Telstra SecureEdge Network Technical Guide

Welcome to Telstra SecureEdge Network Technical Guide

About this technical guide

The purpose of this document is to provide the customer (you) with valuable information on various aspects of features provided by SecureEdge Network (SEN). For every feature offered, the guide references the Palo Alto Network (PAN) guides, which serve as comprehensive references. The PAN guides are instrumental in understanding the intricacies of SEN and provide step-by-step instructions on its implementation. However, it is important to note that there may be exceptions to the PAN guides that either do not apply to the SEN deployment or should not be followed in specific scenarios. These exceptions will be clearly mentioned in this document, ensuring you are aware of any deviations or alternative approaches.

This document has been specifically designed for your network and IT personnel and assumes a thorough technical understanding of Palo Alto firewall management and PAN-OS for optimal comprehension.

If you have any questions, please contact your Telstra Sales/Account representative.

Conventions used in this guide

The following typographical conventions are used in this guide for simplicity and readability:

Web addresses, e-mail addresses and hyperlinks are shown in bold, for example **www.telstraenterprise.com.au.**

User input is shown in typewriter font.

What's inside

1 Introduction to SecureEdge Network

1.1 What is Telstra SecureEdge Network Service?

SecureEdge Network (SEN) is a cloud-based next generation firewall hosted in Telstra infrastructure within Australia that provides you with a security gateway for your Telstra IP WAN, IP MAN, or Connect IP service ("Next IP Service"). SEN extranet connection also enables you to set up a private network with other SEN customers.

SEN infrastructure is managed by Telstra and comprises control plane and data plane components. The supporting infrastructure platform provides high availability and geographical redundancy in five data centre locations – Melbourne (VIC), Sydney (NSW), Perth (WA), Adelaide (SA), Brisbane (QLD).

Your firewalls on SecureEdge Network Platform are implemented in Active/Passive High Availability mode.

The next generation firewall features for SEN are powered by the Palo Alto Networks VM Series firewalls. We make these features available via the SEN User Interface (SENUI). The SENUI comprises:-

1. The Telstra Connect Customer Portal (**T-Connect**)
2. The Customer SecureEdge Network Console (**CSENC**)

Please refer the SEN User Guide for more details on the SENUI.

1.2 Customer SecureEdge Network Console (CSENC) and PAN Panorama

The CSENC provides you access to the Palo Alto Networks (PAN) Panorama application that enables you to manage the configuration on your SEN service.

Panorama is designed to simplify the management and monitoring of network security policies, threat prevention settings, and configuration across a distributed network of Palo Alto firewalls. All standard tier self-managed firewall policy configurations can be applied to your SEN service via Panorama provided by CSENC.

For further information on PAN Panorama, please visit the link below:
https://docs.paloaltonetworks.com/panorama

PAN-OS is the software that runs all SEN features powered by Palo Alto Networks next-generation firewalls.

You can utilise the PAN-OS documentation to maximise the potential of your SEN service. Whether you're just starting out and need help with integrating your SEN firewall into the network, or you're in the process of applying advanced techniques to combat credential theft, the support you need is easily accessible in the PAN-OS documentation available at PAN-OS Web Interface Help (paloaltonetworks.com)

This technical guide has therefore been structured to provide an outline of the features offered by SEN and for each feature, you will be redirected to the PAN-OS guide which serves as a comprehensive reference and the ultimate source of truth.

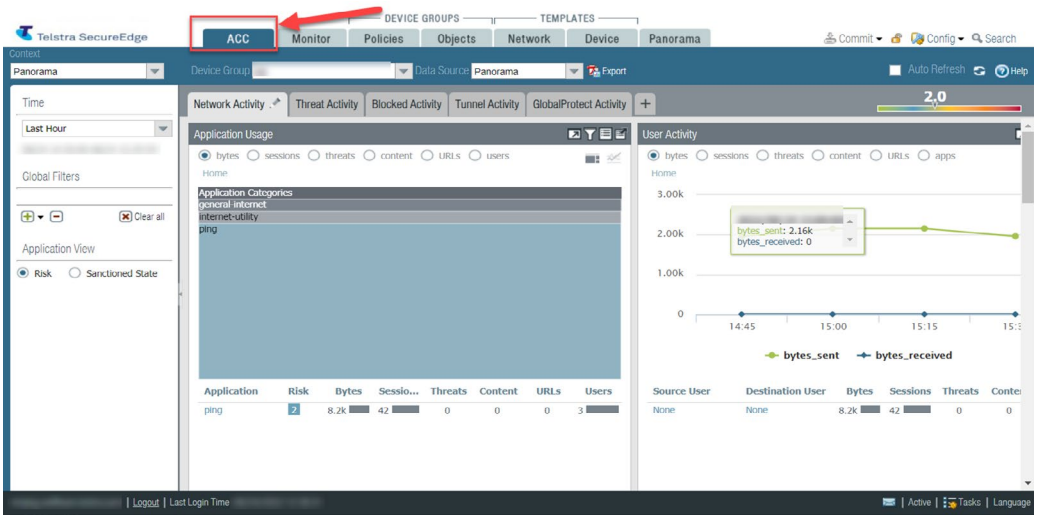
2 Navigating the Customer SecureEdge Network Console (CSENC)

The CSENC provides you access to the Palo Alto Networks Panorama application. Panorama enhances the management, visibility, and control of your SEN service. It simplifies administrative tasks and helps you maintain a strong and consistent security posture across your distributed network environments. It consists of several key components that contribute to its capabilities.

