ThreatSTOP Shield IP Firewall for Microsoft Azure

Key benefits:

- Automatically delivers continuous, real-time threat intelligence to your Azure DNS servers based on user-defined policies.
- Proactively deflects inbound malware, DDoS and other attacks, regardless of the attack type or vulnerability. Renders your network invisible to scanners, so attackers move on.
- Prevents data theft and corruption by stopping malware from "phoning home" to threat actors. Prevents activation of ransomware.
- Cloud-based scalable service is easy to deploy and manage

Operationalized Threat Intelligence for Microsoft Azure

Securing your Azure environment is paramount. The ThreatSTOP Shield Platform delivers scalable, easy-to-use protection for cloud workloads that blocks known and emerging threats immediately. ThreatSTOP IP Firewall can be deployed quickly on new and existing Azure networks.

ThreatSTOP IP Firewall is a powerful service that automatically blocks unwanted and dangerous inbound and outbound connections with the command and control IP infrastructure used by threat actors, across a broad range of attack vectors.

ThreatSTOP IP Firewall delivers up-to-the-minute protection against advanced attacks, and enhances your existing security posture by adding a powerful layer of security that functions at the IP infrastructure level. IP Firewall delivers immediate blocking of inbound and outbound network traffic including: Malware, botnets, scanners, phishing, ransomware, DDoS, geo targets, and more.

Protect your Azure IP Infrastructure

The ThreatSTOP Shield Platform empowers users to customize and manage security policies composed of threat types, severity levels, and user-defined block lists and whitelists. Once enabled, these policies function as a set of dynamic IP Firewall rules to protect Azure workloads. Then, ThreatSTOP's real-time reporting provides visibility into blocked threats and affected machines to aid in quick remediation.

The service protects Azure environments by automatically delivering real-time threat intelligence policy updates for enforcement within the Azure network. A cloud-based service, it is easy to deploy and manage, and does not require upgrades to your infrastructure or new hardware. Once deployed, ThreatSTOP IP Firewall provides immediate relief by preventing inbound attacks and the exfiltration or corruption of data, and blocking unwanted connections that consume bandwidth and pose risks to network security.

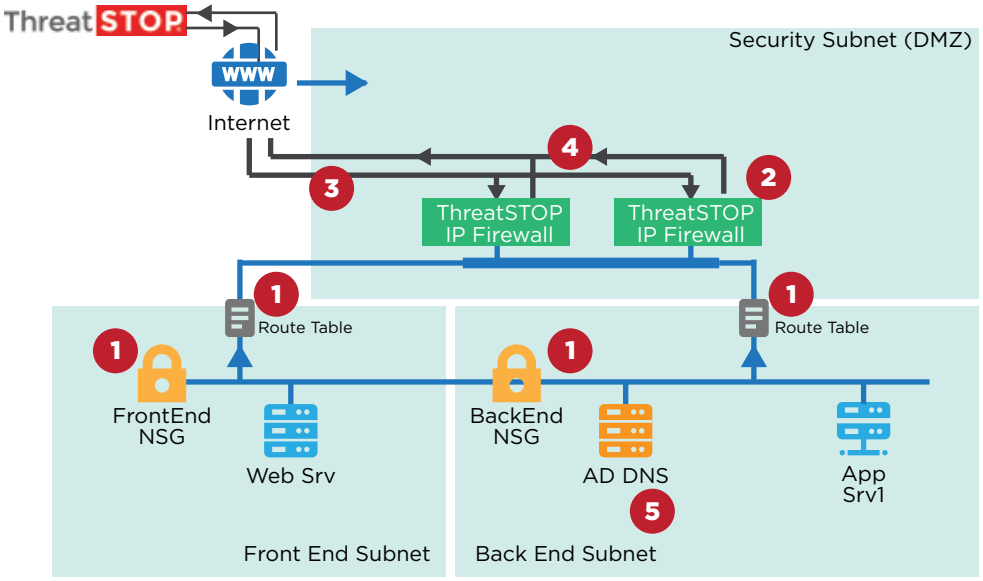
Operationalizing Best-in-Class Threat Intelligence

ThreatSTOP IP Firewall leverages the company's Shield Platform, a comprehensive and authoritative database of IP addresses, domains and the infrastructure used for cyberattacks. ThreatSTOP's world-class security team curates the latest threat information and cross-correlates threat data against multiple public and private sources to ensure a high degree of accuracy and prevent false positives. Policies created using the Shield Platform are continuously and automatically updated to protect against new and emerging threats.

How it Works: IP Firewall for Azure

Leveraging the power of the ThreatSTOP Shield platform, ThreatSTOP's IP Firewall for Azure provides comprehensive inbound and outbound threat protection against constantly evolving threats using real-time threat intelligence to block communication with malicious IP addresses.

- Blocks inbound attacks and unwanted traffic, and prevents data loss and corruption
- Define a policy that fits your security posture, including custom whitelists and block lists
- Policies are automatically and continuously updated with real-time threat data
- Deploys in an hour and easily scales to secure your entire cloud surface area
- Powerful reporting delivers visibility to blocked threats and aids in remediation
- Proven to reduce unwanted inbound network traffic by 20% to 30%



1. NSG and Route Tables enforce use of the ThreatSTOP IP Firewall
2. ThreatSTOP IP Firewall provides inbound & outbound protection
3. Security policies from ThreatSTOP are transmitted with TSIG authentication. Policies are customizable for each IP Firewall device
4. Logs sent to ThreatSTOP for analysis and reporting, and are received via SSL
5. AD queries are sent to internal DNS for lookup

Shield Your Azure Workloads

Protect your workloads, VDI, and data hosted on Azure with an effective new security layer. ThreatSTOP Shield delivers automated continuous protection against today's active threats

Operationalize Threat Intelligence

Unlike traditional threat intelligence used to investigate incidents after they occur, ThreatSTOP Shield's dynamic threat updates deliver real-time proactive protection directly to Azure

Secure Your Cloud Quickly

Deployment of ThreatSTOP Shield in your new or existing Azure environment is straightforward and quick with easy to use, scalable solution templates that automate implementation