Supported

- Windows 7/10/11, Ubuntu Linux endpoints
- VMware appliances
- AWS, Azure, and KVM

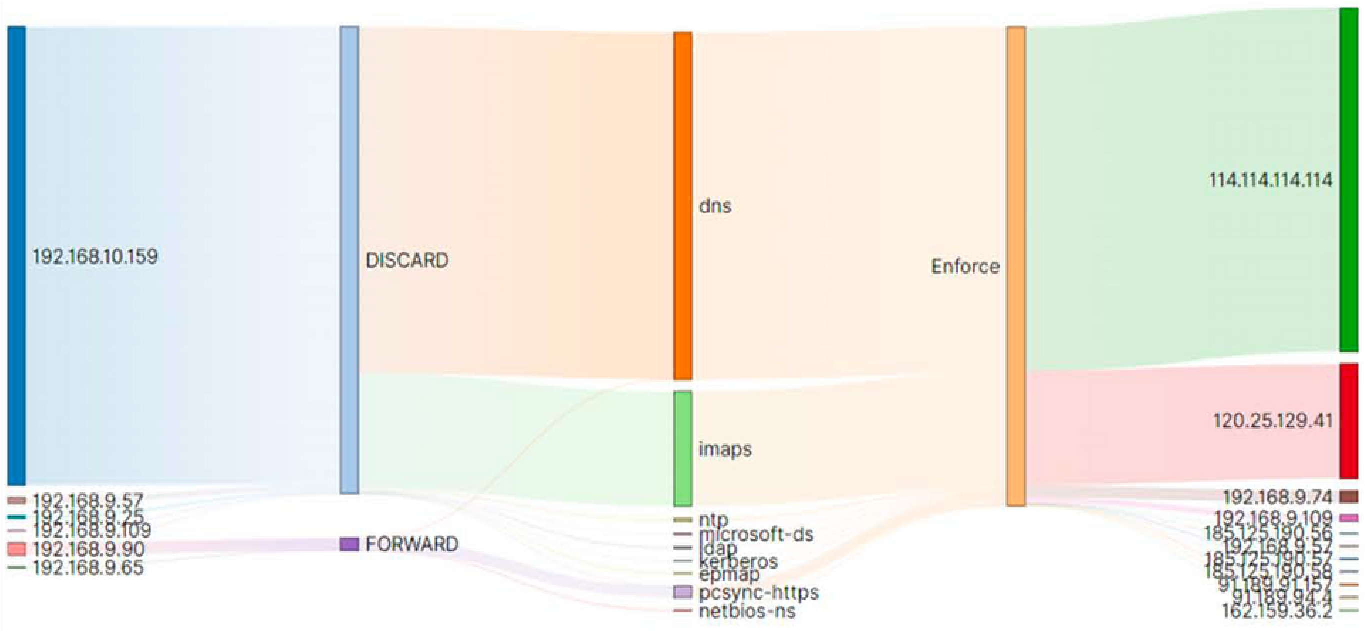
Gateway Modes of Operations

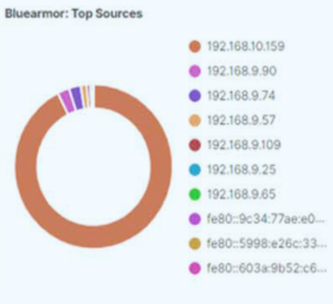
- Bridge Mode
- Policy Monitor Mode
- Policy Enforce Mode
- Layer 2 Transparent Mode
- Layer 3 NAT Mode

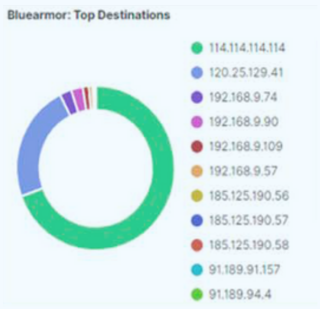
Gateway Management

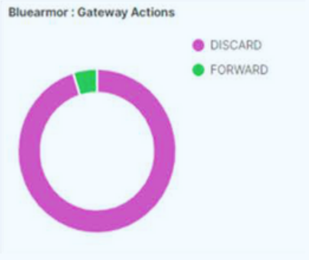
- Command Line and Console Access
- Web-based Management Counsel
- Invisinet Enterprise Manager
- Integrated Database
- REST APIs
- Integrated Database

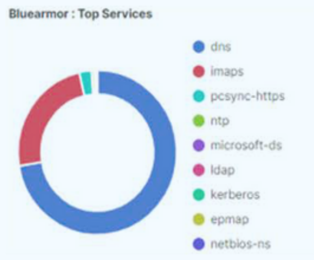
Sankey-Diagram











www.invisinet.com | info@invisinet.com

INVISINET
Where Zero Trust Begins

About Invisinet

Invisinet provides adaptive, zero trust cyberdefense to empower our customers to become more secure and resilient in today's rapidly evolving threat environments. Our patented First Packet Authentication™ technology authenticates identity and enforces security policy on the first packet of network sessions. This new level of real-time protection blocks or redirects unidentified and unauthorized traffic at the earliest possible time to stop discovery, access, and possible breach of your critical network resources. In addition to providing virtual airgap between critical resources based on identity, Invisinet also enables identity-based microsegments without requiring any physical or logical changes to your network. Reduce your cyber-risk using the most simple, certain and effective identity-based attack prevention.