This chapter provides an overview of the key components symbolised by tabs in Panorama:

2.1 Application Command Centre (ACC) Tab

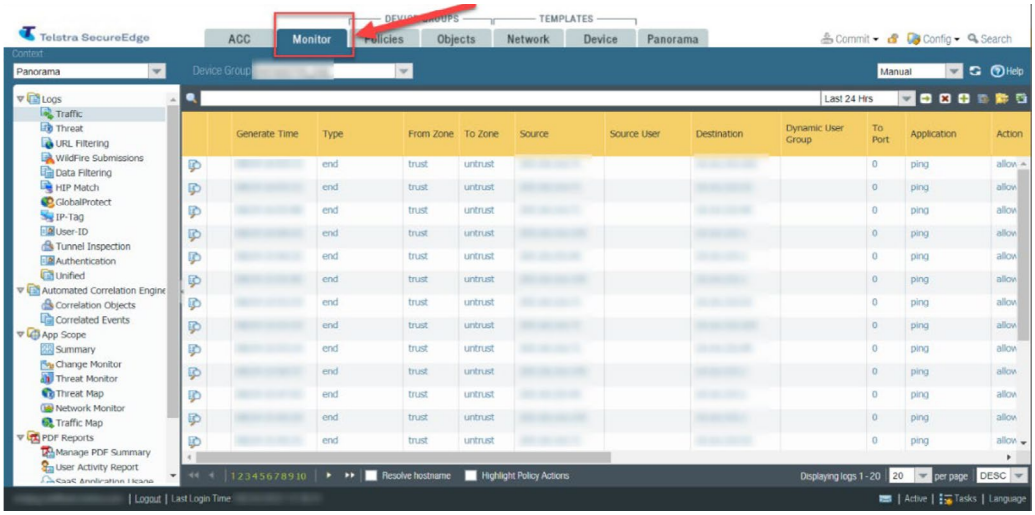
ACC is an analytical tool that provides actionable intelligence about the network activity. It uses the firewall logs to graphically depict traffic trends. The graphical representation allows you to interact with the data and visualise the relationships between events, including network usage and traffic patterns, suspicious activity, and anomalies.



For more information, please refer to PAN-OS Administrator's Guide – ACC

2.2 Monitor Tab

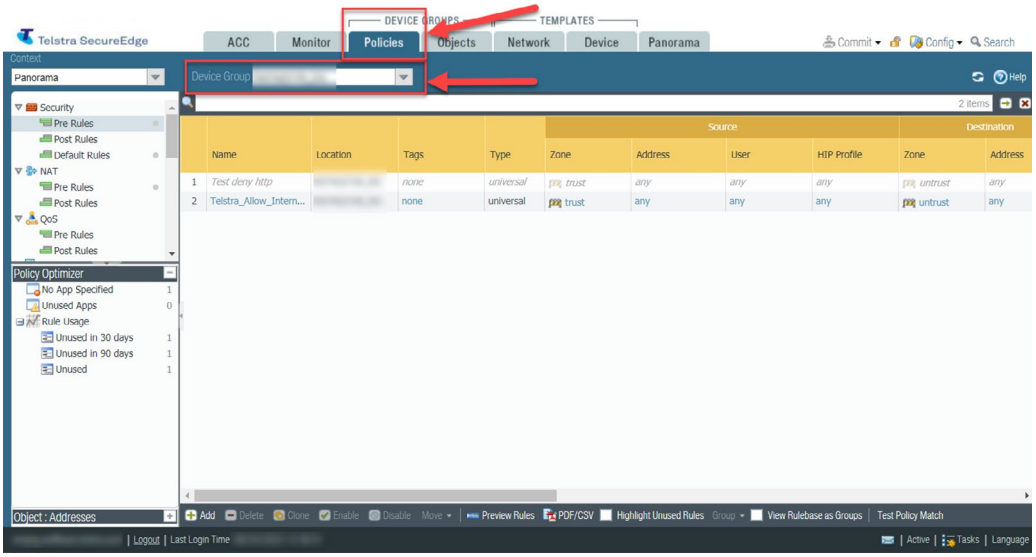
The Monitor tab gives you the ability to see variety of logs (e.g., Traffic logs, Threat logs, URL Filtering logs, WildFire Submissions logs, GlobalProtect logs, User-ID logs, Authentication logs, etc.). You can also see and generate reports using this tab.



