Solution domain

User Guide
Next Generation Firewall

Date 15/01/2020
Sensitivity **Unrestricted**

Table of contents

1. Introduction

The Explore Next Generation Firewall (NG-FW) is a multitenant high grade security layer that is placed between the private Explore network and the public Internet. It allows each Customer to have its own personalized firewall protection.

When ordered, the NG-FW is pre configured with default policies allowing standard Internet services.. Those are described in the annexes of the present guide.

The management of the NG-FW can be done:

- by the Customer's own IT by the means of the configuration platform
- by Proximus by contacting the Proximus Service Desk

The goal of this user guide is get access to the configuration platform of the NG-FW and be able to manage its security configuration.step-by-step

2. Proximus Service Desk

The Service Desk is the interface between the Customer and Proximus for all aspects of the Service, including receiving, recording, registering and escalating Incidents and other requests. The Service Desk allocates resources (first line, second line, experts) and communicates regularly with the Customer.

Proximus provides the Customer with centralized Service Desk Access by phone or via a portal. The Service Desk is only accessible to authorized Customer representatives (24/7) every day of the year via the following channels:

Service Desk Access	
Phone	• 0800/14888
Portal	https://www.proximus.be/login

3. Presentation Next Generation Firewall

3.1 Product presentation

Proximus Next Generation firewall is based on Palo Alto Networks VM-series firewall technology. Palo Alto Networks is a renown security leader. The Palo Alto Networks VM- series provides an integrated set of essential security technologies.

From one easy to deploy and manage plateform, it allows advanced threat protection, including firewall, application control, advanced threat protection, IPS, and URL Filtering. Threat Prevention security services add automated protection against today's sophisticated threats. SSL teleworking functionnality is also available.

The firewall capacity and the activated set of security services depends on the chosen Proximus bundle. Following table summarizes the the available bundles

Proximus offer	Palo Alto Networks security feature
Next Generation Firewall	Application firewall protection
Advanced Security	Anti-virus Anti-Spyware Vulnerability Protection
	URL filtering
	Wildfire sandboxing
Teleworking	Global Protect

3.2 The firewall connectivity

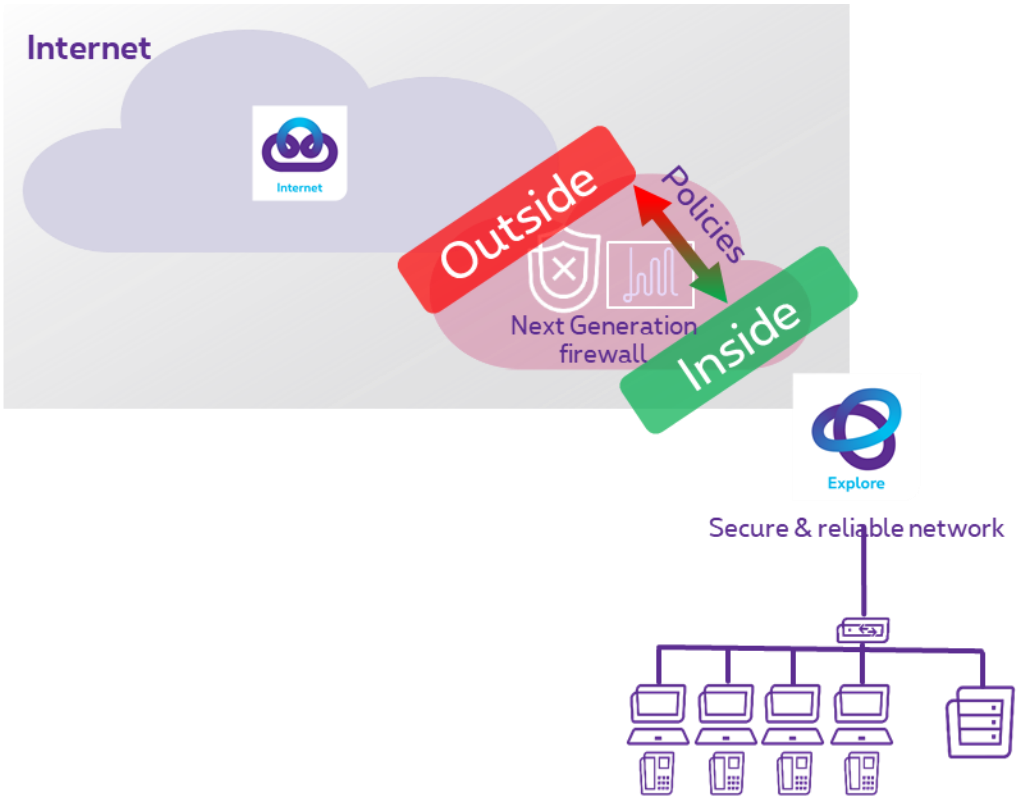
The Explore Next Generation Firewall (NG-FW) is placed between the private Explore network and the public Internet.

The firewall offers 2 interfaces:

- Inside interface: connected to the Explore private network
- Outside interface: connected to the public internet and configured with the public IP address

Proximus cares about those connectivities and assures the commited SLA on it.

The picture below gives an overview of the network architecture of this NG-FW solution:



The access to the firewall management dasboard is only possible from the inside interface.The configuration of the firewall is about defining policies between the inside and outside interfaces. Since the public IP address is configured on the outside interface, network address translation (NAT) is applied. A specific management interface is dedicated to Proximus in order to manage and operate the firewall.

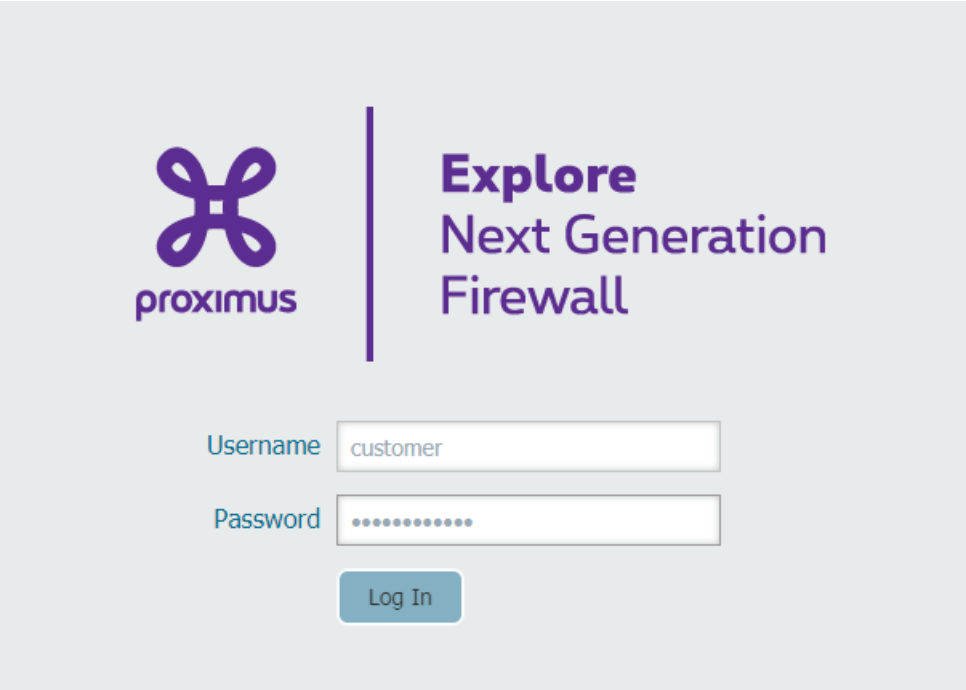
3.3 First acces to the Next Generation Firewall management dashboard

Remote access to the firewall uses the secured HTTPS protocol. You can access this firewall from your internal network using any web browser. Before accessing the home page of the firewall, you need to authenticate and are requested to change your default password provided by Proximus. You will receive by email your identifiers and the web address to access your firewall

So click on this provided web link to access your firewall and follow the procedure requested by the firewall to change the password. The firewall indicates as well the password policy needed that you apply to the new defined password. Apply those policies otherwise the new password will not be accepted by the firewall and will propose you another tentatvie to define your password.

Steps to access the firewall :

1. Click on the following link : https ://ngfw.explore.proximus.com
2. Introduce in the protal the credential provides by Proximus



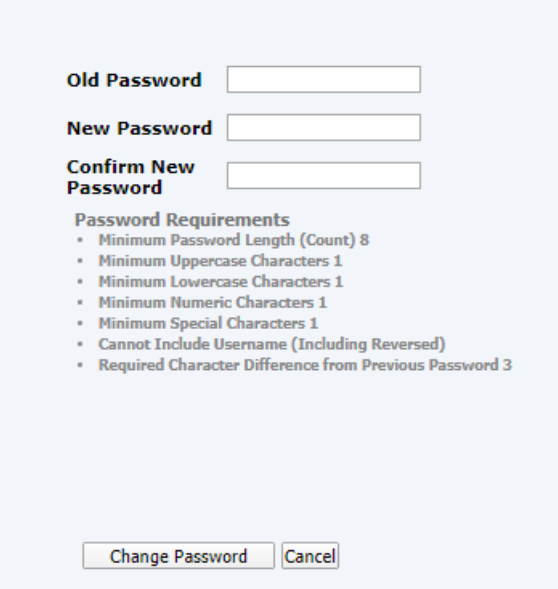
When you first connect to the firewall, you must use the following credentials:

Name : **customer**

Password : NGFW_3xplore

!! the username is also case-sensitive, make sure you type “customer” with a small “c” !!

At the first connection on the firewall, a message appears asking you to change your login password credentials. It is highly recommened to change your password at the first access to your firewall.



Old password : introduce the password provided by Proximus

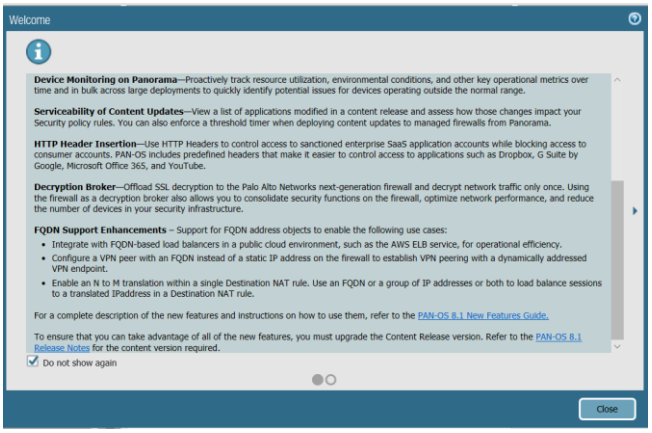
New Password : introduce your new passsword by taking into account the password requirements proposal by the portal

Confirm new password : re-introduce your new password.

