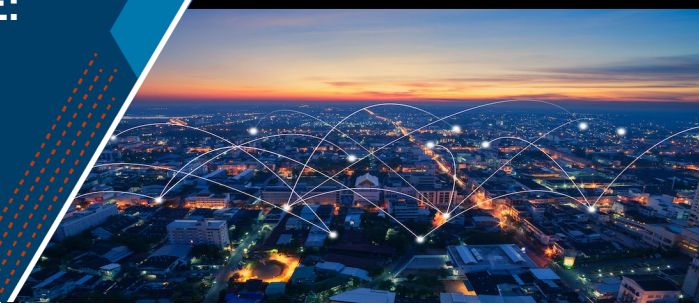
TLP:CLEAR

IMPLEMENTATION GUIDANCE: SEGMENTING TRAFFIC AND TELEMETRY FROM AGENCY GUEST NETWORKS AND SECURITY APPLIANCES



OVERVIEW

The Cybersecurity and Infrastructure Security Agency's (CISA) mission to understand, manage, and reduce cybersecurity risk includes defending federal civilian executive branch (FCEB) agencies against cybersecurity threats. CISA does this by providing security services like the Protective Domain Name System (DNS) Resolver service, monitoring agency traffic, and detecting events occurring on federal networks. When events of operational interest are detected, they must be triaged and analyzed in a timely manner to determine if they merit further analysis.

Agency requirements to adopt CISA security services like Protective DNS, and to provide traffic and telemetry to CISA, extend to agency guest networks, security appliances, and cybersecurity lab networks. These traffic sources frequently generate false positive events capable of overwhelming agency security operations teams, wasting precious resources, and potentially preventing resolution of cyber incidents before major damage occurs. CISA developed this implementation guidance to enable agencies to provide traffic and telemetry so events can be prioritized and triaged in a timely manner.

AUDIENCE

This document provides guidance for FCEB agency IT and cybersecurity professionals who need to forward DNS queries and network traffic, logs, and other telemetry to CISA for monitoring and analysis.

SCOPE

This guidance applies when a federal agency has any of the following assets, whether operated by or on behalf of the agency, whose traffic is routed through CISA security capabilities, including Protective DNS, traditional Trusted Internet Connections (TIC) access points, or similar capabilities:

- **Guest Networks:** Networks that are used by non-agency endpoints for purposes of accessing the internet or other network-based services. For example, an agency might offer a wireless network to provide visitors with internet access.
- **Security Appliances:** Security capabilities such as firewalls, endpoint detection and response (EDR), and intrusion detection and prevention systems (IDPSs) that resolve known malicious domains or that generate or receive potentially malicious traffic (e.g., security scanners).
- **Cybersecurity Lab Networks:** Special purpose lab networks that require access to known malicious destinations or permit resolution of known malicious domains. For example, an agency might use a lab for malicious software analysis or security research.

MANAGE AGENCY DNS TRAFFIC IN PROTECTIVE DNS

Agencies must route all DNS requests originating from federal information systems, including guest networks, security appliances, and cybersecurity lab networks, through Protective DNS. To facilitate triage and analysis of detected anomalous events, agencies should ensure that all associated traffic is segmented off and that source assets are both labelled appropriately (e.g., "Guest wireless network HQ lobby") within Protective DNS and can be grouped by source sets[1] of the same type (e.g., guest networks). Agencies may consider deploying separate caching DNS infrastructure dedicated to such assets to facilitate differentiation and to limit potential impacts to their agency enterprise DNS infrastructure.

1 – See Protective DNS User Guide for full details on authorized sources/source set management.

TLP:CLEAR

Examples of separate DNS traffic, also depicted in Figure 1, include:

- Guest networks, security appliances, and cybersecurity lab networks use separate agency-managed DNS resolver infrastructure from that used by the agency enterprise.
- Guest networks, security appliances, and cybersecurity lab networks directly access Protective DNS from behind a network address translation (NAT) point. The address is distinct from that used by the agency enterprise DNS resolver.

