Enforcing ZTNA principles using Versa Endpoint Information Profiles

Creating 'context' through device posture to deliver a ZTNA architecture.

Introduction

Zero Trust Network Access (ZTNA) assumes all network traffic is by default untrusted. Indeed, ZTNA assumes the network has already been compromised. Instead, access between Entities (such as end users) and Resources (such as enterprise applications) is permitted through context using strong Authentication, Authorization, and device posture.

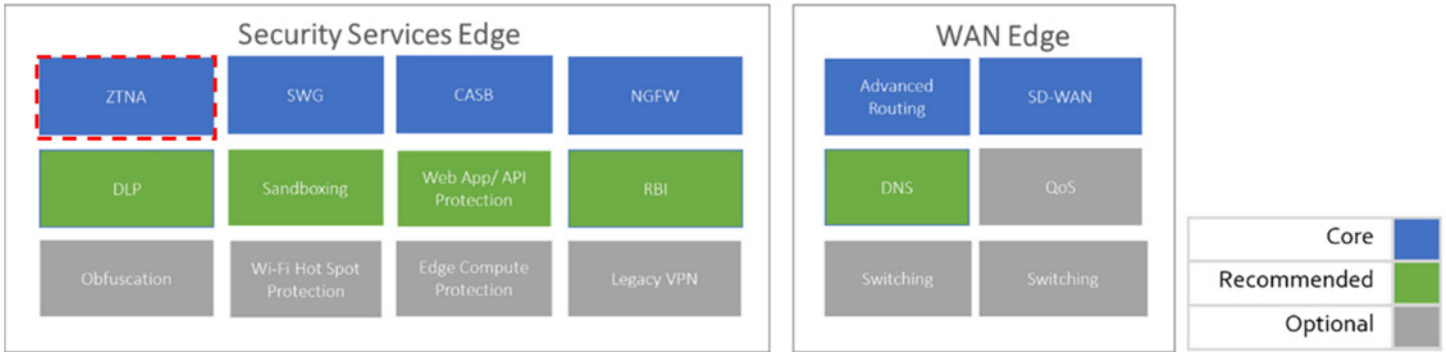
Versa Endpoint Information Profiles (EIPs) use Endpoint Information Objects (EIOs) to build a device posture profile of each Entity in the network. This posture profile information is assessed against the Enterprise's security policy to determine whether an Entity is authorized to connect to the network or Resources.

This document provides an overview of ZTNA and EIPs. It then highlights how ZTNA principles can be enforced between Entities and Resources using EIPs.

Additionally, from a holistic perspective, brief consideration is given to other areas related to SASE, such as micro-segmentation and Unified versus Disaggregated SASE architectures.

ZTNA 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 security capabilities (such as 'Secure Web Gateway' (SWG)) or networking capabilities (such as 'Advanced Routing'). Another SSE capability and the focus of this solution brief is ZTNA:



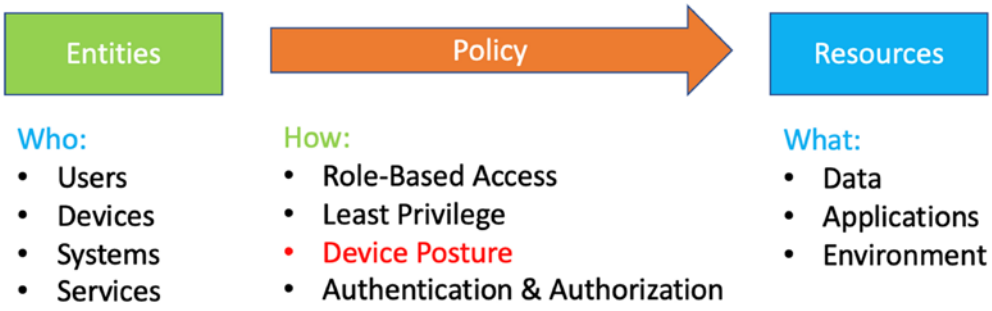
In 2019 the National Cyber Security Centre (NCSC)[1] recommended network architects consider a zero-trust approach[2]. NCSC described zero trust architectures as those that "remove the inherent trust from the network while building confidence in each request. This is achieved through building context through strong authentication, authorisation, device health, and value of the data being accessed".

In the recommendation, the NCSC identified six ZTNA considerations. In the context of this Solution Brief, the use of Versa Endpoint Information Profiles (EIPs) shall be assessed against the following relevant NCSC considerations:

- Context, such as policy compliance and device health.
- Authorization policies to access an application.
- Access control policies within an application.