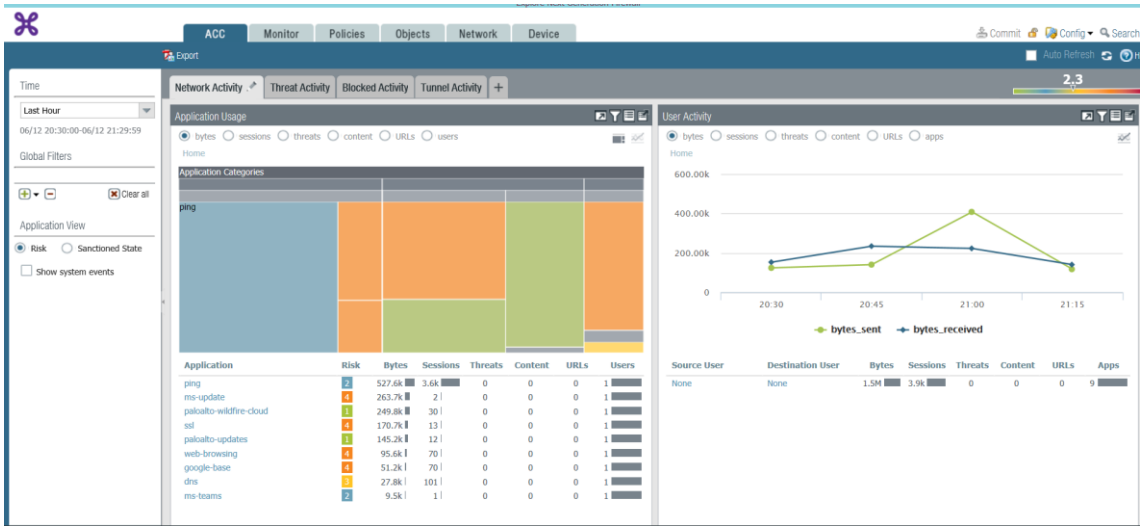
To confirm your change click then on the « change password » button.

If the new password is accepted by the firewall you will be prompted to introduce your new credentials again.

After the authentication by the firewall you will be prompted by a Welcome message.



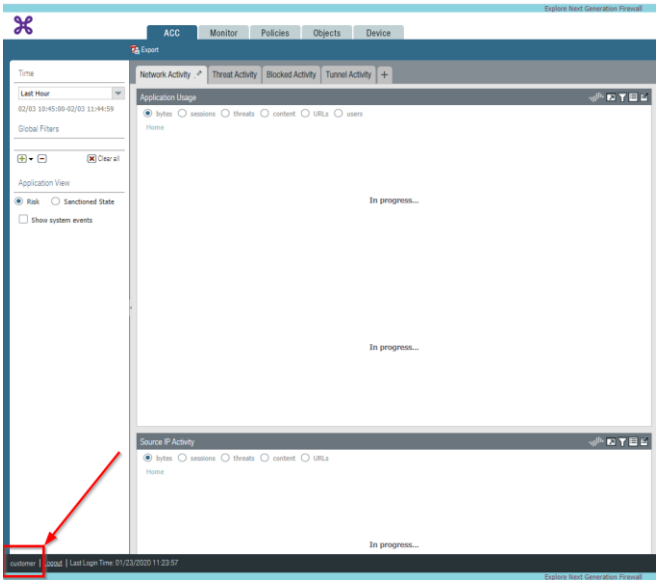
After closing this window you will get your access to the main page of the Palo Alto Networks GUI of your firewall. See picture below.



Note : If the password change message does not appear, please follow the procedure below "**How to change your password?**" to change the default password provided by Proximus.

3.4 How to change your password ?

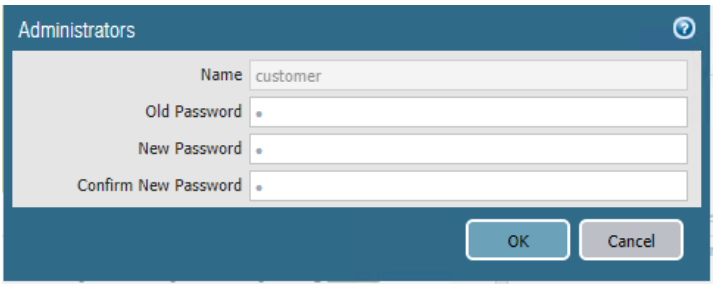
From the bottom left of the page, select the connected “customer” user .



:

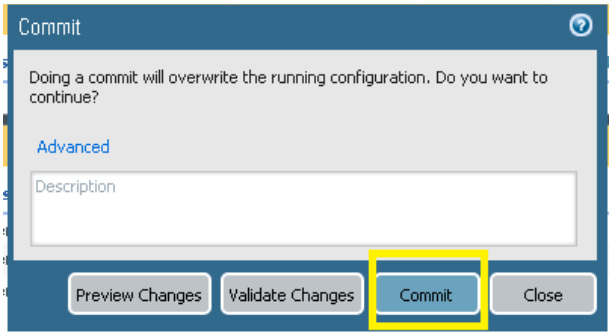
A new window appears asking you to enter the current password « NGFW_3xplore » as well as the new password you want to use to connect to your firewall.

Click then on OK to confirm your new password.



To apply the change you need to commit it : Click on the « Commit » located on the top right of the GUI :

Click the « Commit » button to confirm your changes ;



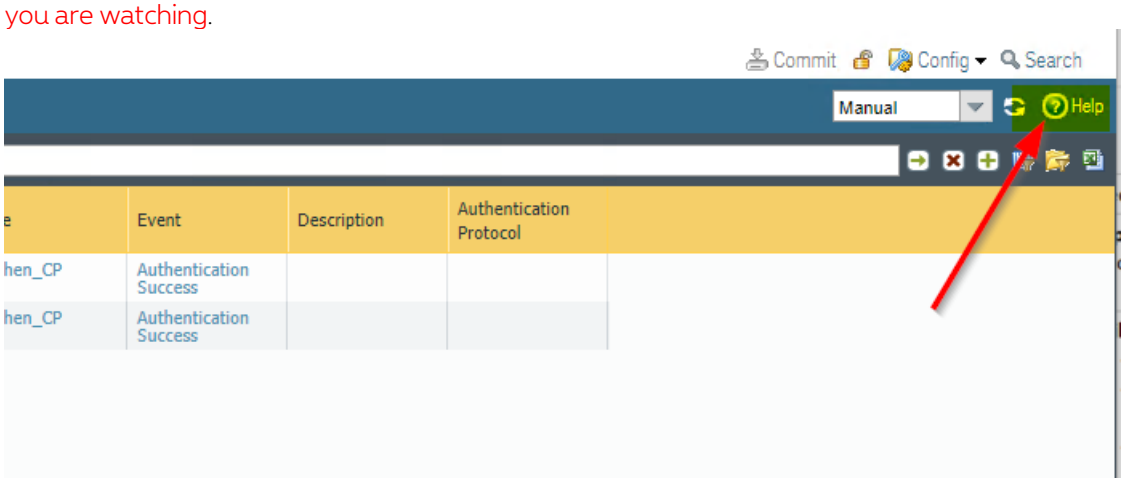
Your login and password can only be used by you. Proximus has separate credentials to access the Firewall. If you lose your password, you must contact the Service Desk to request a reset of your password.

4. Overview of the web interface of the Next Generation Firewall.

This graphical interface allows to access the firewall using HTTPS and it is the best way to perform most of the administrative tasks. The PA web interface consists of five main sections :

- The Application Command Center (ACC) : an analytical tool that provides actionable intelligence on activity within your network.
- Monitor : firewall reports and logs you can use to monitor activity on your network.
- Policies : This tab provides the firewall web interfaces you can use to configure policies (security, NAT, Policy Based Forwarding, QoS, ...)
- Objects : They are the elements that enable you to construct, schedule, and search for policy rules, and Security Profiles provide threat protection in policy rules. This tab describes how to configure the Security Profiles and objects that you can use with Policies:
- Network : It allows you to configure the network settings and parameters of your firewal as security zones, interfaces and VLANS and routing (virtual routers)
- Device : Use the following sections for field reference on basic system configuration and maintenance tasks on the firewall.

Hint: use the contextual help to learn more about the different elements present on the page you are watching.



4.1.1 The Application Control Center (ACC)

The Application Command Center (ACC) is an analytical tool that provides actionable intelligence on activity within your network. It uses the firewall logs for graphically depicting traffic trends on your network.

The Network Activity section gives you an overview of traffic and user activity on your network. The main widget of this section are :

- The Application usage widget displays the top ten applications used on your network, all the remaining applications used on the network are aggregated and displayed as other. The graph displays all applications by application category, sub category, and application. Use this widget to scan for applications being used on the network, it informs you about the predominant applications using bandwidth, session count, file transfers, triggering the most threats, and accessing URLs.
- The user activity widget displays the top ten most active users on the network who have generated the largest volume of traffic and consumed network resources to obtain content. Use this widget to monitor top users on usage sorted on bytes, sessions, threats, content (files and patterns), and URLs visited.
- The source IP Activity widget displays the top ten IP addresses or hostnames of the devices that have initiated activity on the network.
- The Destination IP Activity widget displays the IP addresses or hostnames of the top ten destinations that were accessed by users on the network.
- The rule usage widget displays the top ten rules that have allowed the most traffic on the network. Use this widget to view the most commonly used rules, monitor the usage patterns, and to assess whether the rules are effective in securing your network.

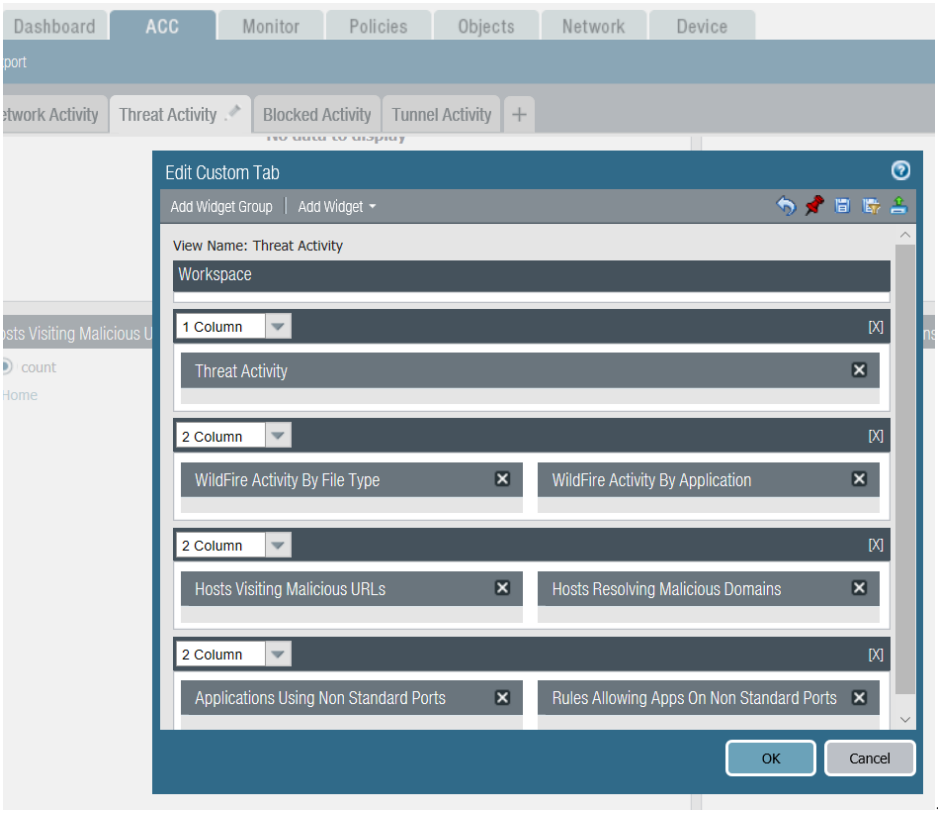
The Threat section provides an overview of the threats on the network.. This information is based on signature matches in Antivirus, Anti-Spyware, and Vulnerability Protection profiles and viruses reported by WildFire.

