Enhancing Network Obfuscation through harmonized SASE Capabilities

A harmonized blend of SASE capabilities to protect enterprise resources.

Introduction

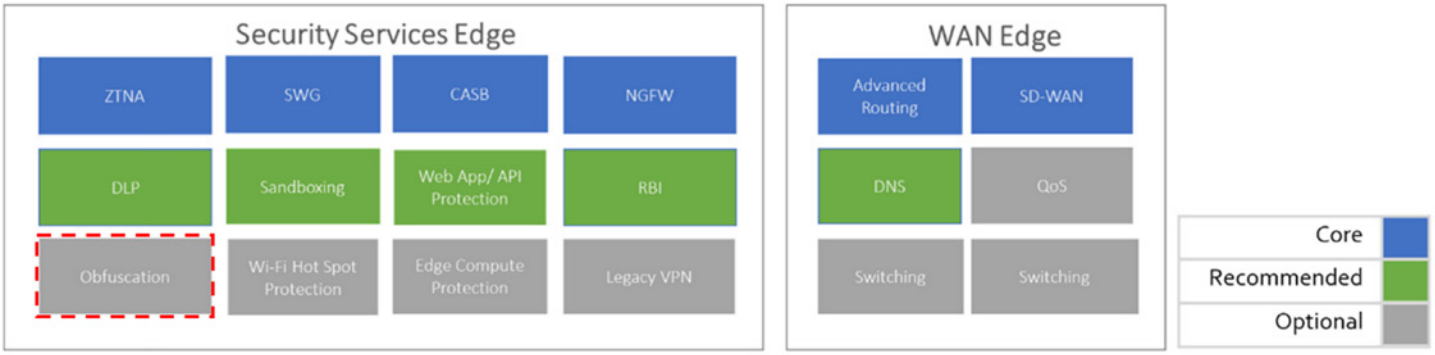
In a Secure Access Service Edge (SASE) architecture, Network Obfuscation is a Security Service Edge (SSE) capability. Network Obfuscation refers to the hiding of end-users (Entities) and Applications (Resources) on the public internet and within the enterprise. In isolation, Network Obfuscation is achieved using Domain Name Service (DNS) Proxy and Carrier Grade Network Address Translation (CGNAT). However, in the context of a SASE architecture, Network Obfuscation is enhanced by harmonising with other SASE capabilities. Only through the blending of these capabilities via a single pane of glass can the use-case of keeping threat actors from knowing the existence of enterprise Resources be appropriately and efficiently addressed.

This solution brief shall describe Network Obfuscation in the context of a SASE architecture. It shall highlight how Network Obfuscation is enhanced by harmonizing with other SASE capabilities, specifically Enhanced Routing (using a tunnelling protocol such as IPsec), Zero Trust Network Access (ZTNA) and Next Generation Firewall (NGFW).

Additionally, from a holistic perspective, brief consideration is given to other areas related to Network Obfuscation and SASE in general, such as ease of configuration and management via a single pane of glass as well as Unified versus Disaggregated SASE architectures.

Network Obfuscation Overview

Secure Access Service Edge (SASE), as defined by Gartner, is a combination of Security Service Edge (SSE) capabilities and WAN Edge capabilities delivered via the cloud. Within each 'Edge', there are layers of either networking (such as 'Advanced Routing') or security capabilities (such as 'Zero Trust Network Access' (ZTNA)). Additionally, one of these capabilities is 'Network Obfuscation':