Versa Endpoint Information Profiles Overview

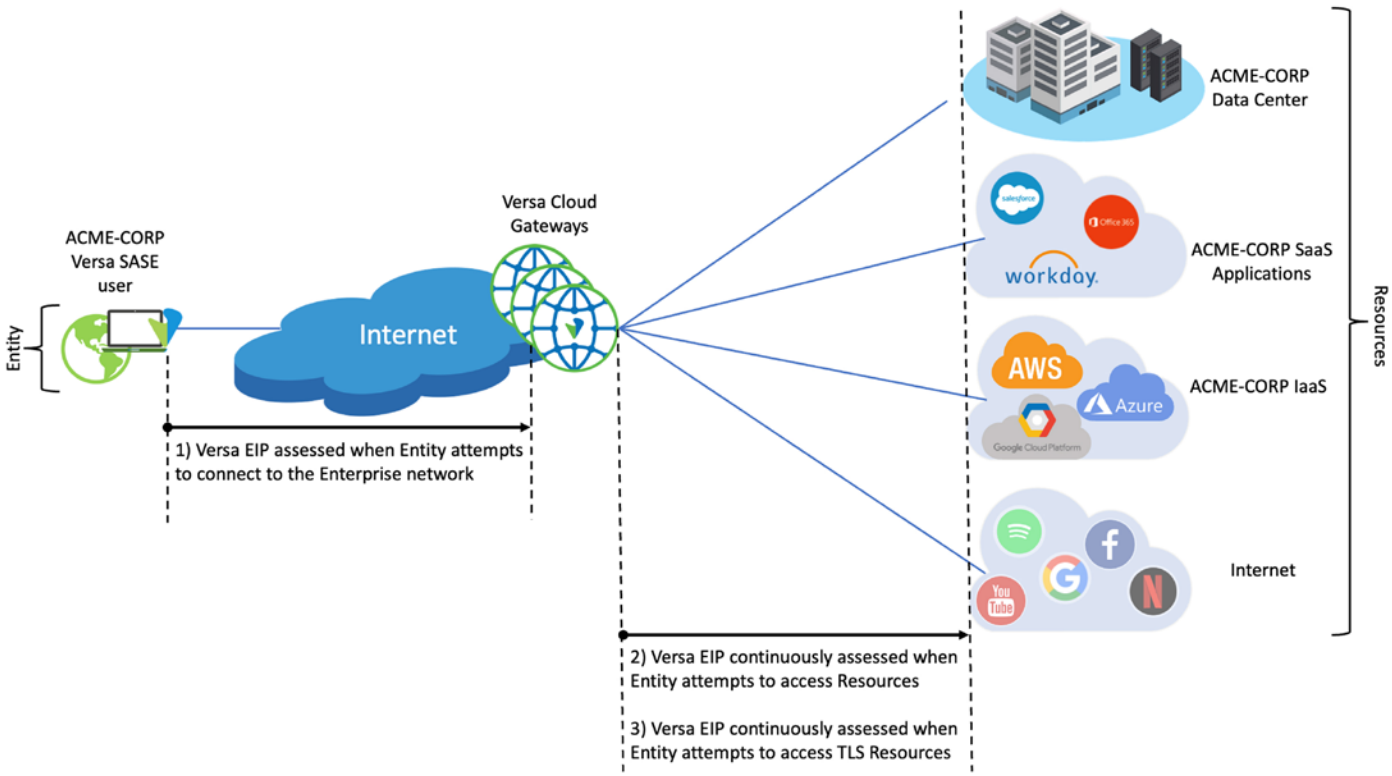
To protect Resources, such as data and applications, EIPs are configured by Security Administrators on Versa Cloud Gateways (VCGs). EIPs ensure remote Entities (such as users, devices and systems that access Resources) maintain and adhere to Enterprise security standards based on the Entities posture. EIPs can therefore be considered policy objects which control 'who' is accessing 'what' via the 'how':



Versa EIPs can be used by policy in several ways:

1. When Entities attempt to connect to the enterprise network using the Versa SASE client, the remote device is assessed against Enterprise security standards to determine its posture. Based on the result, the Entity may be permitted or denied access to the network.
2. Assuming access to the network has been permitted in [1], when Entities attempt to connect to Resources, the remote device can be assessed against Enterprise security standards to determine its ongoing posture. Based on the result, the Entity may be permitted or denied on a per Resource access basis. Optionally, for permitted traffic, additional security measures may be applied (such as Intrusion Prevention System (IPS), malware scanning, etc.).
3. When Entities attempt to connect to Resources via a TLS connection, the Entity is continuously assessed against Enterprise security standards to determine its posture. Based on this result, the Entity may have their TLS session proxied by the Versa SASE Gateway or passed through.