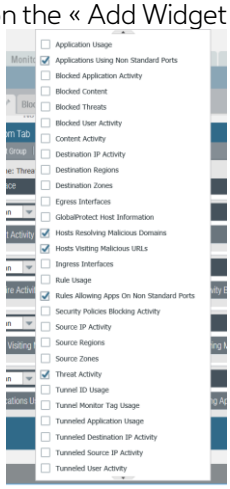
The Blocked Activity section focuses on traffic that was prevented from coming into the network

- The Blocked Application Activity widget displays the applications that were denied on your network, and allows you to view the threats, content, and URLs that you kept out of your network.
- The Blocked User Activity widget displays user requests that were blocked by a match on an Antivirus, Anti-spyware, File Blocking or URL Filtering profile attached to Security policy rule.
- The Blocked Threats widget displays the threats that were successfully denied on your network. These threats were matched on antivirus signatures, vulnerability signatures, and DNS signatures available through the dynamic content updates on the firewall.
- The Blocked Content widget displays the files and data that was blocked from entering the network. The content was blocked because security policy denied access based on criteria defined in a File Blocking security profile or a Data Filtering security profile.

- Security Policies Blocking Activity widget displays the security policy rules that blocked or restricted traffic into your network. Because this widget displays the threats, content, and URLs that were denied access into your network, you can use it to assess the effectiveness of your policy rules. This widget does not display traffic that blocked because of deny rules that you have defined in policy.

You can remove and add individual widgets, as needed on all the ACC tabs. To add a widget to one of the ACC tab, select the « pen » on the left of the tab name. A new window is prompted and allow you to add and custom widgets. See figutre below.

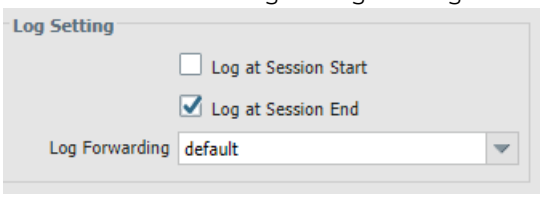


Then click on the « Add Widget » drop down list and select all the widgets you want to add in this section.  .To delete a widget, click the ☒ symbol in the title bar.

4.1.2 The Monitor Tab

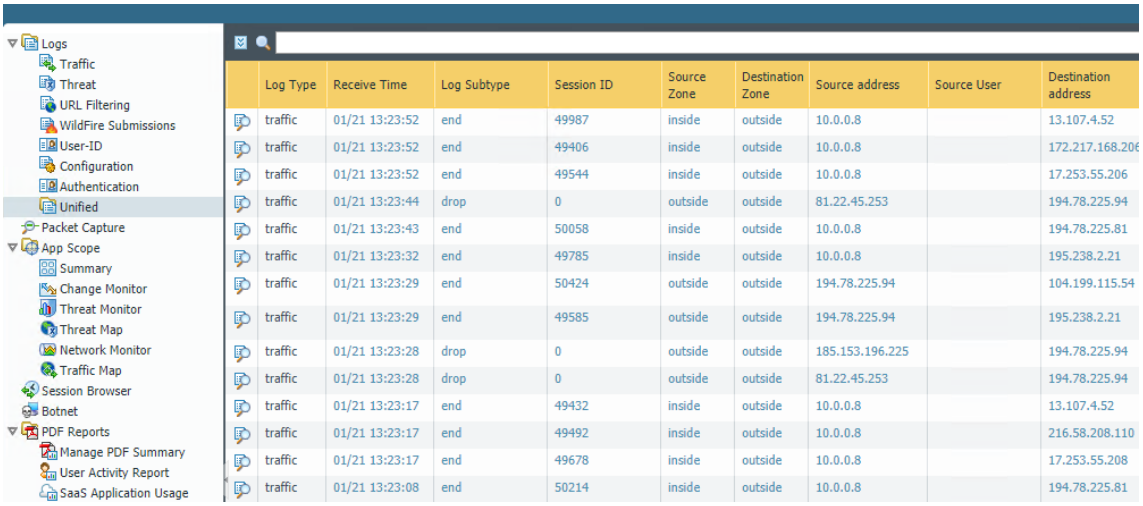
This section of the GUI provides you all the logs you need to monitor the traffic of your network.

- **Traffic logs** : related to the traffic crossing the firewall. Remark : the firewall policies must have the correct log settings for logs to be collected – by default :

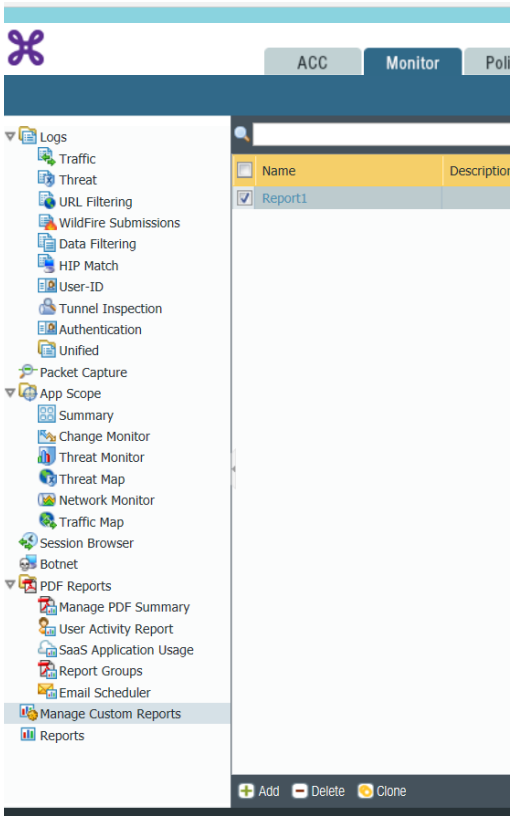


- **Threats :** will centralize all security alarms generated by the firewall. Types can vary (Virus, Malware, etc). Certain protections, like Antivirus, are part of the Advanced security pack available in option at Proximus, as well as **URL Filtering and Wildfire.**
- **User-id logs** : shows events related to the Palo Alto UserID™ function
- **System logs** : contains configuration changes that occured on your firewall (including Proximus interventions)
- **Authentication** : centralizes access authentication-related events (generally related to the Teleworking and UserID™ functions).

- **Unified** : Displays the latest Traffic, Threat, URL Filtering and WildFire Submissions log entries in a single view. The collective log view enables you to investigate and filter these different types of logs together (instead of searching each log set separately). Or, you can choose which log types to display: click the arrow to the left of the filter field and select **traffic**, **threat**, **url**, and/or **wildfire** to display only the selected log types.



Log Type	Receive Time	Log Subtype	Session ID	Source Zone	Destination Zone	Source address	Source User	Destination address
traffic	01/21 13:23:52	end	49987	inside	outside	10.0.0.8		13.107.4.52
traffic	01/21 13:23:52	end	49406	inside	outside	10.0.0.8		172.217.168.206
traffic	01/21 13:23:52	end	49544	inside	outside	10.0.0.8		17.253.55.206
traffic	01/21 13:23:44	drop	0	outside	outside	81.22.45.253		194.78.225.94
traffic	01/21 13:23:43	end	50058	inside	outside	10.0.0.8		194.78.225.81
traffic	01/21 13:23:32	end	49785	inside	outside	10.0.0.8		195.238.2.21
traffic	01/21 13:23:29	end	50424	outside	outside	194.78.225.94		104.199.115.54
traffic	01/21 13:23:29	end	49585	outside	outside	194.78.225.94		195.238.2.21
traffic	01/21 13:23:28	drop	0	outside	outside	185.153.196.225		194.78.225.94
traffic	01/21 13:23:28	drop	0	outside	outside	81.22.45.253		194.78.225.94
traffic	01/21 13:23:17	end	49432	inside	outside	10.0.0.8		13.107.4.52
traffic	01/21 13:23:17	end	49492	inside	outside	10.0.0.8		216.58.208.110
traffic	01/21 13:23:17	end	49678	inside	outside	10.0.0.8		17.253.55.208
traffic	01/21 13:23:08	end	50214	inside	outside	10.0.0.8		194.78.225.81



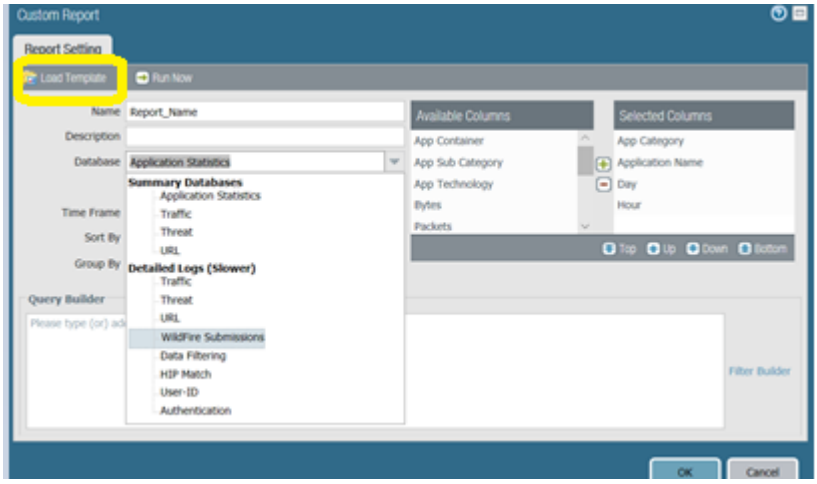
From the Monitor tab you can also configure several types of reports that the firewall generates immediately (on demand) or on schedule.

For example to generate a custom report

1. Select « **Manage Custom Report** »

2. Click **Add** then enter the name for the report.

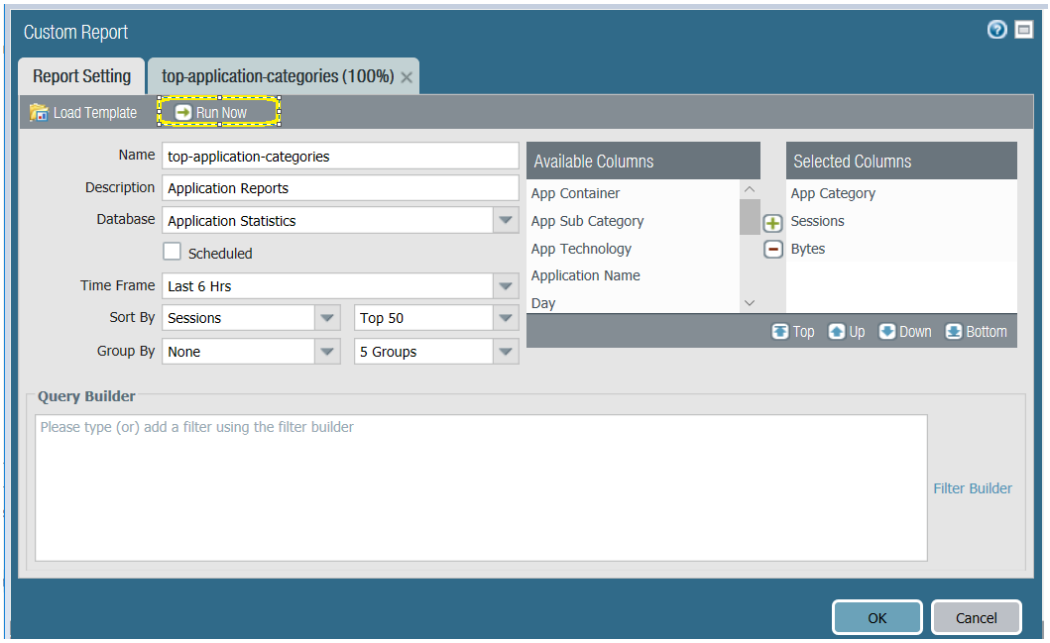
3. To base a report on an predefined template, click Load Template and choose the template. You can then edit the template and save it as a custom report.