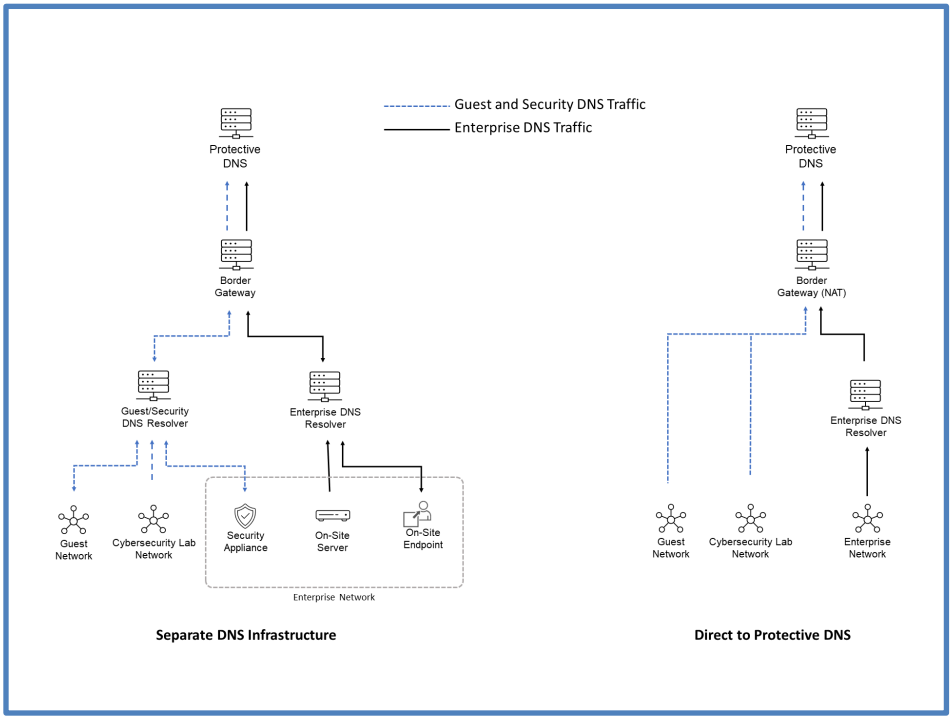


Figure 1: Examples Depicting Two Possible Use Cases With and Without Dedicated DNS Infrastructure

SEPARATE THE NETWORK TRAFFIC PROVIDED FOR INSPECTION

When providing network traffic for analysis by CISA, agencies should use dedicated source addresses or networks for guest networks, security appliances, and cybersecurity lab networks that are distinct from those used to send enterprise traffic to CISA security services. Segmenting the guest and cybersecurity lab networks, ideally through physical means, can help facilitate this traffic differentiation. When the network traffic includes potentially malicious traffic sources (e.g., guest networks, security scanners, honeypots, cybersecurity lab networks), this setup can help to identify the source and limit potential impacts to the agency enterprise.

Examples of separate network traffic, also depicted in Figure 2, include:

- Guest networks, security appliances, cybersecurity lab networks, and enterprise networks share physical infrastructure, but the guest and security traffic are sent upstream via distinct virtual local area networks (VLANs).
- Guest networks and cybersecurity lab networks are physically segmented from the enterprise network, with the traffic sent upstream via a dedicated internet service provider (ISP) link.

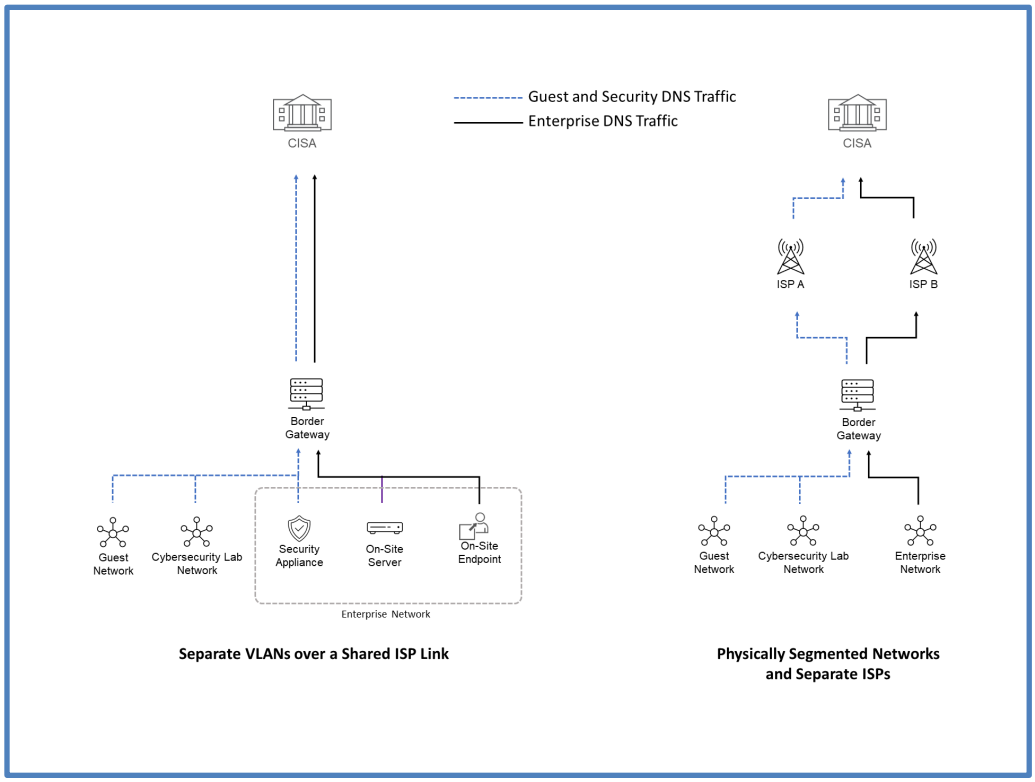


Figure 2: Examples Depicting Two Possible Use Cases Separating Traffic Using VLANs Over a Shared ISP and Physical Segmentation via Separate ISPs