The policy approaches described above are depicted in the following diagram:

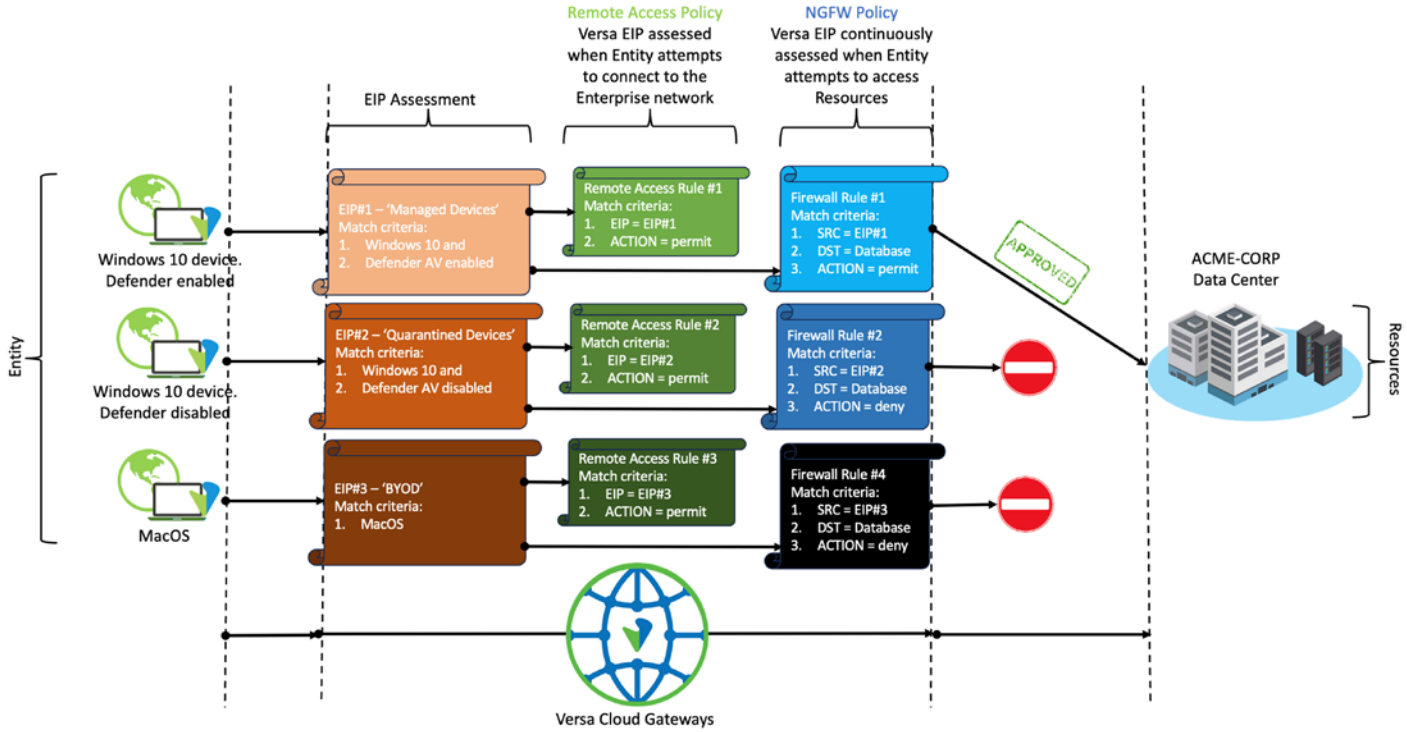


The 'assessment' of the Entity is achieved by collecting posture information of the endpoint device. This information is broadly categorized into different EIP categories as described below:

Antimalware	Antiphishing	Browser	Cloud Storage
Data Loss Prevention	Disk Backup	Disk Encryption	Firewall
General (e.g. OS)	Health Agent	Management Status	Messenger
Patch Management	Public File Sharing	Remote Control	Virtual Machine

For each EIP category, the security posture information is assessed against the configured EIOs for that category. The list of assessed EIOs is then used for the assessment against the configured EIPs.

As an example, for the ACME-CORP organisation, authorized remote users can connect to the ACME-CORP network. This is depicted in the diagram below. Entities connect to VCGs using the Versa SASE client. The SASE client shares EIP posture information with the VCG. Based on posture information, such as Operating System, the VCG associates each Entity with one or more EIOs for each EIP category and thereby associates one or more EIP profiles. In this example, there are three EIP profiles. Depending on information from the Entity, the SASE client is associated with one or more of these profiles. The Remote Access Policy defined on the VCG is used to match Entities to EIPs. (Although not shown, if the SASE client doesn't match any EIP, access can be denied. This prevents unknown Entities (from a security posture perspective) connecting to the Enterprise network). When Entities access Resources, the EIP can be additionally used as a match criterion in SSE/NGFW Policy to control access:

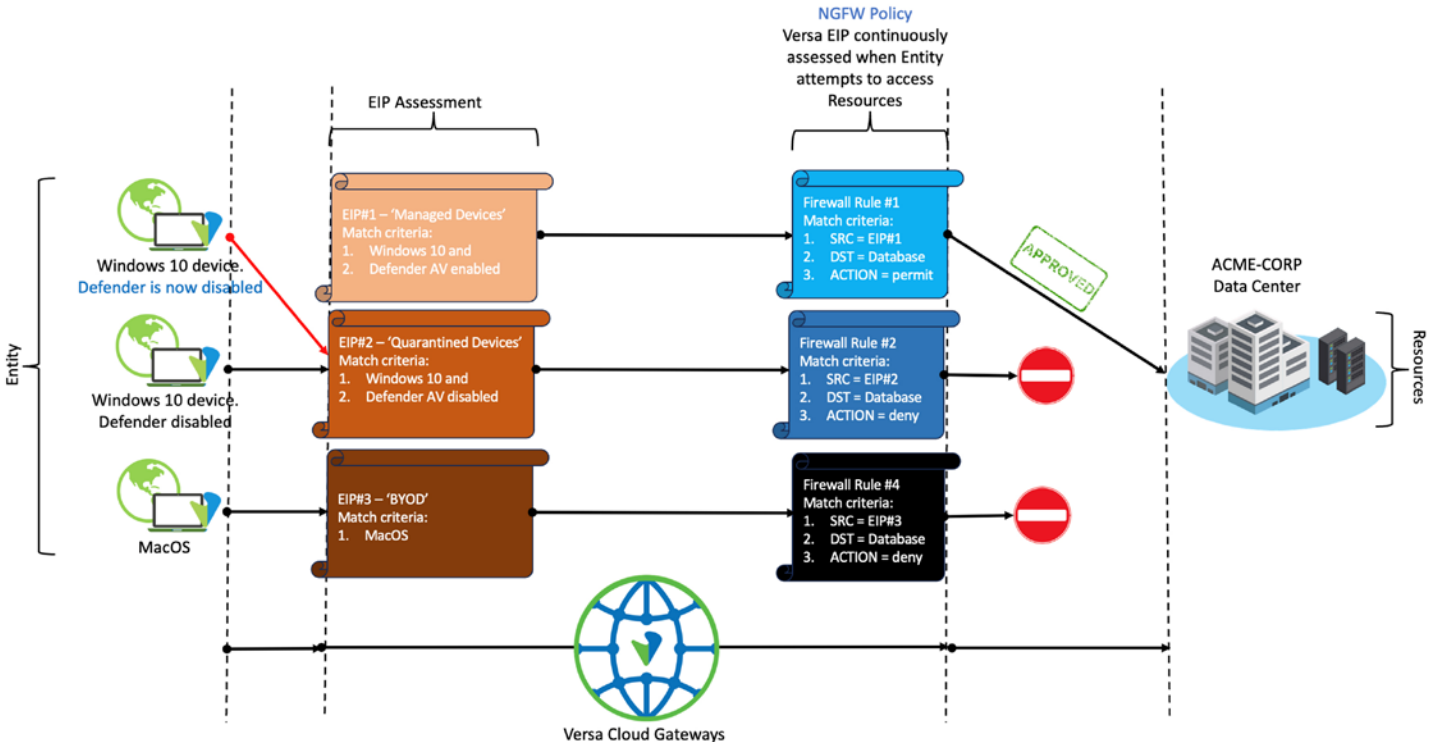


In the example above, any Entity associated with EIP#1 is:

- Authorized to connect to the network based on Remote Access Rule #1.
- Authorized to access the database in the ACME-CORP data center (DC) due to NGFW Policy #1.

In addition, the posture of the Entity is continuously assessed by the VCG as the Versa SASE Client keeps the VCG informed of device posture changes. Therefore, as an example, if Defender becomes disabled on the Windows 10 device (previously associated