4. Select the **Database** to use for the report
5. Select the Scheduled **check box** and define the filtering criteria : Select the Time Frame, **the** Sort By **order,** Group By **preference**, and select the columns that must display in the report.
6. Optionally select the Query Builder attributes if you want to further refine the selection criteria.

For example, the following figure (based on the Traffic Log database) shows a query that matches if the Traffic log entry was received in the past 24 hours and is from the untrust zone.

7. To test the report settings, select Run Now. Modify the settings as required to change the information that is displayed in the report.



8. Click **OK** to save the custom report.

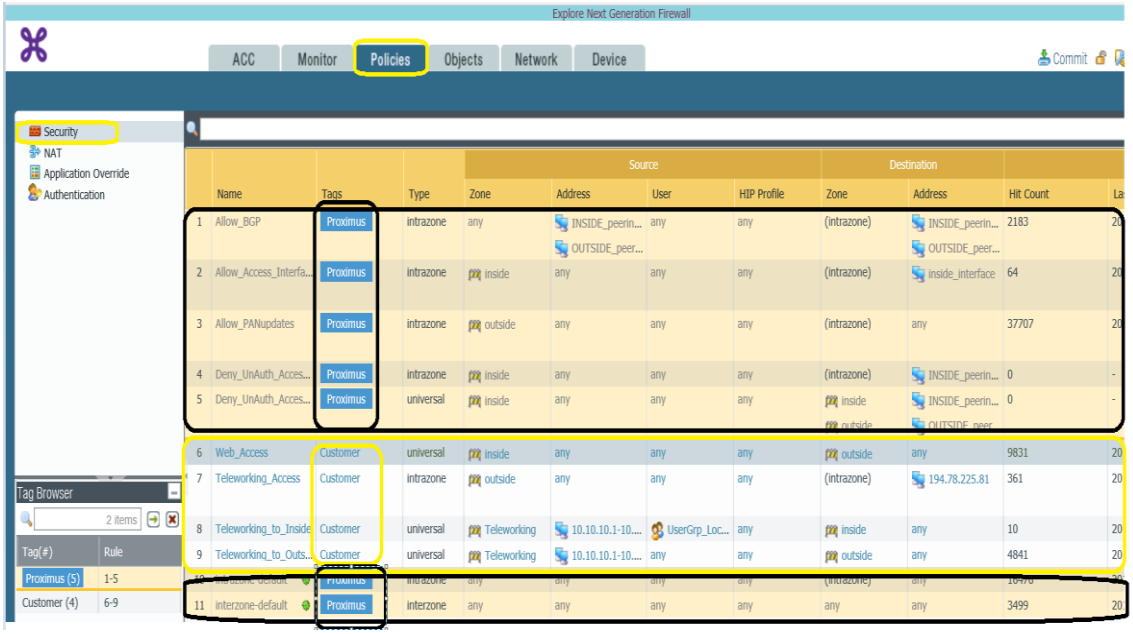
4.1.3 The Policies

This section of the GUI allows you to define all policies you need to configure in your firewall :

- Security rules
- Network Address Translation
- Application Override
- Authentication.

By default the Firewall is pre-configured by Proximus, including some security and NAT rules. **Those policies are displayed in orange and cannot be modified**. Those standard policies do not intervene in the customer's traffic, but are there to ensure the basic functionalities of the firewall, like access to the Explore network, or access to the management interface by the customer.
The customer can add his own access policies as needed, which will automatically be correctly placed between the orange pre-defined Proximus policies.

The figure below illustrates an example of customer policies implemented in the firewall.

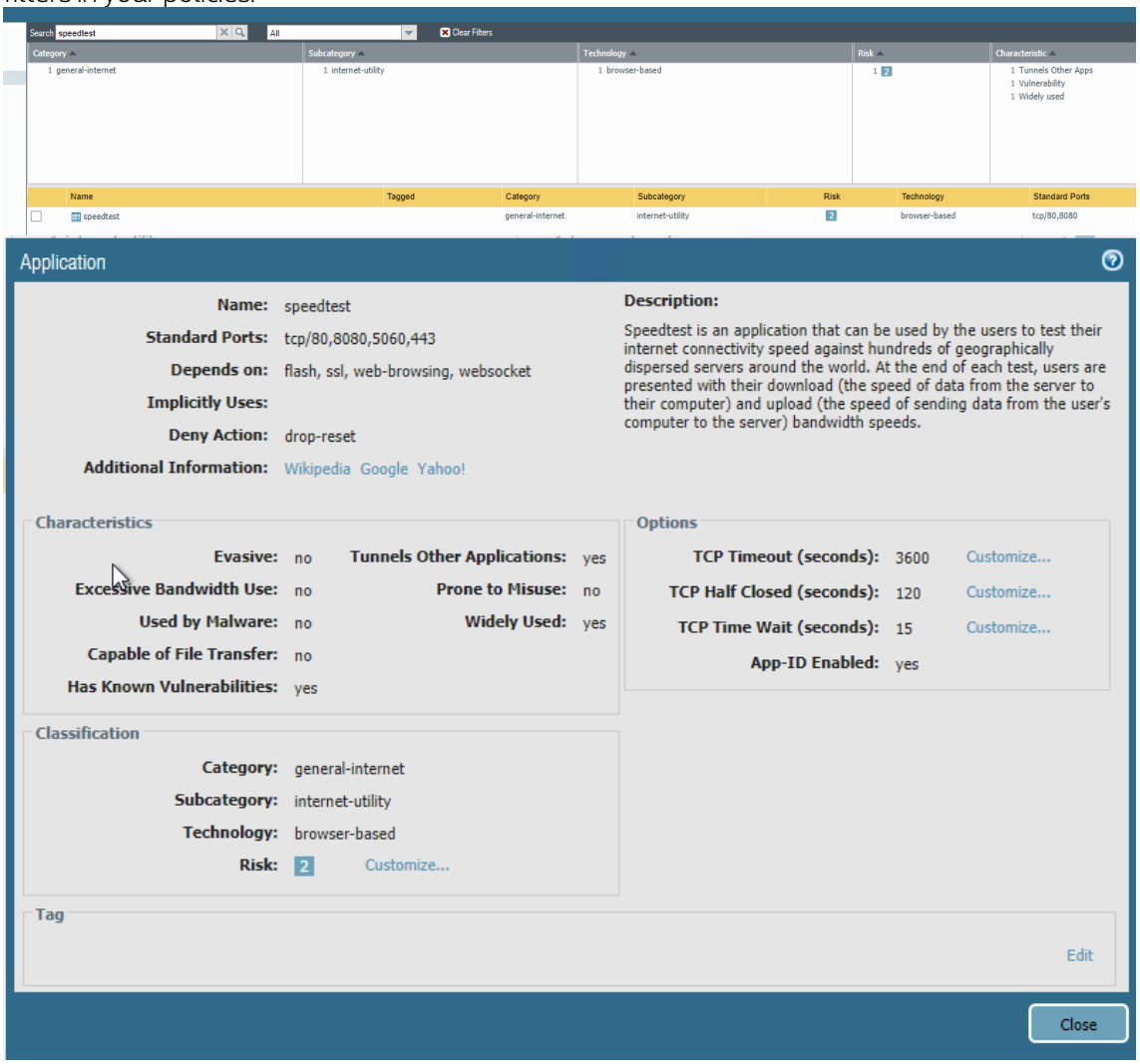


4.1.4 The Object Section

Objects are the elements that enable you to construct, schedule, and search for policy rules and Security Profiles provide threat protection in policy rules.

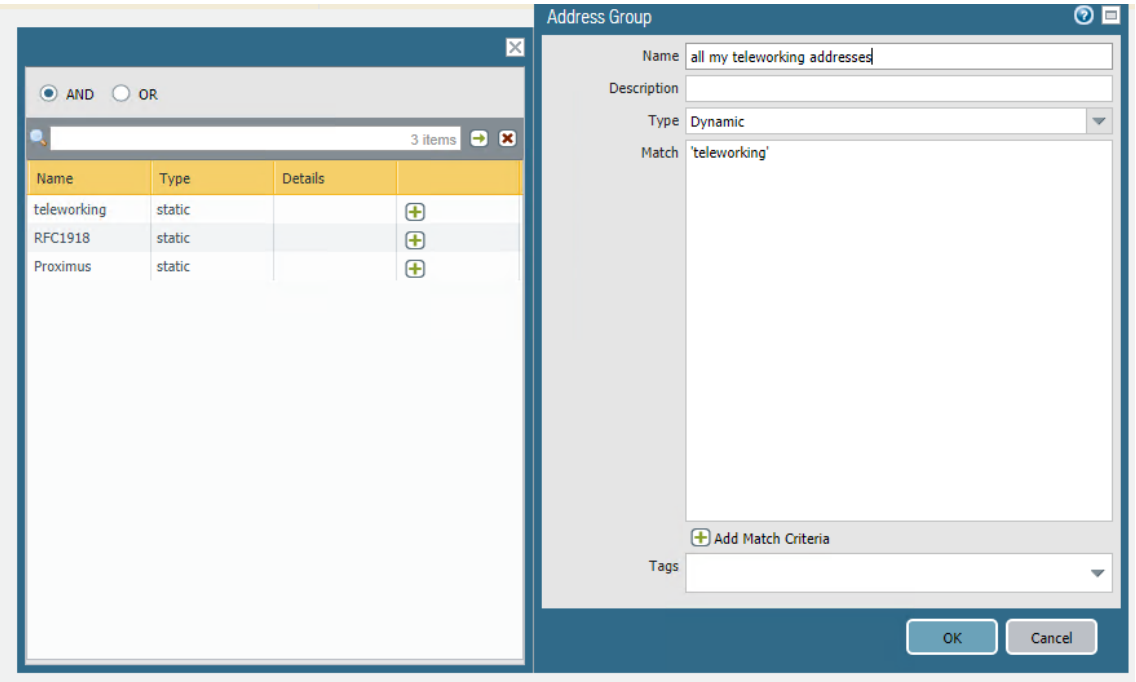
Addresses and Address groups: permit to define IP subnets, ranges or FQDN (which can be grouped) to be used in a firewall policy

Applications (and Application groups/filters): this Next Generation firewall is provided with a complete, constantly updated list of applications (provided and maintained by Palo Alto). In the application page, you can find all the known application, which can be used to do next-generation filtering. Used in a firewall policy, those applications permit more granular and precise filtering than with the TCP/UDP port filtering generally available if previous-generation firewalls.
Using the **search** field, you can easily find the application you look for, and see all details, dependencies etc. about it.
See below for a more detailed explanation on how to use applications, applications groups and filters in your policies.