LABEL OR SEPARATE LOG AND SECURITY ALERT INFORMATION

Where agencies provide logs, security alerts, or other telemetry to CISA (e.g., via CISA's Cloud Log Aggregation Warehouse [CLAW]), they should label or otherwise differentiate the telemetry for guest networks, security appliances, or cybersecurity lab networks. Alternatively, agencies may work with CISA to determine what security alerts and other telemetry to send for guest networks, security appliances, and cybersecurity lab networks.

Examples of differentiating telemetry sent to CISA, also depicted in Figure 3, include:

- The security alerts generated by guest networks, security appliances, and cybersecurity lab networks are stored separately from security alerts covering the agency enterprise.
- The security alerts generated by guest networks, security appliances, and cybersecurity lab networks' traffic are tagged prior to transmission to CISA.

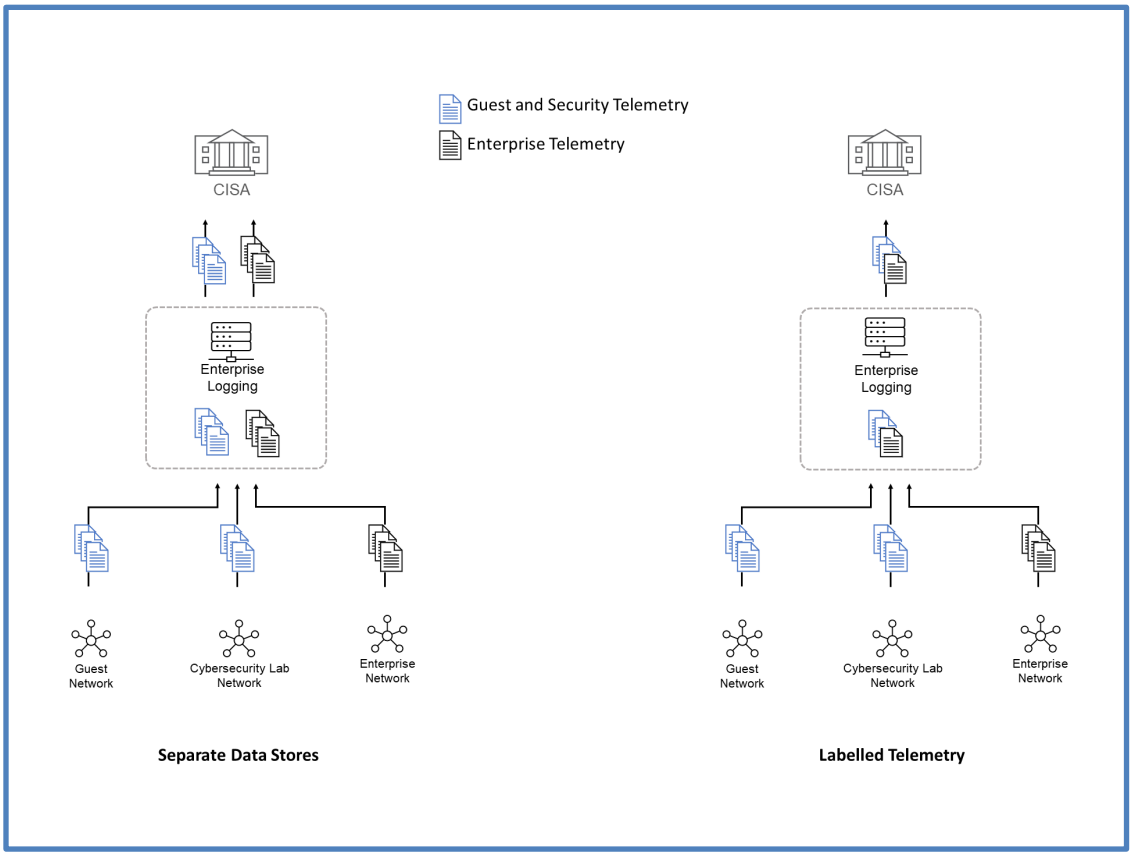


Figure 3: Examples of Possible Use Cases for Labeling and Separating Log and Security Alert Information

INFORM GUEST USERS OF MONITORING

When guest user traffic, including both network traffic and DNS traffic, is routed to CISA protective capabilities (e.g., Protective DNS, EINSTEIN), agencies should ensure that a legal banner is displayed prior to allowing guest users to access the network.

CONTACT INFORMATION

For inquiries regarding implementation of Protective DNS, CLAW or other questions, contact CyberSharedServices@cisa.dhs.gov.