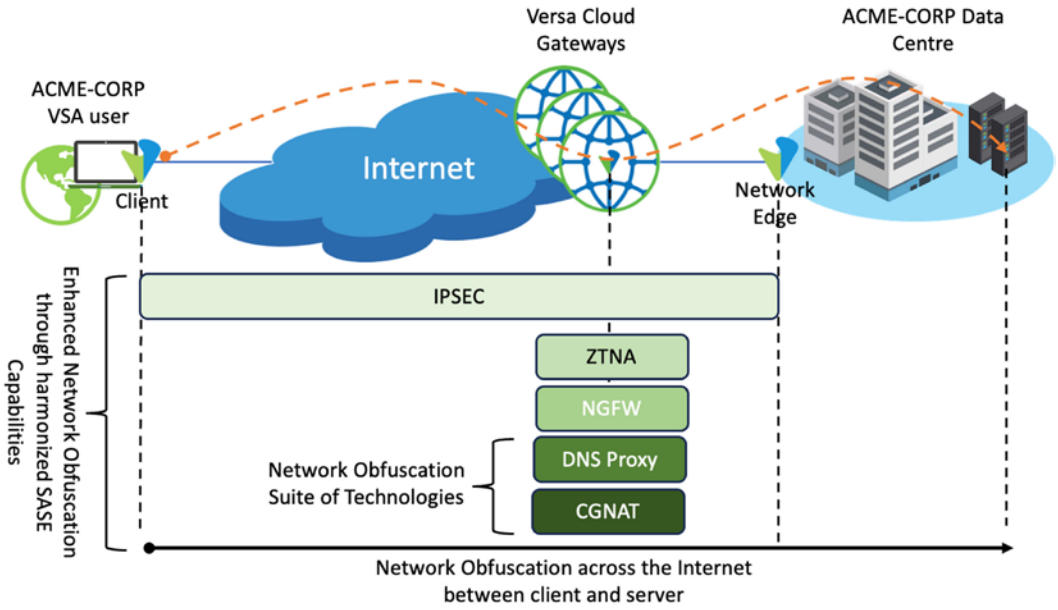
Broadly speaking, Network Obfuscation refers to the hiding of end-users (Entities) and Applications (Resources) on the public internet and within the enterprise. It is also referred to as 'Enterprise Topology Hiding'. More specifically, Network Obfuscation refers to keeping threat actors from knowing the existence of enterprise Resources. This protects enterprise applications from attack vectors like lateral movement and port scanning.

Network Obfuscation is a combination of two technologies: Domain Name Service (DNS) Proxy and Carrier Grade Network Address Translation (CGNAT). Although true, in a SASE context, Network Obfuscation is enhanced by harmonizing with other SASE capabilities. Therefore, a truly effective Network Obfuscation capability should be considered a blend of integrated technologies covering both networking and security disciplines.

In the case of Versa's SASE product, in addition to DNS Proxy and CGNAT, Network Obfuscation is integrated with a tunnelling protocol such as Internet Protocol Security (IPSec) encryption, Zero Trust Network Access (ZTNA) and Next-Generation Firewall (NGFW). Without an integrated suite of technologies such as these, the strength of Network Obfuscation is weakened.

Network Obfuscation is a feature of the Versa Secure Private Access product (VSPA[1]). VSPA is a globally distributed solution that connects Entities, such as users to Resources, such as enterprise applications. Resources can be distributed across private cloud, enterprise data centers (DCs) and public cloud instances.

At a high level, a secure tunnel is used between end user device and network edge. All SSE capabilities are enabled on Versa Cloud Gateways (VCGs) hosted in the cloud:



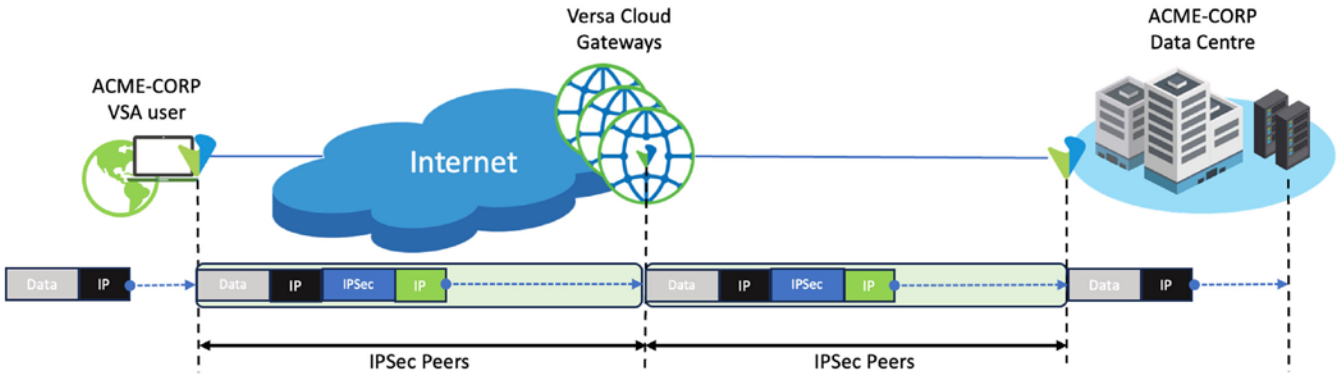
SASE Capabilities

Although the secure tunnel between end user device and VCG can be IPSec, DTLS or TLS, for the purpose of this article IPSec is demonstrated.

IPSec

IPSec is a suite of protocols related to network security. It provides Confidentiality, Integrity, and Authentication (CIA) between communicating IPSec peers.