The **Services and Service Groups** offer the possibility to configure TCP and/or UDP ports to match in firewall policies, either in combination with application filtering (for example to limit an application to certain ports), or in standalone if you do not want to filter at application level.

Tags is a feature available all over the firewall, which permits to refer to specific keywords (tags) instead of the objects directly. It can be used with varied objects. As an example, with IP addresses, you can create a **dynamic** address group that will contain all **Addresses** with the tag "**teleworking**", and use it in a firewall policy (see below screenshot).



Each new **Address** that will receive the same tag will be automatically added to the **Address Group**, as well as removing the tag from an **Address** will remove it from the group. That is a powerful feature that we advise you to use where needed.

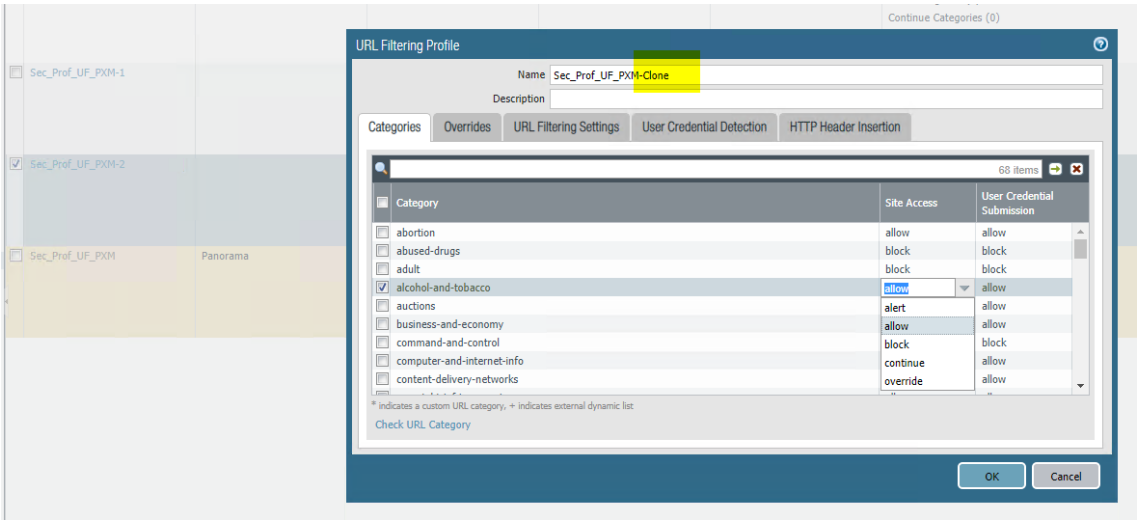
Note : it might require that you Commit your changes before the dynamic group is updated with the actual objects matching the tag…

External dynamic list is an address object based on an imported list of IP addresses, URLs, or domain names that you can use in policy rules to block or allow traffic. Proximus can eventually populate that list if needed. With an **active Promixus Advanced Security pack**, Palo Alto Networks® provides two Dynamic IP Lists: Palo Alto Networks - High risk IP addresses and Palo Alto Networks - Known malicious IP addresses. The firewall receives daily updates for these feeds through antivirus content updates.

Custom Objects are related to the advanced security features and are configured by Proximus, with the exception of URL category. They are meant to be use in conjonction with their corresponding security profiles (see below).

Security Profiles contains all advanced security included in the **Promixus Advanced Security pack.** For every feature, there is one or more default profile that cannot be changed or deleted and is part of the **Palo Alto default** configuration, and a **Proximus-default (in orange)** that can be used, but not modified as well.

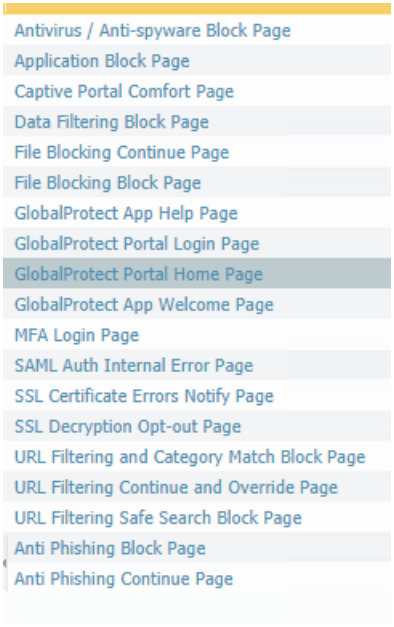
In order to create your own profile, you can either create if from scratch, or Clone an existing one. The newly created object can then be freely configured as you need, and then referred in security policies.



4.1.5 The Device Section

This section details several elements related to the device configuration globally, including :

- URL filtering timers
- App-ID settings
- Response pages configuration & customisation : Response pages are used in several situations, like URL filtering, Teleworking etc. You can upload a customized version of each page, or consult the details of the page in-use.



- Local User database can be use to authenticate users before they are allowed through the firewall (Teleworking or UserID™).

- Global Protect Client show the version of Teleworking client proposed on the Teleworking portal (maintained by Proximus)

- Dynamic updates gives you and information about the different subscriptions updates, with a status, schedule information and release notes. (maintained by Proximus).

- Licenses : on this page you can see the status of the different licenses installed on the firewall. Proximus has the charge to update and maintain all licenses related to the package you have bought. The amount of licenses depend on the options active on the product.

5. Change handling with customer's specific access rights

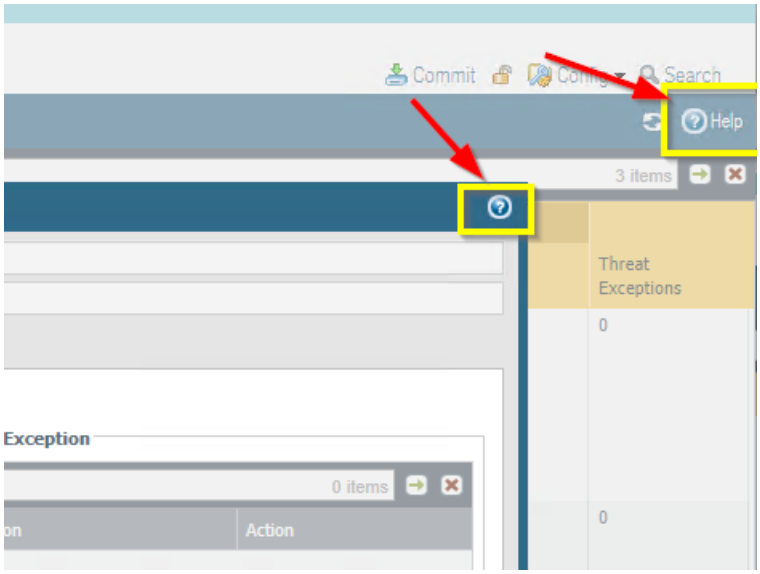
5.1 General: Commit configuration changes in the firewall

In this guide, you will learn how to use the user interface to configure most Next Generation Firewall settings and parameters. Please note that the configuration changes made using this interface do not take effect immediately. **To apply any configuration change you must click on the commit button located at the top right of the WEB interface**.

This applies to all updates in the firewall configuration.

5.2 General: help pages

The firewall ships with contextual help, that can be useful if you seek more details about certain options. Seek for the help icon, present in most of the configuration pages to access the help pages.

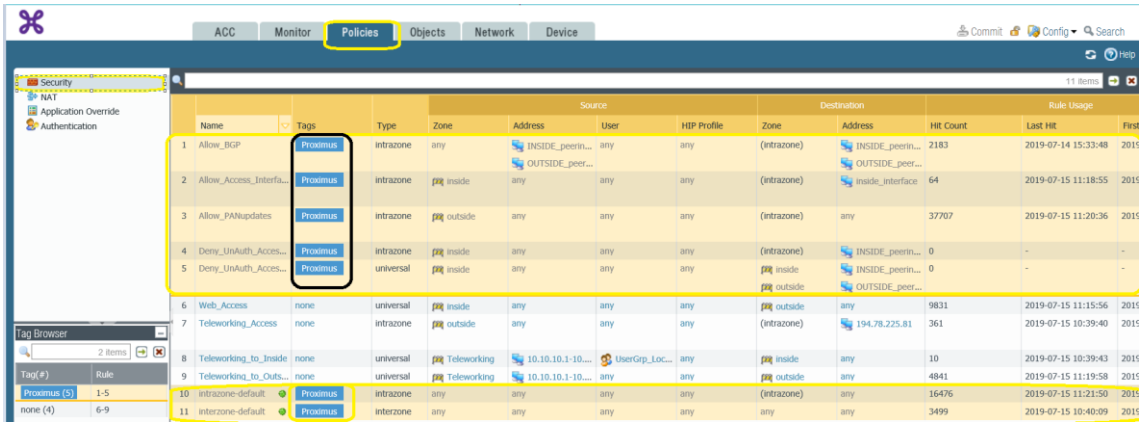


5.3 Configuration of a Security Policy.

This is probably the main configuration you might need to implement on the firewall.

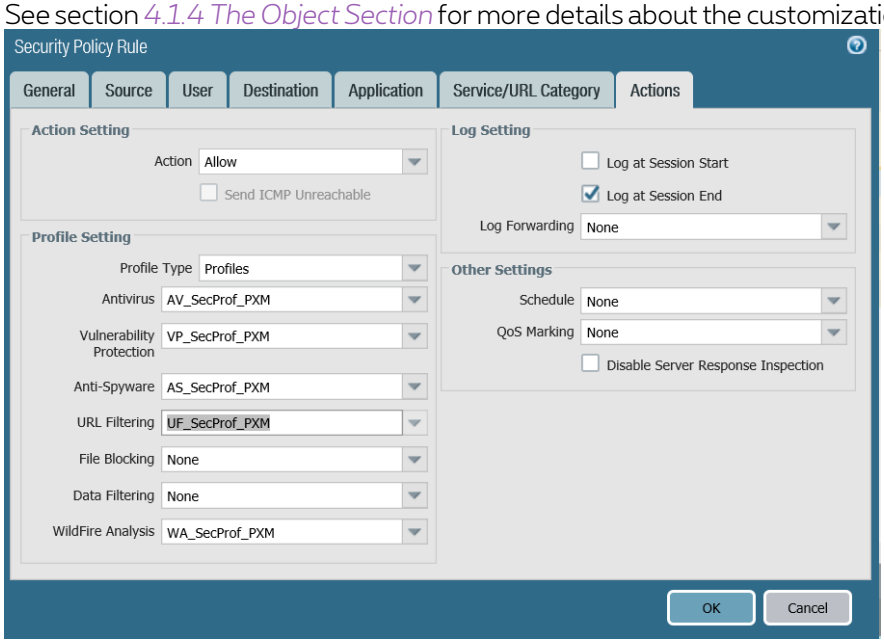
By default Proximus configure a set of default policies that you can see on the policy section of the GUI : (read only policies). These policies are not influencing the customer traffic, but rather ensure basic connectivity is always present in & trhough the firewall at all times. In other words, those policies will NOT be involved in your traffic management.