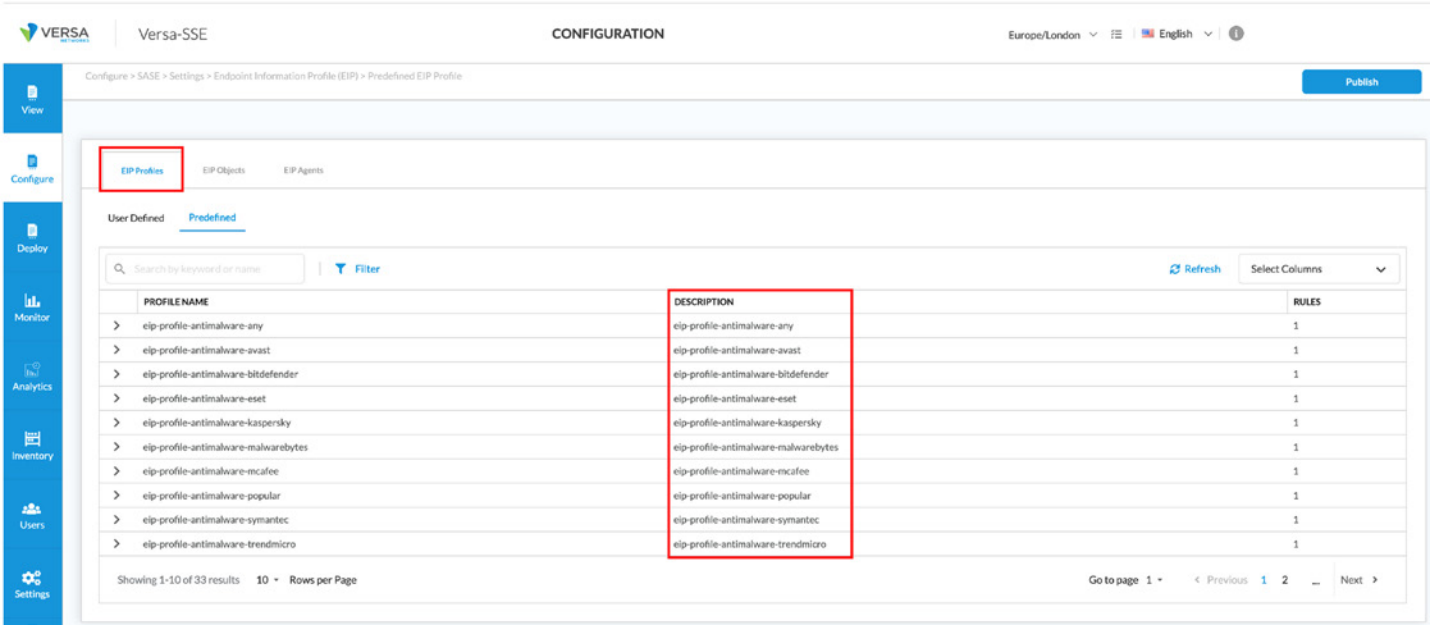
with EIP#1), the posture of the Entity changes. Consequentially, the EIP profiles associated with the Entity are automatically updated. In this example, the Entity moves from EIP#1 to EIP#2. NGFW rules matching on this EIP profile prevents access to the ACME-CORP database. This was previously permitted based on the device posture:



Enforcing ZTNA Principles using Versa EIPs

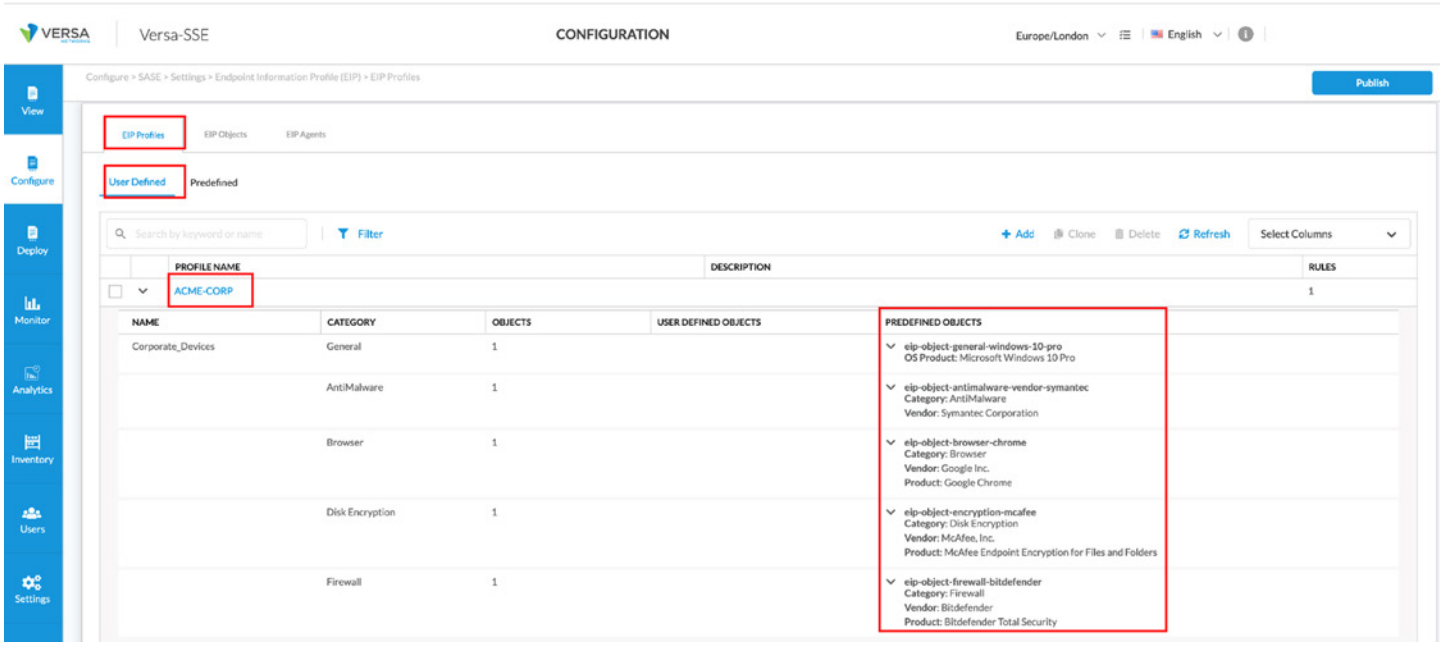
Versa EIP are used to address the following NCSC ZTNA considerations:

1. NCSC ZTNA Consideration: "Context, such as policy compliance and device health"
    a. Versa Response:
        i. When Entities request access to Resources, VCGs apply context to the request. This is achieved by assessing the Entities compliance with enterprise security standards. In essence, 'device health' is assessed to determine if access to the requested Resource is permitted or denied by the VCG.
        ii. VCGs support 'predefined' EIOs as well as the ability for the Security Administrator to create 'user defined' EIOs.
            1. As an example, antimalware software defined objects allow the Administrator to granularly select the enterprise approved vendor(s) of antimalware software. Such information can then be used in policy on the VCG to determine the Entities compliance from an antimalware software context:



iii. VCGs support 'predefined' EIPs as well as the ability for the Security Administrator to create 'user defined' EIPs. User defined EIPs can make use of both predefined and user defined EIOs.

iv. EIPs can be created either using a single EIO (as shown in the screenshot above) or by combining multiple EIOs. In the example below, the EIP Profile ('ACME-CORP') is a user defined EIP combining five predefined EIOs. The predefined EIOs range from Operating System through Firewall vendor. In this example, an Entity would need to match each EIO in each EIP category to be associated with this EIP:

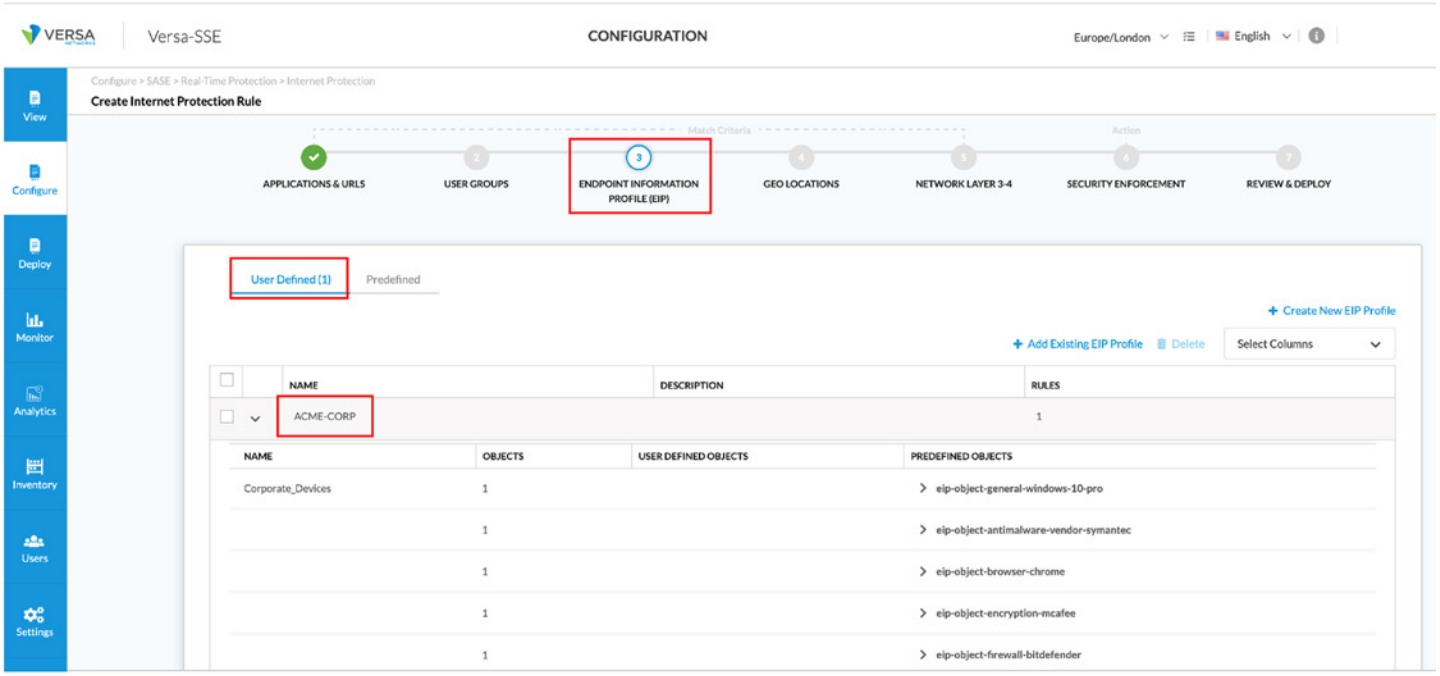


2. NCSC ZTNA Consideration: "Authorization policies to access an application"

a. Versa Response:

i. When Entities access Resources, VCGs use multiple match criteria to determine if an Entity is authorised to access a Resource. For example, is the username or user group permitted access to the Resource? Is the traffic permitted based on IP tuple or application information? These criteria are in addition to match criteria in the EIP. The blend of match criteria including EIP data permits Security Administrators to create granular policies for access to be authorised to Resources.