Between ACME-CORP user and VCG, IPSec is used. If traffic is destined for the ACME-CORP DC, an additional IPSec tunnel between VCG and ACME-CORP DC is used. In effect, IPSec 'stitching' is performed between ACME-CORP user and ACME-CORP DC for traffic destined for Resources in the DC. (An IPSec tunnel between the VCG and customer's DC could originate inbound (i.e., originated by the SSE cloud) or outbound by the DC network device to the VCG in the SSE cloud. Versa supports both approaches):



As a further note, the IPSec tunnel between VCG and ACME-CORP DC could leverage either a Unified or Disaggregated SASE architecture. This is discussed in a following section (Unified SASE).

ZTNA

In 2019 the National Cyber Security Center[2] (NCSC) recommended network architects consider a zero-trust approach[3]. NCSC described zero trust architectures as those that "remove the inherent trust from the network while building confidence in each request. This is achieved through building context through strong authentication, authorisation, device health, and value of the data being accessed".

In terms of building context, the Versa SASE Client periodically reports to the Versa SASE Registrar-Portal and VCGs about the 'health' of the device. This allows the Versa SASE platform to continuously build 'context' information about every Entity and uses that information to authorize access to the network and its Resources. Health related information is sent from the Entity to the VCG in the form of Endpoint Information Objects (EIO). For example:

1. OS Type, version, and OS service-pack information of the accessing Entity.
2. Installed anti-malware and anti-phishing software on the accessing Entity including:
    a. how recently were these updated?
    b. are the security signatures up to date?
3. Whether the Entity is managed or un-managed.
4. Whether the Entity supports disk encryption.
5. Version and running state of applications installed on the Entity.
6. Whether certain registry values are set on the Entity.

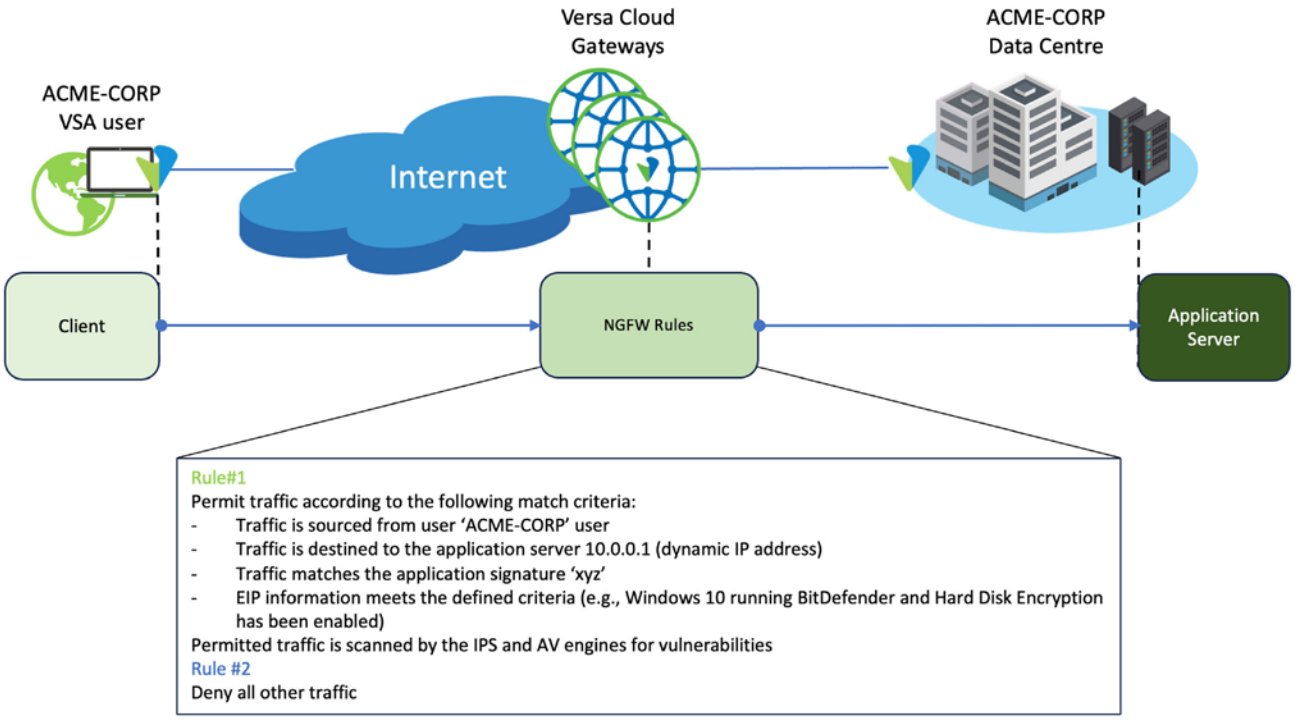
The Versa SASE platform uses EIOs to determine whether to authorize access from the Entity to the requested Resource based on policies using Endpoint Information Profiles (EIP). EIP are used to enforce conditional access based on device posture. For example, based on the EIP, the Entity can be allowed, denied, or provided restricted (quarantined) access to Resources. More on this can be found in the following section (NGFW).