Those policies could not be modified or deleted by the customer. But you can add your own security policies to control the traffic that will traverse your network.



In order to provide a basic access to Internet to the customer from the beginning, Proximus pre-provision a “Web_Access” policy allowing all traffic from the internal network to Internet, along with a standard NAT rule. **This policy should be adapted or even replaced by the customer in order to satisfy his internet access requirements**. The NAT rule, on the other hand, cannot be removed, but can be overwritten by other NAT rules.

If the customer subscribes to the" **Advanced Security**" service, a set of security profiles are applied to this policy in order to protect the customer from malicious traffic (virus, malware, spyware….). See section *4.1.4 The Object Section* for more details about the customization of security profiles.



5.3.1 What does "Next Generation" mean ?

This Next Generation firewall allows you to specify security policies based on **accurate identification of each application** that will traverse your network. Unlike traditional firewalls that identify applications only by protocol and port number, the Next Generation Firewall uses packet inspection and a library of application signatures to distinguish between applications that have the same protocol and port and to identify potentially malicious applications that use nonstandard ports.

To safely enable the use of applications, maintain complete visibility and control, and protect the organization from the latest cyber threat, you can define security policies for specific applications or application groups rather than use a single policy for all port TCP 80 connections for example. For each identified application, you can specify a security policy to block or allow traffic based on the source and destination zones and addresses (IPv4 and IPv6). Each security policy can also specify security profiles to protect against viruses, spyware, and other threats.

Security policies reference security zones and enable you to allow, restrict, and track traffic on your network based on the application, user or user group, and service (port and protocol).

Note: though this is not the advised way, it is still possible to fall back on the "classical" TCP/UDP port filtering instead of using the application-based filtering. To do so, simply enable all applications in your policy and specify the TCP/UDP ports to filter in the "Service/URL Category" tab.

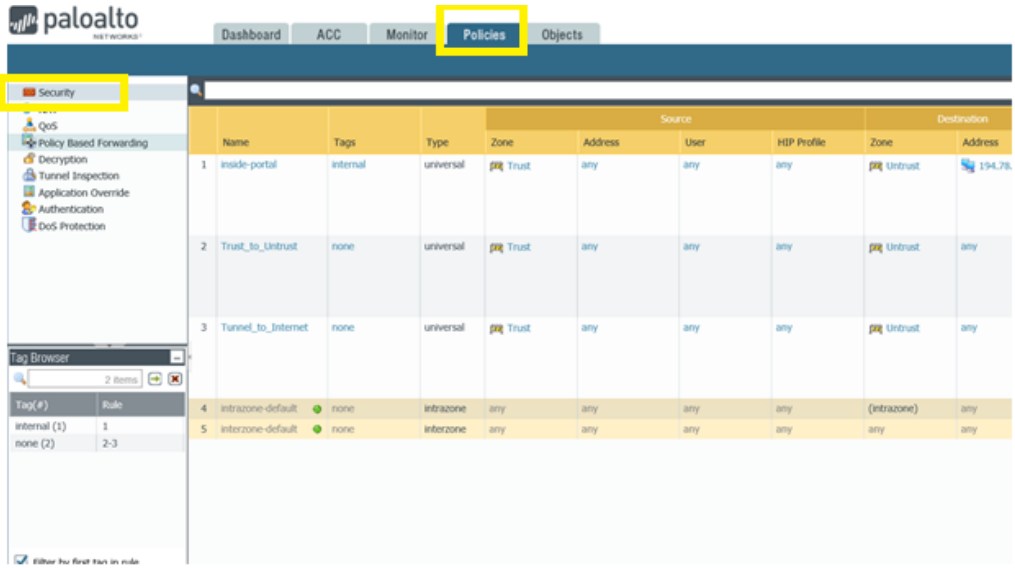
5.3.2 How to create a security policy ?

STEP 0: Create all necessary objects you will require in your policy in the **Objects** tab.

Note: In most cases, the system will permit you to create also objects "on the fly" directly inside the policy, but we strongly suggest that you create the necessary objects before creating the policy, as it will ease their organization, especially when there are a big amount of them.

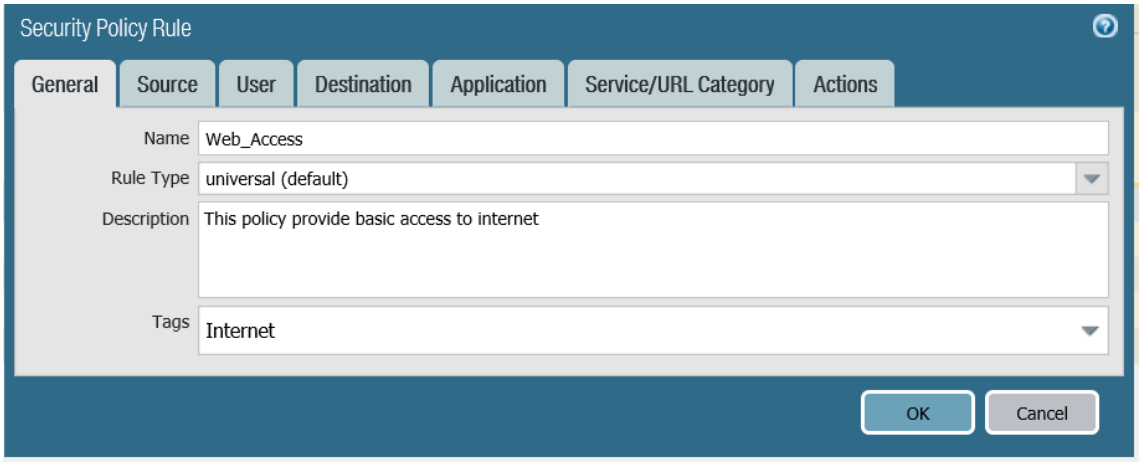
STEP 1: On the Firewall GUI click the policy tab and select « **security** ». See figure below. And add a security rule.

- **Select Policies > Security and click Add.**



STEP 2: Define the policy name and type of rule.

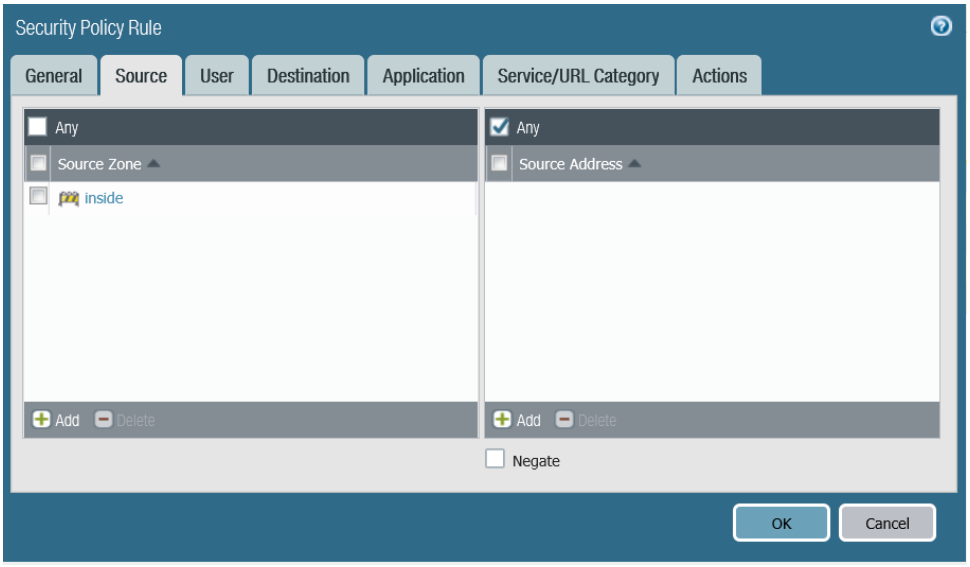
- **Enter a descriptive Name for the rule in the General tab.**
- **Select a Rule Type. (keep the default value)**
- **(optional) add one of more Tags related to the policy**



STEP 3: Define the matching criteria for the source fields in the packet.

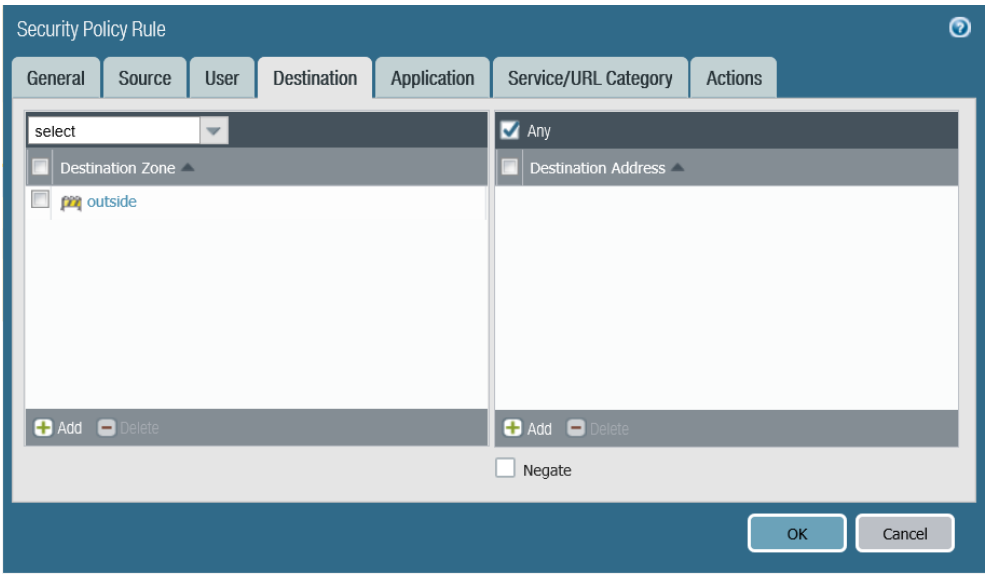
- In the Source tab, select a Source Zone. The zones are:
  - Inside (Explore side): This is the trust zone where all your Explore connections are located
  - Outside (Internet side): This zone is the untrust zone (the internet)
  - A third zone (Teleworking) is defined if the customer has subcribed to the Telewoking service: all traffic from/to the remote users (Teleworkers) will be in relationship with that zone.

- Specify one or more Source IP Address (or address group) or leave the value set to any.
- Specify a Source User or leave the value set to any.



STEP 4: Define the matching criteria for the destination fields in the packet.