For more information, please refer to PAN-OS Administrator's Guide – **Monitor**

2.3 Policies Tab

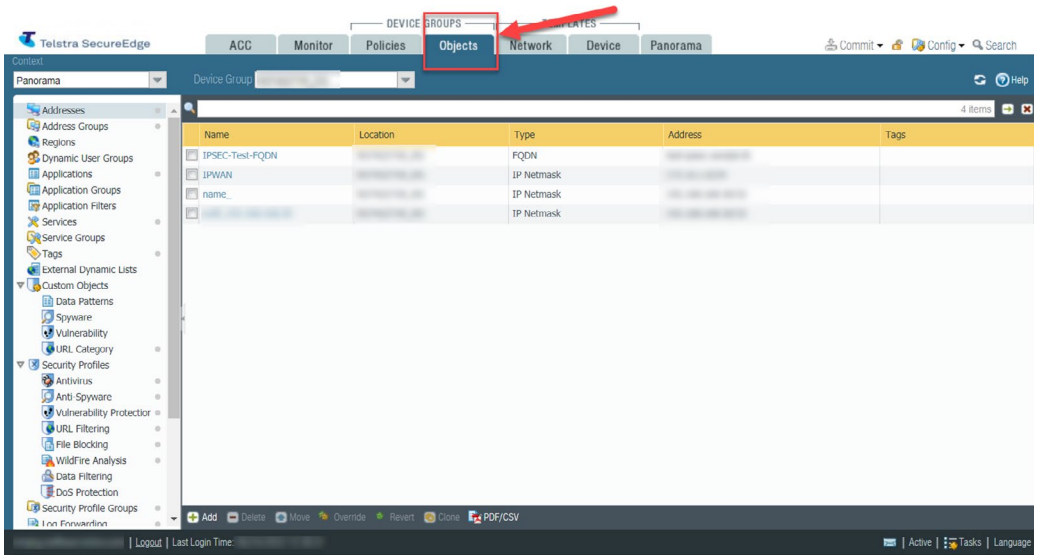
Policies enable you to control firewall operations by enforcing rules and automating actions. Do not forget to select the Device Group from the drop-down list when configuring.



For more information, please refer to PAN-OS Administrator's Guide – **Policies**

2.4 Objects Tab

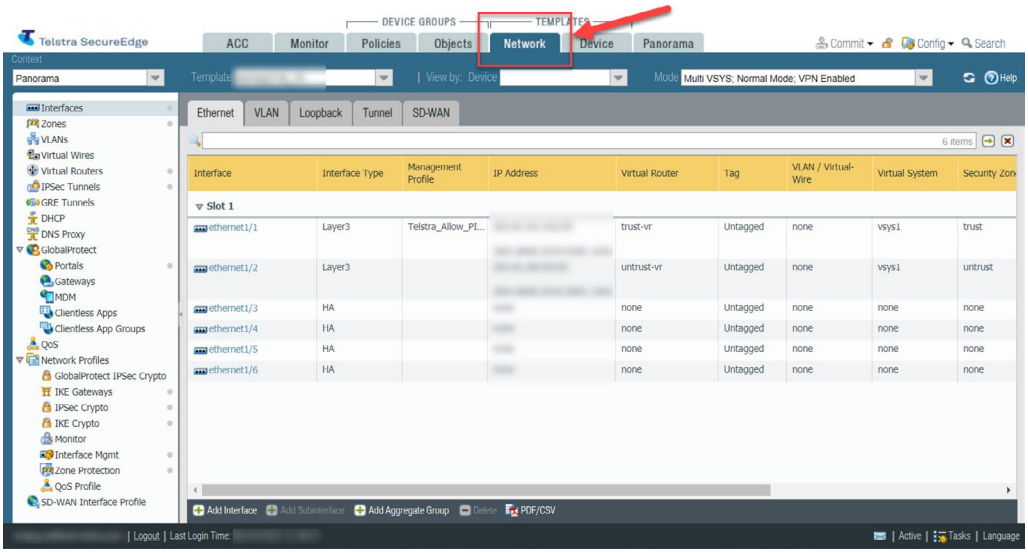
Objects are the elements that enable you to construct, schedule, and search for policy rules, Security Profiles provide threat protection in policy rules. You can configure the Security Profiles and objects (e.g., URL Filtering) that you want to use with Policies.