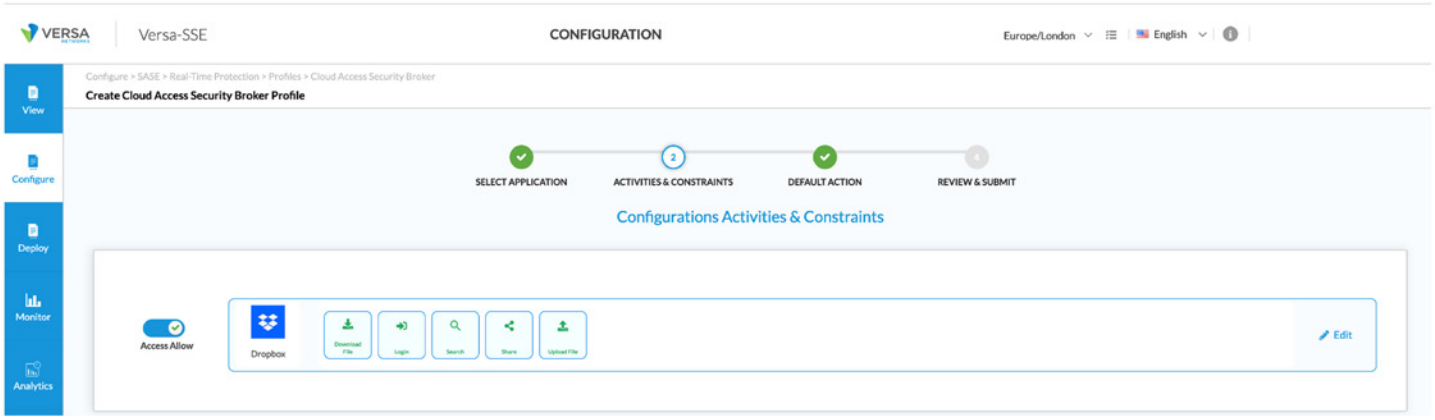
ii. As an example, in the following screenshot, an Internet access rule is created. The rule applies to all Entities matching the criteria defined in the rule. One of five match criteria is EIP information. In this example, the EIP match criteria is the User Defined EIP profile created earlier:



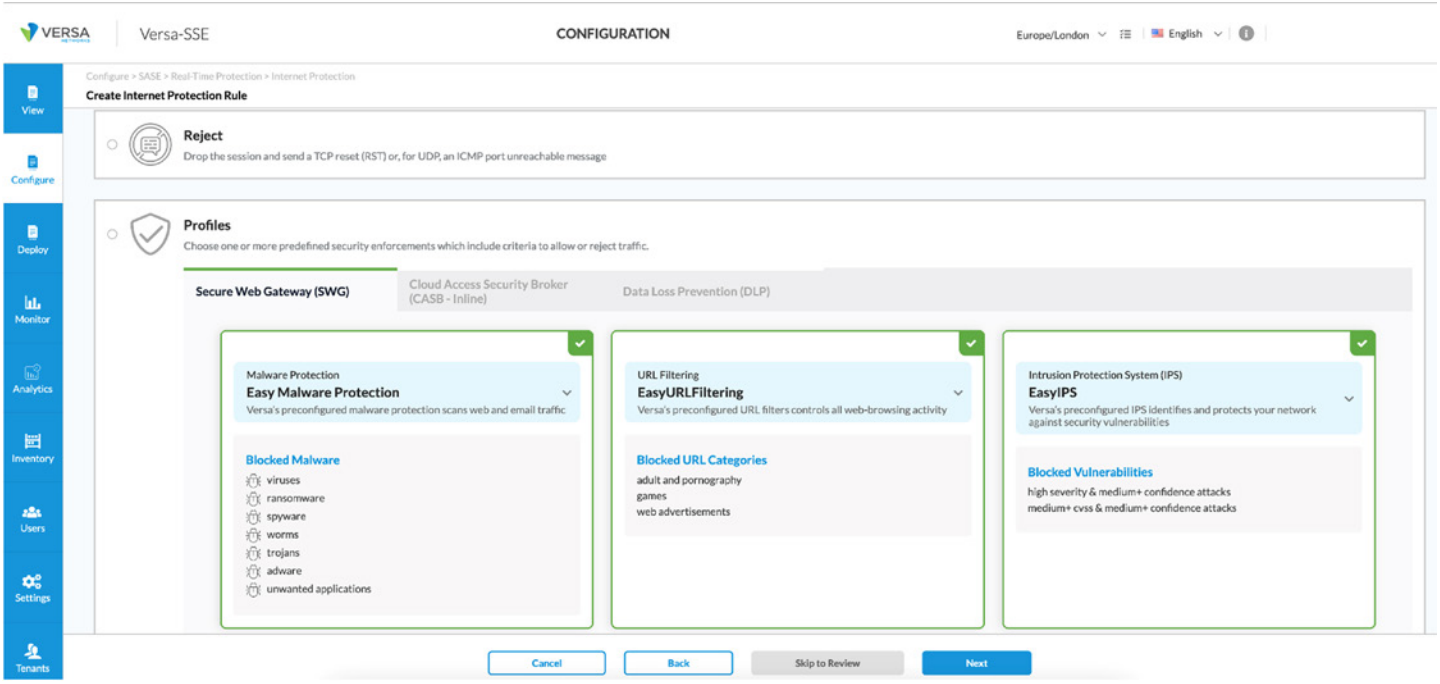
3. NCSC ZTNA Consideration: "Access control policies within an application"