- In the Destination tab, set the Destination Zone.
- Specify a Destination IP Address or leave the value set to any



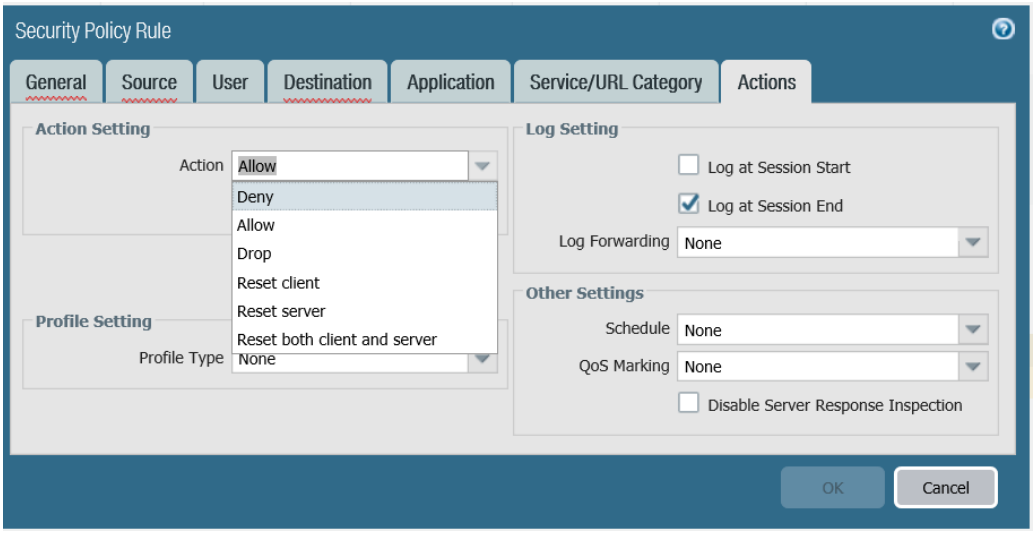
STEP 5: Specify the application the rule will allow or block.

As a best practice, always use application-based security policy rules instead of port based rules and always set the Service to application-default unless you are using a more restrictive list of ports than the standard ports for an application.

- In the Applications tab, Add the Application to safely enable. You can select multiple applications, or use application groups or application filters.
- In the Service/URL Category tab, keep the service set to application-default to ensure that any applications permitted by the rule are only allowed on their standard ports.

STEP 7: Define what action you want the firewall to take for traffic that matches the rule

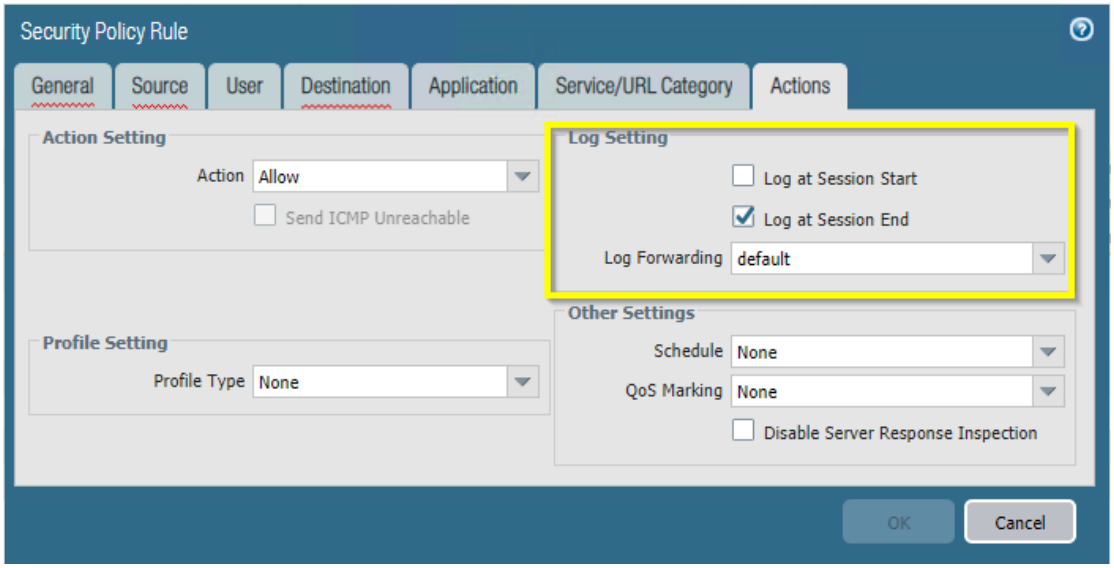
Allow—(default) Allows the matched traffic.
Deny—Blocks matched traffic and enforces the default Deny Action defined for the application that is denied. To view the deny action defined by default for an application, view the application details (*Objects* > *Applications*).
Because the default deny action varies by application, the firewall could block the session and send a reset for one application while it silently drops the session for another application.
Drop—Silently drops the application. A TCP reset is not sent to the host or application.
Reset client—Sends a TCP reset to the client-side device.
Reset server—Sends a TCP reset to the server-side device.
Reset both—Sends a TCP reset to both the client-side and server-side devices.



STEP 8 (optional): Configure Log settings.

- select the moment where a log entry should be written (start or end or both).
  Note: unless – at least – one is selected, no log will be written for that specific policy, so no reporting or troubleshooting will be possible on such traffic.
  - **By default, log settings are set to "log at Session End", which is fine for most traffic**.

- **Log Forwarding: please leave this setting to the default value, as is will permit Proximus to receive a copy of the logs, which are used for support and global traffic analysis for eventual security actions we can take to protect all our customers from some threats.**

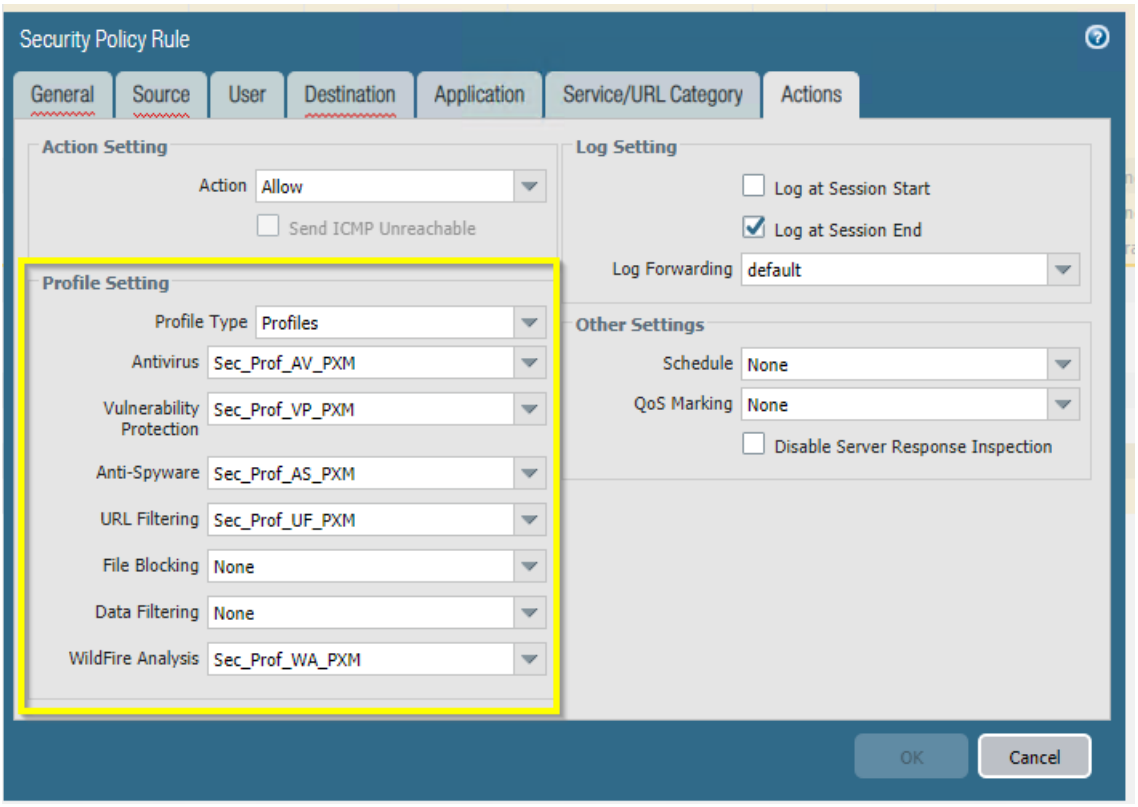


STEP 9: Attach security profiles to enable the firewall to scan all allowed traffic for threats.

(Only for customers who subscribe to the advanced security service)

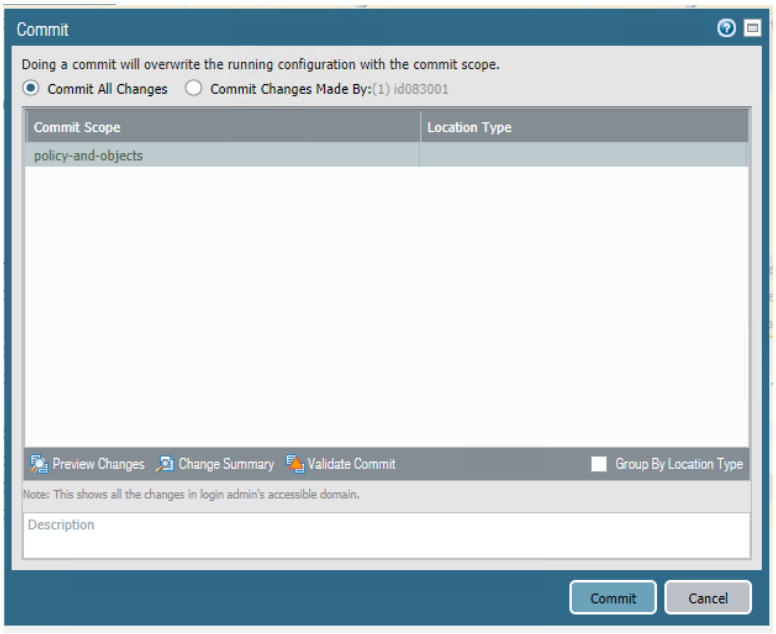
- In the **Actions** tab, select Profiles from the Profile Type drop-down and then select the individual security profiles to attach to the rule (Proximus default or customized version).
  see section *5.1.3 How to create security profiles?* for more information about how to create customized security profiles

Note: Proximus does not implement File Blocking and Data Filtering features in his managed product.



STEP 10 Save the policy rule to the running configuration on the firewall.

- Commit your changes (you can add a description on the changes for easier tracing)



5.3.3 How to create custom Security Profiles ?

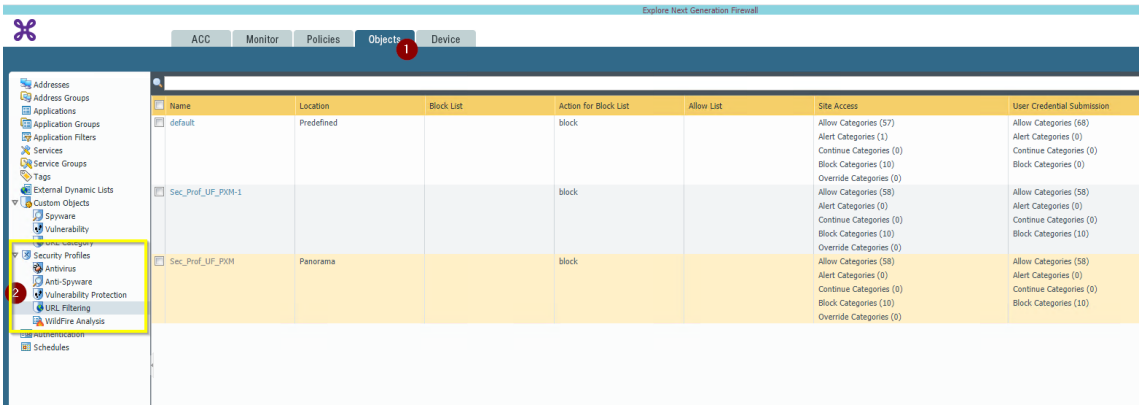
By security profiles, we are referring to all security features we can implement on top of the standard firewall inspection. A NGFW is able to analyze the content of the packets over the life of a session in order to detect and block malicious or illegitimate traffic. Security profiles are objects that allow to configure those advanced features. They represent additional security checks to be performed on allowed network traffic. So they provide a more granular control over allowed traffic. Security Profiles implement therefore additional security checks on allowed traffic.