For more information, please refer to PAN-OS Administrator's Guide – **Objects**

2.5 Network Tab

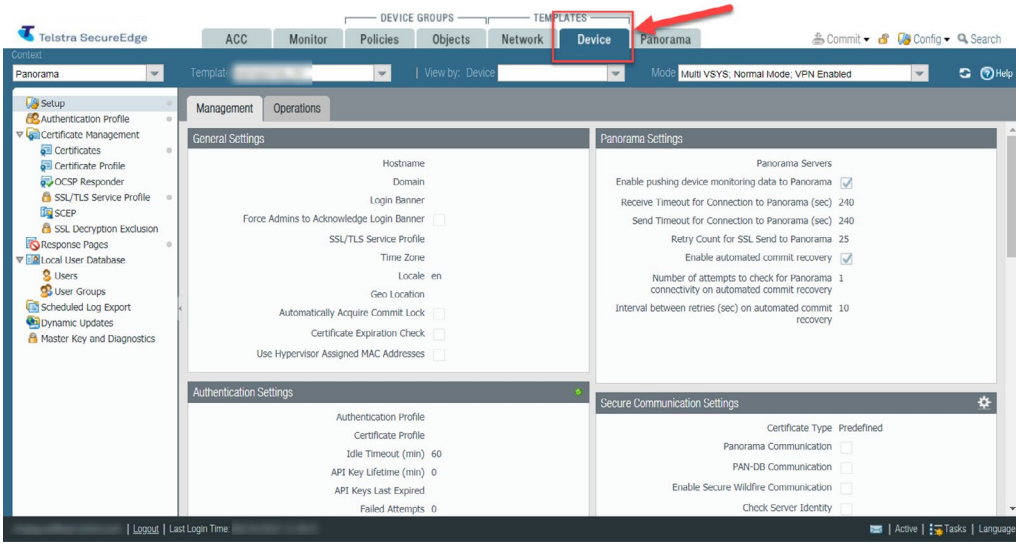
Firewall network settings can be found under this tab. You can configure Interfaces, Zones, VLANs, IPSec Tunnels, GlobalProtect, Network Profiles, etc.



For more information, please refer to PAN-OS Administrator's Guide – **Network**

2.6 Device Tab

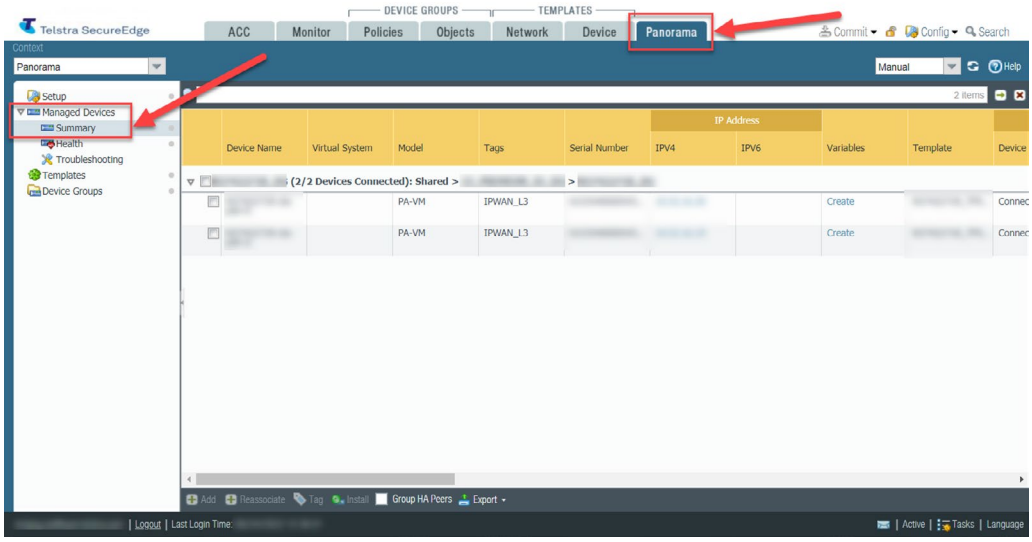
Device tab is for basic system configuration and maintenance tasks on the firewall. You can configure the Authentication Profile, Certificate Management, Response Pages, and Local User Database here.



For more information, please refer to PAN-OS Administrator's Guide – Device

2.7 Panorama Tab

Panorama tab is to configure Panorama which is a centralised management application using which you can oversee all your firewalls. The Summary section under the Managed Devices is a nice place to have a quick glance at the status of your firewalls.



For more information, please refer to PAN-OS Administrator's Guide – Panorama Web Interface

3 Configuring your Telstra SecureEdge Network (SEN) Service

This chapter provides an overview of all the major features offered by SEN and the steps involved in configuring them. The outlined steps are intended as initial and high-level guidelines only. For comprehensive configuration instructions, consult the referenced links.

3.1 URL Filtering

URL Filtering gives you a way to control not only web access but also how your users interact with online content. It helps classify sites based on content, features, and safety, and you can enforce your security policy based on these URL categories. You can also prevent credential phishing theft by tightly controlling the types of sites to which your users can enter their corporate credentials.