Of course, policies can be crafted on more than just the EIP/device posture of the Entity. For example, match criteria could include username or usergroup as well as tuple and application information of the accessed Resource. Information such as this ensures each request from an Entity to access Resources is built on context as per the principles of ZTNA. More on this can also be found in the following section (NGFW).

NGFW

VCGs support NGFW features. NGFW is a robust security module that has the intelligence to distinguish different types of traffic. NGFW provides network protection beyond that based on ports, protocols, and IP addresses. In addition to traditional firewall capabilities, NGFW includes filtering functions such as an application firewall, an Intrusion Prevention System (IPS), TLS/SSL encrypted traffic inspection, DNS Filtering, File Filtering, Antivirus (AV) and URL Filtering.

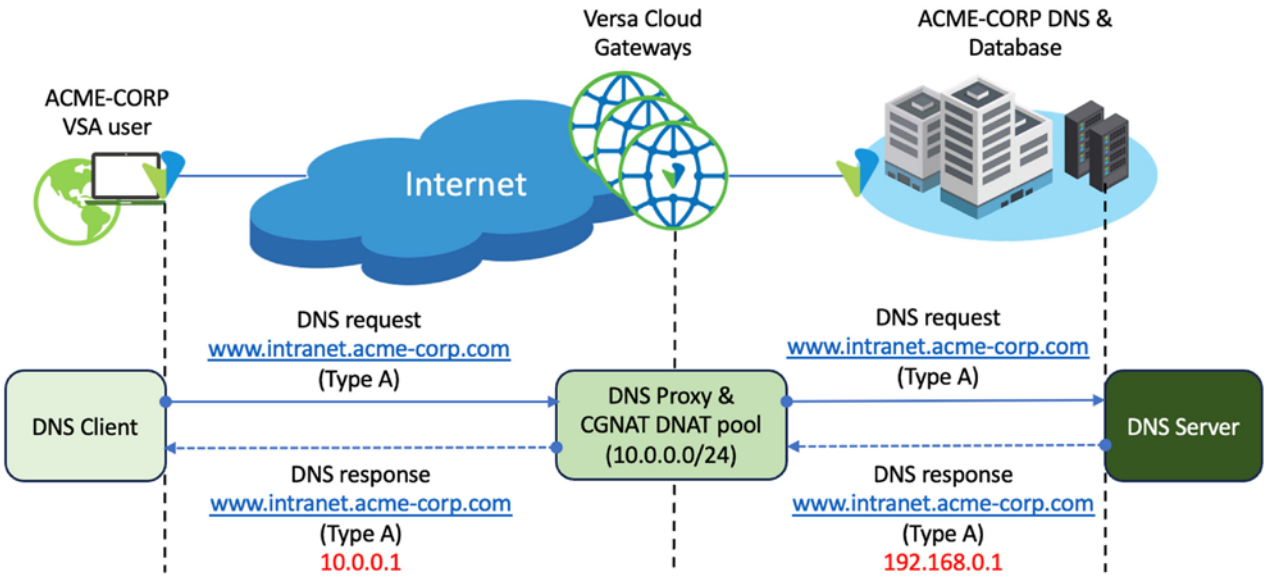
In this example, 'private access' rules are created. Match criteria are defined using a range of possible metadata, such as username and device posture (derived from EIOs). Each rule is associated with a policy action, such as 'permit' or 'deny'. Additionally, the policy action can invoke vulnerability checks throughout the lifetime of the session. For example, AV and IPS scanning may be continuously executed to check for vulnerabilities in data transmitted between Entity and Resource:



DNS Proxy

VCGs support DNS Proxy. A DNS Proxy, in a Network Obfuscation context, responds to a client's DNS query using the server's 'dynamic' destination address. This is retrieved from a CGNAT pool hosted on the VCG. The VCG creates a cache entry in which it binds the 'dynamic' destination IP address to the server's 'actual' IP address. For subsequent DNS requests, the DNS Proxy uses the entry in the cache when it sends its reply to the requestor.

