Protecting Microsoft Azure Workloads with Sanitized DNS

April 2023

Sanitized DNS for Microsoft Azure Workloads

Attackers & malware leverage recursive DNS to compromise an organization, including attacks on Microsoft Azure workloads

To protect these valuable assets you need visibility & control for all Microsoft Azure external recursive DNS traffic, ensuring that only clean and safe DNS requests are resolved - all malicious requests are proactively blocked

Akamai **Secure Internet Access + Azure Firewall**

Sanitized DNS for Azure Workloads

Simplicity

Simple integration with Azure Firewall - DNS traffic is redirected to Akamai's global cloud security platform

Proactive Security

DNS requests checked against real-time threat intelligence, proactively blocking malicious requests

Insights

All DNS requests are logged for analysis, investigation & compliance

Sanitized DNS for Microsoft Azure Workloads

Microsoft Azure Firewall & Akamai Secure Internet Access

- Sanitized DNS - only safe and legitimate DNS traffic is resolved
- Malicious DNS requests including DNS exfiltration proactively blocked with real-time threat protection
- Create DNS allow or deny lists
- All DNS requests logged for analysis and investigation
- Secures your Azure DNS traffic with DNS over TLS (DoT) and DNSSec

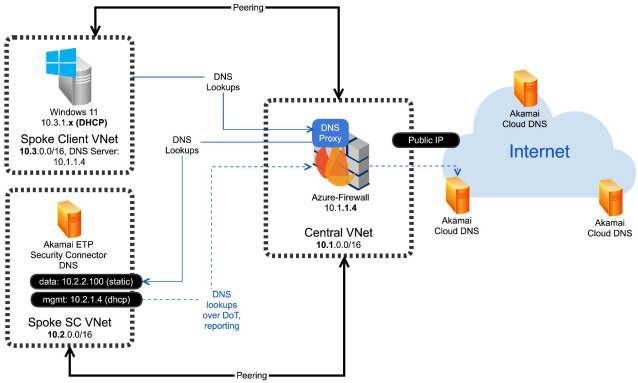
Benefits

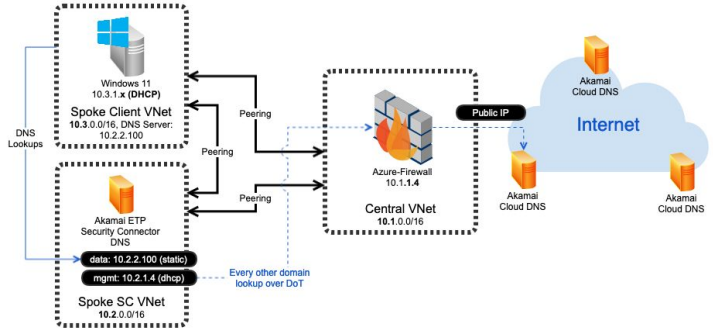
- Improves Azure workload security & reduces risk by blocking access to risky domains
- 100% visibility & logging for all external resources requested
- Helps meet compliance & audit requirements

Key Features

Feature	
Deployment	Quick and simple deployment
Proactive Security	Real-time threat protection to proactively block malicious DNS requests including DNS exfiltration - only safe and legitimate DNS traffic is allowed
Flexible Policies	Create DNS allow or deny lists to control DNS resolution
Threat Alerts	Threat alerts are available directly in Secure Internet Access and can be integrated into your SIEM
Logging	DNS requests are logged for analysis, investigation and compliance
Secure DNS	DNS traffic is secured end-to-end with DNS over TLS (DoT) and DNSSec

Simple Activation & Deployment





Sanitized DNS for an Azure Virtual Network	Sanitized DNS directly through an Azure Firewall
• Virtual Networks where Virtual Instances are deployed need connectivity to the Akamai Security Connectors (Peering). • The Virtual Network DNS Server configuration points to the Akamai Security Connector(s) IP address. • Akamai DNS threat events will include the private IP address of each Virtual Machine to help with remediation.	• The Azure Firewall is acting as a DNS Proxy. • The Virtual Network DNS Server is configured with the Azure Firewall's private IP address. • The Primary DNS log will be Azure Firewall DNS logs. • Akamai DNS threat events will need correlation with Azure Firewall DNS logs to identify the Virtual Machine that made the request.

Akamai in DNS

The world's largest provider of DNS services

Authoritative DNS

Provided authoritative DNS since 1999

DNS is the core of Akamai Content Delivery

200 of Fortune 500 companies use Akamai

Used by world's premier web properties

Recursive DNS

Provided recursive DNS since 1999

World's largest provider of DNS to ISPs & MNOs

Over 7 Trillion DNS requests resolved daily

Over 120 DNS POPs globally

Akamai's Real-time Threat Intelligence

Akamai Data
- Up to 30% of total web traffic
- 7 trillion daily DNS queries
- Akamai Security product logs

Third-Party Data
- Raw threat data
- Premium threat intelligence

Public Data
- WHOIS data
- Registrar data

Automated statistical, trend, and pattern analysis of structured and unstructured data

Data scientists fuse, clean, and scour data for actionable threat intelligence

Akamai CSI
- Big Data analytics deliver cloud-based threat intelligence that is continuously updated
- Multi-layered approach of machines and people
- Fueled by enterprise and consumer traffic that is augmented with third-party sources
- Feedback - if an engine detects a new threat, it is added to the threat intel so all customers are protected
- Lookback - customer logs for past 7 days are compared against most recent threat intel and new alerts created

Useful Information

- Secure Internet Access Azure Marketplace listing
- Secure Internet Access Product Brief
- Secure Internet Access Product Page
- Azure Security Connector setup instructions
- Example Terraform Script


Akamai