The following points detail URL filtering specific tasks that need to be performed in Panorama.

The tasks are:

1. Create customised URL Categories
2. Create a URL Filtering Profile
3. Create a customised Security Profile Group (SPG) and add the URL filtering profile
4. Apply Security Profile Group (SPG) to a security policy
5. Commit changes in Panorama and push to the managed firewalls

For detailed configuration instructions, visit the link below.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/url-filtering

3.2 IPSEC Site-to-Site VPN

The firewall uses the IP Security (IPSec) set of protocols to set up a secure tunnel for the traffic between two sites over a public network.

The following points detail IPSEC Site-to-Site VPN configuration specific tasks that need to be performed in Panorama.

The tasks are:

1. Configure New Loopback Interface
2. Configure New Security Zone for IPSEC VPN Tunnel
3. Configure New Tunnel Interface for IPSEC VPN Tunnel
4. Configure Static Routes for IPSEC Remote Sites
5. Configure New Profile for IPSEC Crypto
6. Configure New Profile for IKE Crypto
7. Configure New Profile for IKE Gateway
8. Configure New Profile for IPSEC Tunnel
9. Configure Security Policies
10. Configure NAT
11. Configure Policy Based Forwarding (PBF)
12. Commit Changes and Push to Firewall

For detailed configuration instructions, visit the link below.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/vpns/set-up-site-to-site-vpn

3.3 IPSEC Client-to-Site GlobalProtect VPN

Whether you are checking emails from home or updating corporate documents from an airport, majority of today's employees work outside the physical corporate boundaries. This workforce mobility increases productivity and flexibility while simultaneously introducing significant security risks. Every time your users leave the building with their laptops or smartphones, they are bypassing the corporate firewall and associated policies that are designed to protect both them and the network.

GlobalProtect solves these security challenges introduced by roaming users by extending the same next-generation firewall-based policies that are enforced within the physical perimeter to all your users, no matter where they are located.

The following points detail IPSEC Client-to-Site GlobalProtect VPN configuration specific tasks that need to be performed in Panorama.

The tasks are:

1. Download and Install GlobalProtect Data File onto Firewall
2. Configure New Security Zone for GP VPN Tunnel
3. Configure New Tunnel Interface for GP VPN Tunnel
4. Configure Static Routes for GP Remote Sites
5. Generate a Self-Signed Certificate
6. Create a New SSL/TLS Service Profile
7. Configure GP Portal
8. Configure GP Gateway
9. Configure Security Policies
10. Configure NAT
11. Configure Policy Based Forwarding (PBF)
12. Commit Changes and Push to Firewall
13. GlobalProtect Client Setup
14. GlobalProtect Tunnel Verification

For detailed configuration instructions, visit the link below.
https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin

3.4 File Blocking

File blocking blocks specified file types over specified applications and in the specified session flow direction (inbound/ outbound/both). You can set the profile to alert or block on upload and/or download and you can specify which applications will be subject to the file blocking profile. You can also configure custom block pages and define custom file blocking profiles.

The following points detail file blocking configuration specific tasks that need to be performed in Panorama.

The tasks are:

1. Create the file blocking profile
2. Configure the file blocking options
3. Apply the file blocking profile to a security policy rule
4. Commit changes and push to firewall.

For detailed configuration instructions, visit the link below.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/set-up-file-blocking

3.5 Sandboxing (Wildfire Analysis)

The cloud-delivered WildFire® malware analysis service uses data and threat intelligence from the industry's largest global community and applies advanced analytics to automatically identify unknown threats and stop attackers in their tracks.

For further information, visit the link below.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding

3.6 DNS Security

Palo Alto Network's DNS Security service is a cloud-based analytics platform that helps secure your DNS traffic by providing your firewall with access to DNS signatures generated using advanced predictive analysis and machine learning, with malicious domain data from a growing threat intelligence sharing community.

For further information, visit the link below.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/dns-security

3.7 Extranet

SEN Extranet Connection service provides connectivity of your Next IP Service to other organisations that also have a Next IP Network Service with us via the other customer's SEN Extranet connection service.

Once you have gained consent from the other organisation and put in a request for your SEN Extranet connection service, we will provision the service for you by building IPsec tunnels between your gateway and the consenting organisation's gateway.

You may also set up IPsec tunnels on your own between two subnets, however, this traffic will travel over the internet and not via our network.

Please note that Telstra will open all communication between the gateways. It is your responsibility to secure traffic between the gateways by setting up policies. Refer Policies for additional information on how to set up policies.

4 Telstra SecureEdge Network Additional Features

This chapter provides an overview of all the additional features offered by SEN and the steps involved in configuring them. The outlined steps are intended as initial and high-level guidelines only. For comprehensive configuration instructions, consult the referenced links.