As an example, in the image below, the ACME-CORP user wishes to connect to www.intranet.acme-corp.com. The DNS proxy service running on the VCG intercepts the DNS request. Once intercepted, the DNS Proxy can insert a dynamic IP address (10.0.0.1) for the server from its CGNAT pool. This obfuscates the actual server IP address (192.168.0.1) from the client:

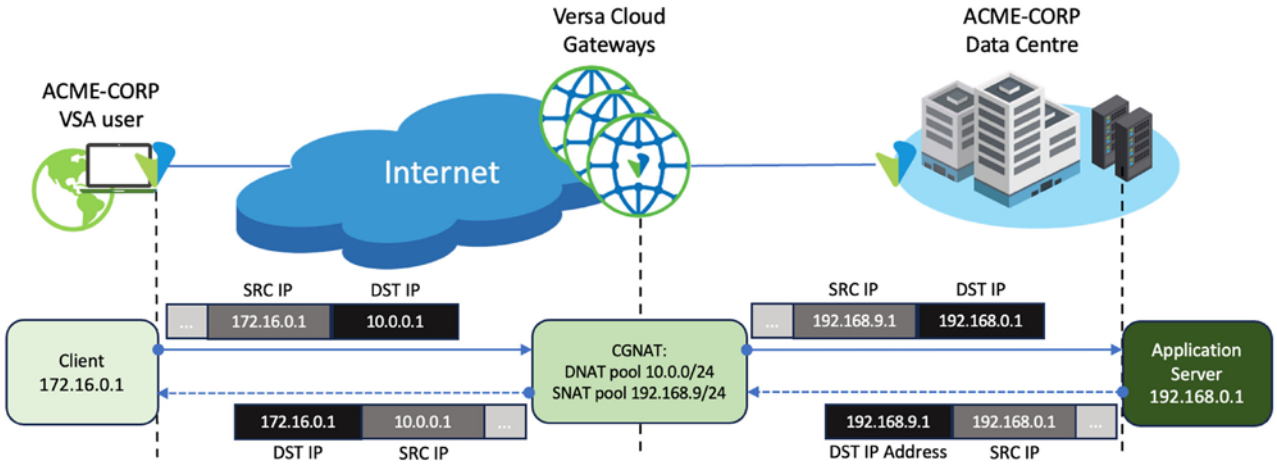


Although not shown, just like any Resource, even the availability of the DNS-Proxy service to an Entity can be controlled using ZTNA policies. As an example, the DNS-Proxy service will deny the existence of a corporate resource, if the endpoint is not compliant with ZTNA policy.

CGNAT

VCGs support CGNAT.

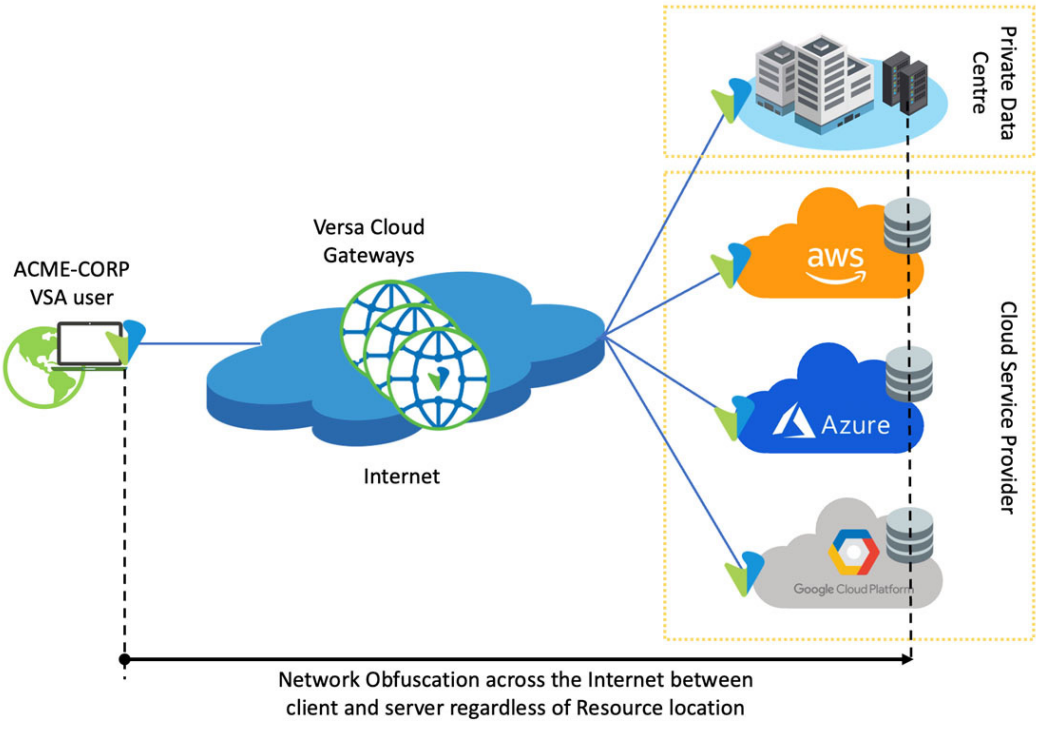
Continuing the example above, once the DNS Proxy cache is populated, as the ACME-CORP user connects to the Application Server hosted in the ACME-CORP DC, the client believes the IP address of the server is 10.0.0.1. However, this is a pool of addresses hosted on the VCG. The VCG will perform Destination Network Address Translation (DNAT) on the packet. This translates the destination IP address from the dynamic IP address (10.0.0.1) to the actual server IP address (192.168.0.1). This obfuscates the server IP address from the client. At the same time, the VCG will perform Source Network Address Translation (SNAT) on the packet. This translates the source IP address from the actual IP address of the client (172.16.0.1) to a dynamic IP address (192.168.9.1) to represent the client. This obfuscates the client IP address from the server. Both client and server actual IP addresses are obfuscated from one another:



Other Considerations

Network Obfuscation of Enterprise Resources Regardless of Location

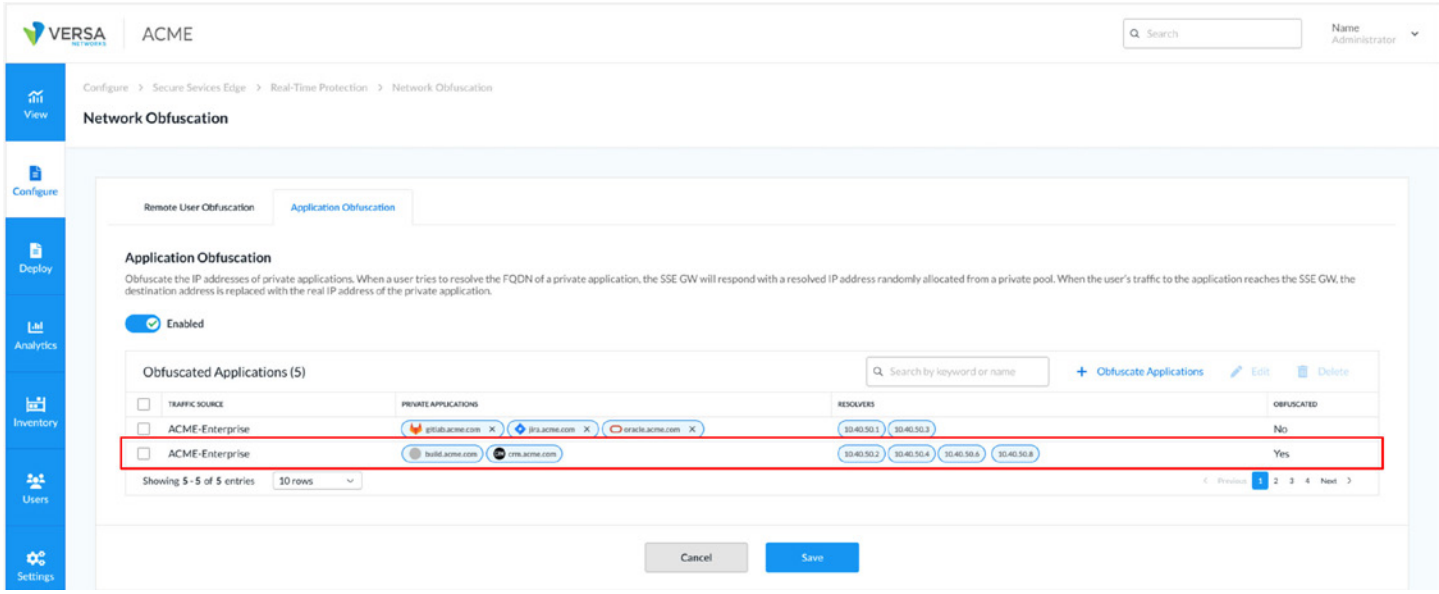
Although focus has been given to Resources hosted within a Private DC, as shown in the diagram below, Network Obfuscation applies to any location hosting enterprise Resources – physical or virtual:



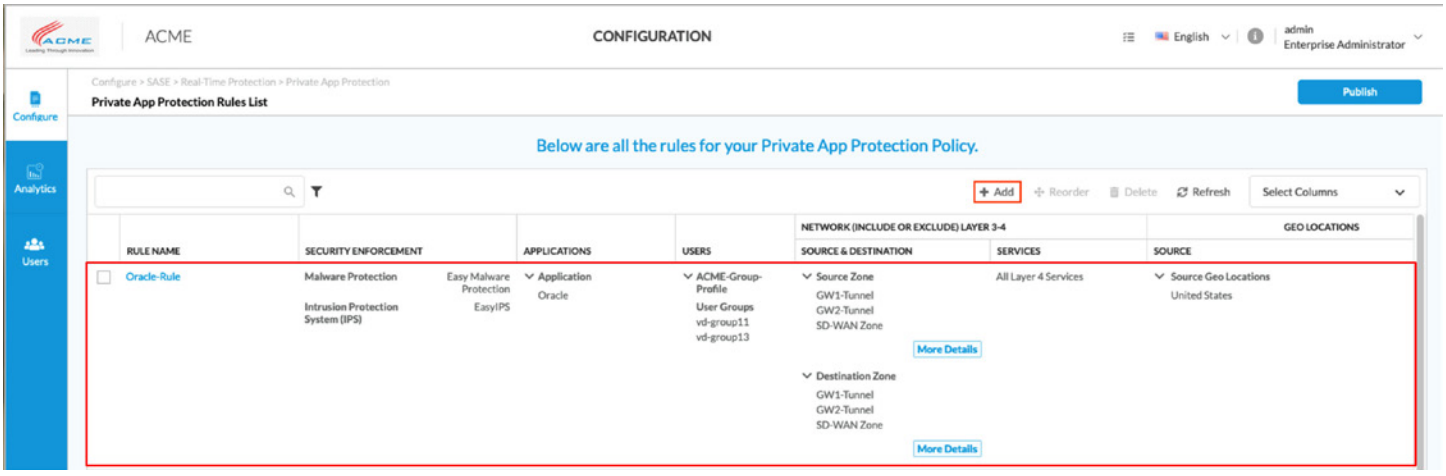
Configuration and Management

Although Network Obfuscation is achieved through the integration of multiple technologies, Versa Concerto (Versa's Orchestration and Lifecycle Management Platform) simplifies policy creation and management. Versa Concerto provides a single pane of glass to manage the SASE platform and its capabilities.

For example, in the following screenshot, DNS Proxy and CGNAT features are configured for applications 'build.acme.com' and 'crn.acme.com':