a. Versa Response:

i. In addition to policies when accessing a Resource, VCGs can continuously assess access within the application itself based on EIP data. For example, Cloud Access Security Broker (CASB) is a capability of SASE and controls access to Software as a Service (SaaS) platforms. Within a SaaS application, such as Dropbox, VCGs can control access to individual elements of the application itself. For example, the ability for Entities to download files; login; search; share and upload files can be individually controlled through policy. In addition, EIP information can be used to provide context to that access control. Thus, the Entities compliance to enterprise policy can be a factor whether an Entity is permitted to perform one of these actions within the SaaS application. As EIP data is continuously updated, control can also be updated as the compliance of the Entity changes:



ii. In combination with EIP, VCGs can inspect traffic for content contravening the enterprise security policy. For example, based on the device posture of the Entity, further control within the application can be invoked. In the following screenshot, the same Internet access rule matching on the user defined EIP is used. In this screenshot, the action is to permit traffic between Entity and Resource whilst at the same time scanning for malware, implementing URL filtering, and invoking Intrusion Prevention System (IPS) checks:



Other Considerations

Micro-Segmentation

Micro-segmentation refers to the need for a more granular level of segregation for Entities such as corporate appliances, Internet of Things (IoT) devices and other network attached appliances. Such segmentation is based on the type of device and status of the device. This information can be delivered using EIPs. Furthermore, by continuously assessing the posture of the Entity, the micro segment associated with the Entity can be dynamically amended as the posture of the Entity changes. Finally, using Firewall policy, EIPs are used as match criteria to control access to Resources in a micro-segmented architecture.

Unified SASE

Versa Networks Unified SASE takes the components of SSE Edge and WAN Edge, including features like ZTNA 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 ZTNA in addition to all other SASE features from Versa Networks. Since Versa SASE components work in unison in a single pass architecture it provides near real-time automated remediation and multi-defense system-based threat protection

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 by following this link - https://versa-networks.com/documents/solution-briefs/natively-integrating-sd-wan-and-sse.pdf.

Conclusion

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

According to NCSC a zero-trust architecture assumes the network is already compromised. Instead, a zero-trust architecture builds confidence in each Entity request to access Resources. This is achieved through building context using considerations like strong authentication, authorization, and device posture.

Versa EIPs are used to ensure remote Entities, such as users, who are accessing Resources, maintain and adhere to enterprise security standards. EIPs can therefore be considered policy objects which control 'who' is accessing 'what' via the 'how'.

EIPs can be used by policy in several ways. For example, when Entities attempt to connect to the enterprise network using the Versa SASE client, the remote device is assessed against enterprise security standards to determine its posture. Based on this result, the Entity may be permitted or denied access to the network. Additionally, when Entities attempt to connect to Resources, they can be continuously assessed against enterprise security standards. Based on the result, the Entity may be permitted or denied on a per Resource access basis. Optionally, for permitted traffic, additional security measures may be applied (such as malware scanning, URL filtering, Intrusion Prevention System (IPS), etc.)

This solution brief then explained how three NCSC considerations for a ZTNA architecture are met using EIPs. Specifically, EIPs can be used to build context into an Entity's access to Resources. This is achieved by comparing the Entities device posture against Enterprise security policy when determining whether authorization is granted. Based on the EIP information, VCGs can authorize access to an application or indeed control access within an application.

It was also briefly explained Versa Networks Unified SASE takes the components of SD-WAN and SSE services, including features like ZTNA and natively integrates them into a single architectural framework. Since Versa SASE components work in unison in a single pass architecture it provides near real-time automated remediation and multi-defense system-based threat protection. 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] 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
[2] 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