4.1 Self-Managed SNMP Service

Simple Network Management Protocol (SNMP) traps can alert you to system events (failures or changes in hardware or software of SEN firewalls) or to threats (traffic that matches a firewall security rule) that require immediate attention.

The following points detail SNMP configuration specific tasks that need to be performed in Panorama to send SNMP traps from your firewall to a self-managed destination located inside your network or anywhere in the cloud.

The tasks are:

1. Create SNMP server profile for new self-managed destination.
2. Add new server profile to Log Settings
3. Add new server profile to Log Forwarding
4. Change the Log Forwarding Profile for Security Policies
5. Change the service route for new self-managed SNMP server as a destination.
6. Commit the changes and push to firewall.

For further information, visit the link below.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/snmp-monitoring-and-traps

4.2 Self-Managed Syslog Service

Syslog is a standard log transport mechanism that enables the aggregation of log data from different network devices such as routers, firewalls, printers from different vendors into a central repository for archiving, analysis, and reporting. SEN firewalls can forward every type of log they generate to an external syslog server.

The following points detail Syslog configuration specific tasks that need to be performed in Panorama to send Syslog messages from your firewall to a self-managed destination located inside your network or anywhere in the cloud.

The tasks are:

1. Create Syslog server profile for new self-managed destination
2. Add new server profile to Log Settings
3. Add new server profile to Log Forwarding
4. Change the Log Forwarding Profile for Security Policies
5. Change the service route for new self-managed Syslog server as a destination.
6. Commit the changes and push to firewall

For further information, visit the link below.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/use-syslog-for-monitoring/configure-syslog-monitoring

4.3 Self-Managed Active-Directory (AD) as Identity Provider

SEN can be integrated with Microsoft's Windows Active Directory (AD) through LDAP. The new version of PAN-OS allows agentless authentication with Active Directory Domain controller; however, Windows Management Instrumentation (WMI) settings on the AD Domain Controller must be modified and you must be Domain Admin to do so.

Before you integrate SEN with AD, you must create a user ID in AD that you'll use to access LDAP. At a minimum, this account must be a member of the built-in Server Operators group in AD. For security reasons and to be compliant with the best practices, you should adhere to the minimum access rights for this account.

The following points detail AD configuration specific tasks that need to be performed in Panorama.

The tasks are:

1. Create LDAP server profile.
2. Create new Authentication profile for LDAP.
3. Add new LDAP server profile to GlobalProtect Authentication
4. Add new LDAP server profile to Captive-Portal Authentication
5. Change the service route for new self-managed Active-Directory server as a destination.
6. Commit the changes and push to firewall.

For further information, visit the link below.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-ldap-authentication

4.4 Self-Managed RADIUS as Identity Provider

SEN can be configured with RADIUS authentication for end users. The GlobalProtect clients trying to connect to the network will be authenticated by RADIUS server. For administrators, you can use RADIUS to manage authorisation (role and access domain assignments) by defining Vendor-Specific Attributes (VSAs)

For further information on VSA, visit the link below.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClIxCAK

Before you integrate SEN with RADIUS, you must create a user account in RADIUS server.

The following points detail RADIUS configuration specific tasks that need to be performed in Panorama.

The tasks are:

1. Create RADIUS server profile
2. Create new Authentication profile for RADIUS
3. Add new RADIUS server profile to GlobalProtect Authentication
4. Change the service route for new self-managed RADIUS server as a destination
5. Commit the changes and push to firewall

For further information, visit the link below.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-radius-authentication

4.5 Self-Managed Cloud Azure as Identity Provider

SEN can be integrated with Microsoft's Cloud Service like Azure.

Before you integrate SEN with Microsoft Azure, you must configure Microsoft Azure portal with Palo Alto Networks - GlobalProtect from the gallery to your list of managed SaaS apps. Once Palo Alto app is configured, download the Federation Metadata XML and save it on your computer (This will be imported into the firewall).

To configure Microsoft Azure Portal, visit the link below and follow the instructions:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000008U48CAE

The following points detail Azure configuration specific tasks that need to be performed in Panorama.

The tasks are:

1. Create SAML server profile for Azure
2. Create new Authentication profile for Azure
3. Add new Azure server profile to GlobalProtect Authentication
4. Add new Azure server profile to Captive-Portal Authentication
5. Commit the changes and push to firewall

For further information, visit the link below.
https://docs.paloaltonetworks.com/cloud-identity/cloud-identity-engine-getting-started/authenticate-users-with-the-cloud-identity-engine/configure-an-identity-provider-in-the-cloud-identity-engine/configure-azure-as-an-idp-in-the-cloud-identity-engine

4.6 Self-Managed Cloud Okta as Identity Provider

SEN can be integrated with Cloud Service like OKTA.