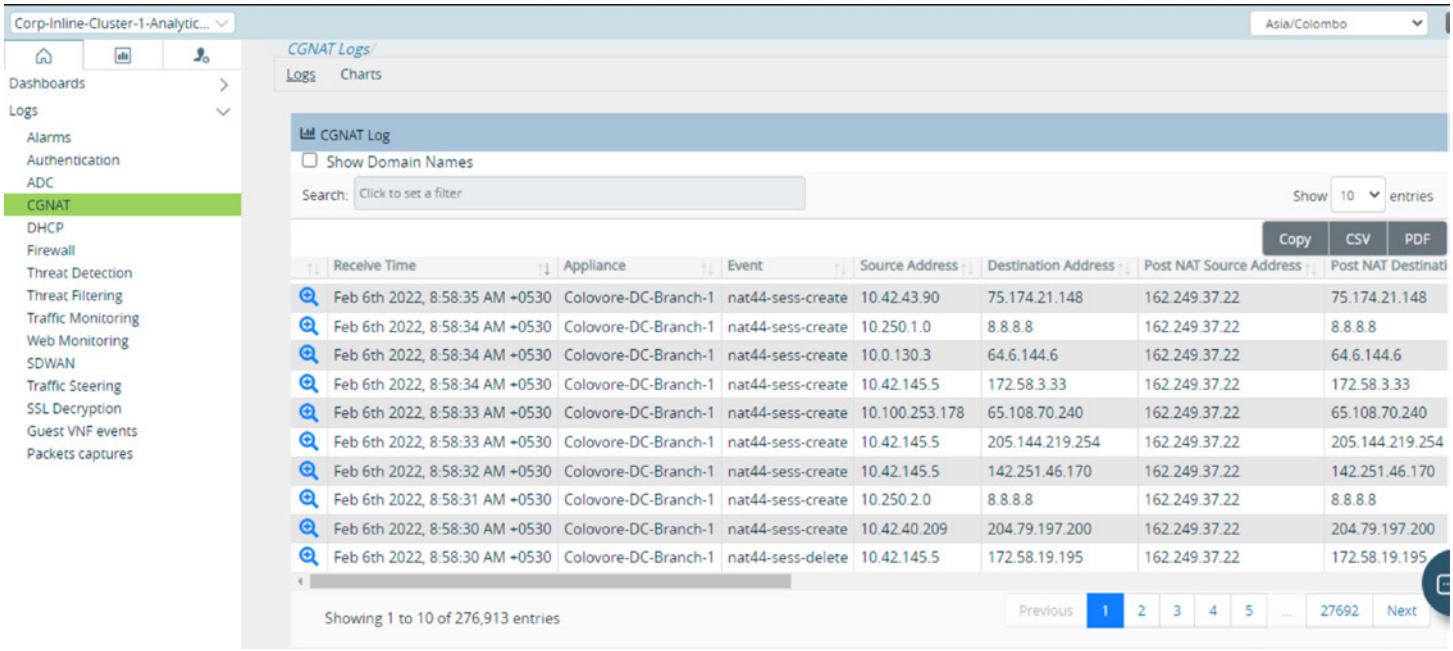


The following screenshot shows an example NGFW/ZTNA rule. This controls access from the Entity to the Resource. In this example, match criteria include the destination application (Oracle); user groups (vd-group-11 & vd-group13); and Geo-Location IP addresses. Also note the 'Security Enforcement' section. Any traffic matching the rule is subject to continuous AV and IPS protection:



At the same time configuration has been simplified, the Network Administrator is still able to create granular rules if required. For example, the Network Administrator can enable Network Obfuscation for sensitive applications only. For non-sensitive applications, Network Obfuscation can be bypassed.

In addition to configuration, as a single pane of glass, Versa Concerto provides access to logging information. For example, the following screenshot shows CGNAT logs which depict pre and post IP CGNAT addresses:



Unified SASE

Versa Networks Unified SASE takes the components of SSE Edge and WAN Edge, including capabilities like Network Obfuscation and natively integrates them into a single architectural framework.

Such an approach has multiple advantages over a Disaggregated SASE approach. For example, the same single pane of glass for management can be used to configure and manage Network Obfuscation in addition to all other SASE features. Another benefit of a Unified SASE architecture is IPSec tunnels can be automatically built between devices thus requiring no manual configuration. Additionally, if multiple paths exist between VCGs and customer DC, Versa probes can pass over the SDWAN fabric to determine underlay performance. This allows preferred paths to be calculated based on factors such as, but not limited to latency, jitter, packet loss and MOS score on a per application basis. This is known as Application Aware Routing.

A multi-vendor and even some single-vendor SASE solutions aren't truly Unified. These are Disaggregated solutions. Such architectures introduce challenges and complexities that are avoided by selecting and leveraging a Unified SASE solution. More on the advantages and disadvantages of Unified versus Disaggregated SASE can be found here.

Conclusion

In this Solution Brief, it was described that SASE is a combination of SSE capabilities and WAN Edge capabilities. Within each 'Edge', there are multiple layers of capabilities. One of these capabilities is 'Network Obfuscation'.

Network Obfuscation refers to keeping threat actors from knowing the existence of enterprise Resources. This protects enterprise applications from attack vectors like lateral movement and port scanning.

Network Obfuscation was discussed from the perspective of VSPA users. These users are Entities connected to the Internet. Through VCGs, Entities are accessing Resources within the enterprise in both on-prem and cloud-based scenarios.

This Solution Brief described Network Obfuscation is the combination of DNS Proxy and CGNAT. However, in a SASE context, Network Obfuscation requires additional technologies to be truly effective. This includes a tunnelling protocol such as IPSec, DTLS or TLS, NGFW and ZTNA. Therefore, Network Obfuscation is enhanced through a blend of integrated SASE capabilities covering networking and security disciplines.

It was also described, through Versa Concerto, configuration and management of Network Obfuscation has been simplified. It was also briefly explained Versa Networks Unified SASE takes the components of SD-WAN and SSE services, including features like

Network Obfuscation, ZTNA and NGFW and natively integrates them into a single architectural framework. Such an approach has multiple advantages over a Disaggregated SASE approach.

For more information on Versa Networks, please visit https://versa-networks.com, contact us at https://versa-networks/contact or follow Versa Networks on X (Twitter) @versanetworks

Reference and Resources

[1] https://versa-networks.com/documents/datasheets/versa-secure-private-access.pdf

[2] NCSC is an organization of the United Kingdom Government that provides advice and support for the public and private sector in how to avoid computer security threats –

[3] https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/network-architectures

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com