Before you integrate SEN with OKTA, you must configure OKTA portal with Palo Alto Networks - GlobalProtect from the gallery to your list of managed SaaS apps. Once Palo Alto app is configured, download the Federation Metadata XML and save it on your computer (This will be imported into the firewall).

To configure OKTA Portal, visit the link below and follow the instructions:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000008U48CAE

The following points detail OKTA configuration specific tasks that need to be performed in Panorama.

The tasks are:

1. Create SAML server profile for OKTA
2. Create new Authentication profile for OKTA
3. Add new OKTA server profile to GlobalProtect Authentication
4. Add new OKTA server profile to Captive-Portal Authentication
5. Commit the changes and push to firewall.

For further information, visit the link below.
https://docs.paloaltonetworks.com/cloud-identity/cloud-identity-engine-getting-started/authenticate-users-with-the-cloud-identity-engine/configure-an-identity-provider-in-the-cloud-identity-engine/configure-okta-as-an-idp-in-the-cloud-identity-engine

4.7 DNS Proxy

SEN includes a function known as DNS Proxy. Typically, this feature is employed with data plane interfaces, enabling you to utilise the Palo Alto interfaces for your recursive DNS server needs.

The following points detail DNS Proxy configuration specific tasks that need to be performed in Panorama.

The tasks are:

1. Create DNS Proxy for customer traffic on trust interface
2. Configure DNS Proxy Rules
3. Configure DNS Static Entries
4. Commit the changes and push to firewall.

For further information, visit the link below.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFcCAK

4.8 SIEM Integration

SEN can be integrated with a self-managed or 3rd party SIEM solution for security monitoring and event management. You will need to configure a log profile in Panorama to send the required log format to a destination IP address. Your self-managed or 3rd party SIEM will need to be configured to accept the logs and normalise it, if needed to a format. Custom log formats can also be configured if required.

For further information on viewing and managing logs, visit the link below.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/view-and-manage-logs

5 Limitations

Listed below are the limitations of PAN in a SecureEdge Network (SEN) deployment. Some of these limitations can be remediated using certain workarounds, which have been mentioned.

5.1 Routing Changes

Routing changes need to be made if you want to configure specific static routes and make changes to the network. Static routes are typically used in conjunction with dynamic routing protocols. You might configure a static route for a location that a dynamic routing protocol can't reach.

While we do understand that this may be necessary, you cannot make routing changes to the network or configure routing policies using CSENC.

Routing changes are classified as a minor service change and a Feature & Network Changes (FNC) request will have to be raised to help inject specific routes into the Firewall.

The FNC Order Online portal can be accessed via Your Telstra Tool (YTT) website under Self Service portlet.
https://www.telstra.com.au/business-enterprise/self-service/online-self-service-apps

Additional details on service changes and FNC requests can be found in the Telstra SecureEdge Network User Guide.

5.2 Addition of Custom Public IP Addresses

By default, when your virtual firewall is created, it will have the SecureEdge public IPv4/IPv6 address, however, this can be changed. SEN supports the addition of Custom or Bring-your-own (BYO) public IPv4/IPv6 addresses which can be configured as Loopbacks or Object-Groups for NAT or for your internal network.

While we do understand that this may be necessary, you cannot make IP addressing changes to the network using CSENC.

Addition of custom IP addresses is classified as a minor service change and a Feature & Network Changes (FNC) request will have to be raised to ensure that your custom IP(s) are delegated to/advertised from SecureEdge Network.

The FNC Order Online portal can be accessed via Your Telstra Tool (YTT) website under Self Service portlet.
https://www.telstra.com.au/business-enterprise/self-service/online-self-service-apps

Additional details on service changes and FNC requests can be found in the Telstra SecureEdge Network User Guide.

5.3 Deleting Default Route

Deleting the default route will break the service chaining and interrupt the end-to-end traffic flow for internet bound traffic, therefore, these changes are not permitted using the CSENC.

This situation can be remediated by configuring specific static routes; however, routing changes are classified as minor service changes and cannot be made using CSENC.

Please refer to section 5.1 for details on how to implement routing changes for your service.

5.4 Increasing Log Storage

Whilst we do understand that you might require additional capacity to store your logged data, log storage cannot be increased in SEN. You are free however, to send your syslog messages from your firewall to a self-managed destination located inside your network or anywhere in the cloud, which is in addition to SEN's default setting of sending Syslog messages to Splunk.

For further information on log settings, visit the link below:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/panorama-web-interface/panorama-log-settings

Please refer to section 4.2 for details on how to configure self-managed Syslog service.

6 FAQs

Frequently Asked Questions

1. Does SEN support port forwarding?

There are a few ways to do port forwarding, e.g., port forwarding with destination NAT or SSH port forwarding (PAN-OS has a feature called the SSH Proxy). Both are supported by PAN-OS features. It can be configured using CSENC, please refer to Palo Alto PAN-OS Administration Guide (https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin) for detailed configurations.

2. Does SEN support HTTPS content inspection?

This will require SSL Decryption. There is a setting in CSENC to create a Decryption Profile for SSL Inbound Inspection or SSH Proxy. Please refer to Palo Alto PAN-OS Administration Guide (https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin) for detailed configurations.

3. Is the SEN platform resilient?

SEN is a fully resilient platform service hosted in Telstra Universal Access Edge (UAE+) platform, offering our MPLS (IP VPN) customers purpose-built network functions, that are built for customer network function virtualisation (Telstra can easily bring up a virtual firewall online in minutes when one fails).

Palo Alto Firewall redundancy is built into SEN by being set up in High availability active-standby (Active passive mode) configuration – so if by any chance a computer node fails, or a firewall fails, the standby firewall will takeover without any session loss.

SEN has access to two different TID Links (two routers) for redundancy, so if one fails the other will be active hence the internet will not drop.

4. Are there any limitations or additional charges for SSL VPN? What is the identity / authentication process? Can the firewall use third-party authentication (Azure AD, Okta, etc)? Is this all managed within the T-Connect portal?

There is no additional cost if you are on the Advance/Premium service tier however there are a number of tunnel limits according to the size of the firewall. Below are the tunnel limits provided by Palo Alto.

SecureEdge Network Size	Palo Alto VM Model	Max Tunnels for GlobalProtect Client VPN (SSL, IPSec, and IKEwith XAUTH)	Max SSL tunnels for GlobalProtect Clientless VPNs
Small	VM-50	250	40
Medium	VM-100	500	100
Large	VM-100	500	100

SEN has the ability to use Azure AD and OKTA as the identity provider for the Client-to-site GlobalProtect implementation with Multi-Factor Authentication.

5. Is Palo Alto GlobalProtect VPN classified as an 'Always On' VPN for iOS, Android, and Windows devices?

GlobalProtect can be configured to address this requirement. It provides a tamperproof zero-touch experience allowing the administrator to set the user privileges.

6. Are we able to set up a default route for all MPLS traffic to go into the site-to-site IPSEC tunnel connected to our head office?

We can set up the default route into the IPSec tunnel.

7. Is there an ability to restrict time periods for use, bar certain websites and set quotas by applying filtering policies?

Most Palo Alto filtering policies and features are supported. There are no quotas that can be applied to the bandwidth per user.

8. Can a mobile user on raw internet have the same level of security protection without having to connect back through the business firewall?

Remote users need to connect to the virtual firewall as you cannot get SEN firewall protection for mobile users without authenticating to the firewall. This would require an IP SEC Client-to-site VPN as part of Palo Alto GlobalProtect within the Telstra SEN offering.

9. Can split tunnelling be implemented?

Split tunnelling can be used as part of GlobalProtect to send traffic to the raw internet without using the firewall, that is, you can include or exclude routes with split tunnelling.

For instance, you may want to offload certain traffic that is threat free to improve performance. You can establish policies based on application, user, content, and host information to maintain granular control over access to a given application. As per the GlobalProtect datasheet using Mobile Device Management in conjunction with GlobalProtect, an organisation can maintain visibility and the enforcement of security policy on a per-app basis while maintaining data separation from personal activities to honour the user's expectations of privacy in BYOD scenarios.

10. How does SEN get patched or updated? What is the rollout schedule for updates, i.e., does Telstra roll out updates in line with Palo Alto?

Your SEN lifecycle is managed by us, even if you are self-managing your firewall. We roll out updates based on vendor recommendations or if there is a security vulnerability or a bug that needs to be addressed via a software update. We do keep the software current and under support. If you want new features, you can request for them via product management for engineering to evaluate.

11. How is data managed and stored when it comes to SEN?

Teams in Australia and India access SEN data that is hosted in Australia.

12. How long are SEN access logs retained for?

SEN longs are retained for up to 30 days for access via the CSENC.

13. Can I run dynamic routing protocols over my IPSec tunnels?

You are free to run dynamic routing protocols over your IPSec Tunnels if you are self-managing your SEN service, however, if you have opted for SecureEdge Managed Service (SEMS), as a standard offering, we do not configure dynamic routing protocols over your IPSec tunnels.

14. Can I run dynamic routing protocols between SEN and MPLS?

We do not allow dynamic routing between SEN and MPLS as blindly propagating all advertised routes may cause routing loops and break networks.

15. Does SEN support User Identification?

Yes, User Identification is supported by SEN, but as part of standard and base firewall build, we do not configure User Identification because this setup needs some input from your end. You are free to set up User Groups if you are self-managing your firewall (you might have to raise FNC request for some management settings), however, if you have opted for SecureEdge Managed Service (SEMS), you will need to raise an FNC request.