The Proximus Managed Next Generation Firewall offers several types of Security Profiles:

- Antivirus
  - Detects infected files being transferred with the application
- Anti-Spyware
  - Detects spyware donwloads and traffic from already installed spyware.
- Vulnerability protection (IPS)
  - Detects attempts to exploit known software vulnerabilities.
- URL filtering
  - Classifies and controls web browsing based on content
- Wildfire Analysis (Cloud base malware analysis)
  - Forward unknown files to the Wildfire service for malware analysis

As best practices, it is recommended to implement the Proximus pre-defined default security profiles. These default security profiles are applied to the standard initial configuration and follow this naming convention: Sec_Prof_xx_PXM Where "xx" is replaced by the profile type (AV for Antivirus, VP for Vulnerability protection etc.).

Note: by default, there is also a built-in profile for most security feature, that is part of the PanOS system and cannot be removed or changed (below in white). We advise **not to use them**, but **prefer the Proximus version (in orange),** as we can update those profiles to adapt to new threats, and if used in a policy, apply new protection automatically to all our managed customers.

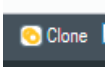


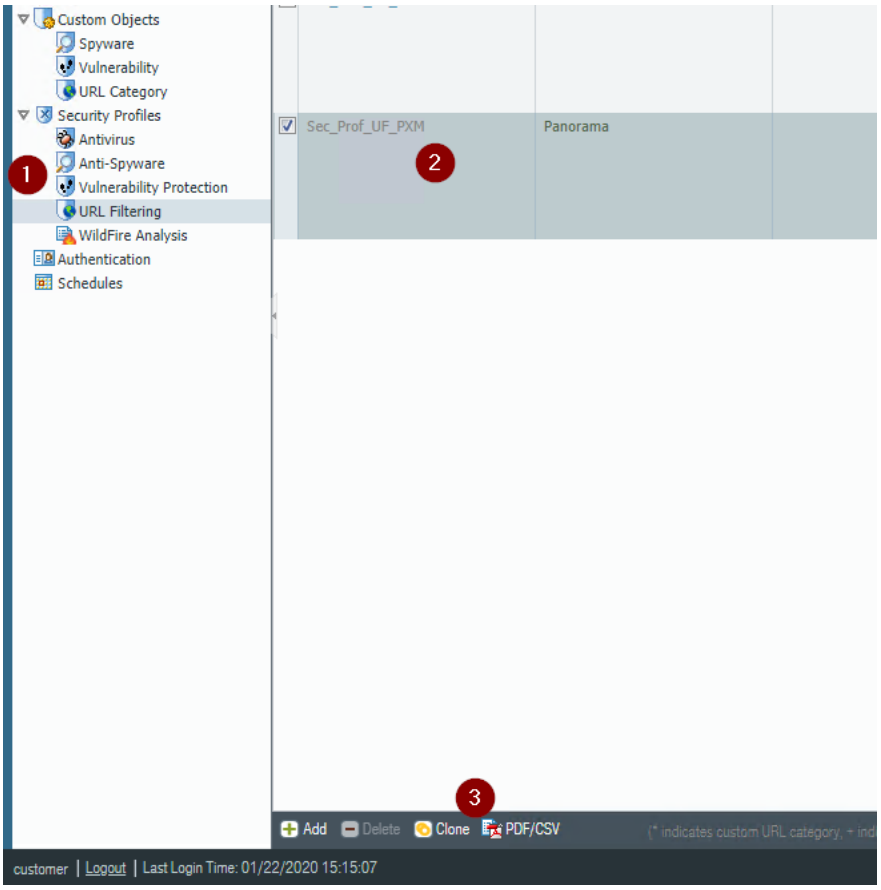
5.3.3.1 Configuration steps for a customized profile

In case you need to modify the standard configuration proposed by Proximus, here are the steps to follow.

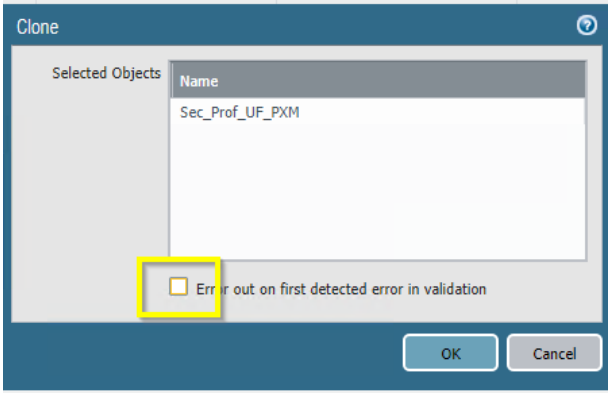
The below procedure takes **URL filtering as example**, but you can easily adapt to any other type of profile:

STEP 1: Clone the Proximus standard profile

From the correct profile type (left panel), select the Proximus standard profile and hit 

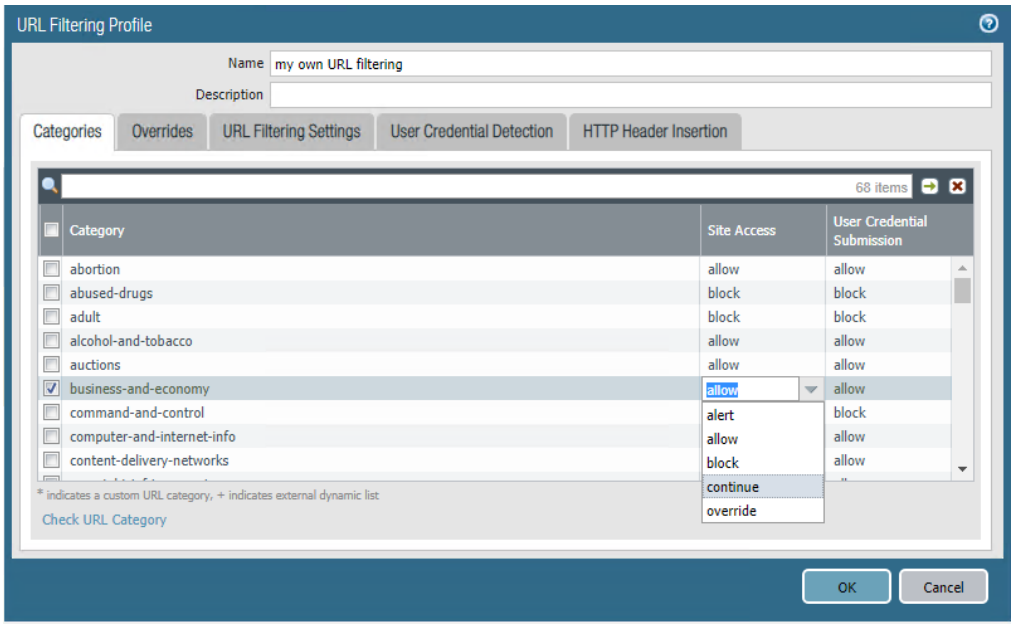


A pop-up windows will appear informing you of the name of the future profile. It is recommended to uncheck the "Error out on first detected error in validation" checkbox as it can, in some rare cases, cause issues in the cloning process.

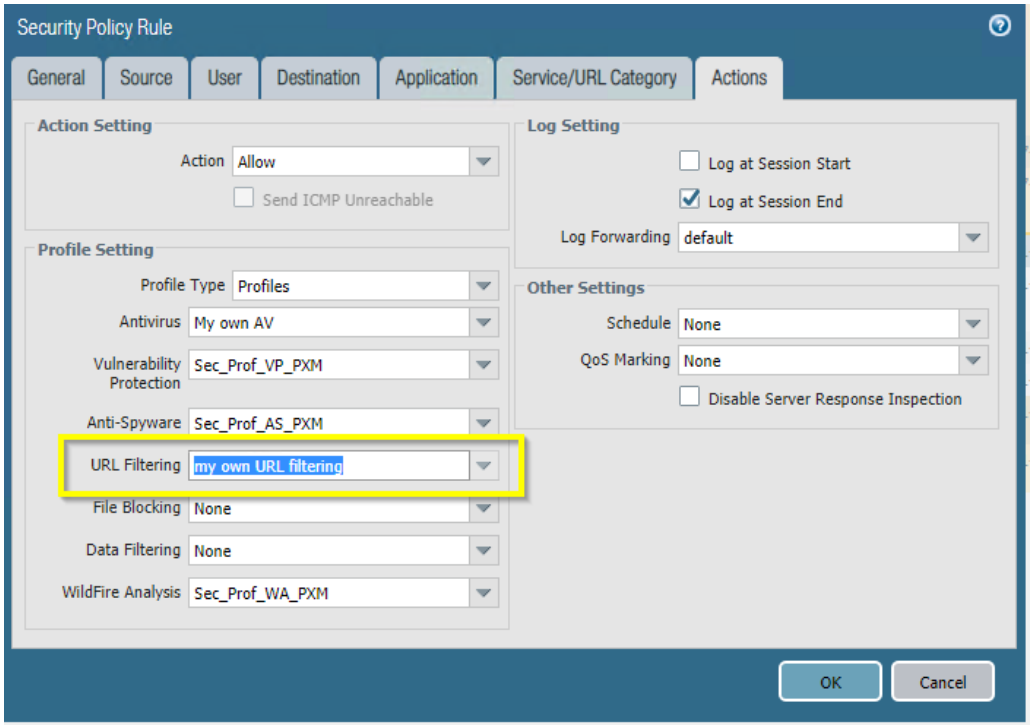


STEP2: adapt the profile as needed

Select the newly created profile and modify what you need into it. You shall also provide it an easy-to-recall name… once finished, **click "OK"**



STEP3: assign the profile to a security policy



STEP4: commit your changes

5.3.3.2 Possible Actions per Security Profile

Action	Description	Antivirus Profile	Anti-Spyware profile	Vulnerability Protection Profile	Custom Object—Spyware and Vulnerability	URL filtering profile
Default	Takes the default action that is specified internally for each threat signature. For antivirus profiles, it takes the default action for the virus signature.	V	V	V	—	—
Allow	Permits the application traffic.	V	V	V	V	V
Alert	Generates an alert for each application traffic flow. The alert is saved in the threat log.	V	V	V	V	V
Drop	Drops the application traffic.	V	V	V	V	—
Reset Client	For TCP, resets the client-side connection. For UDP, the connection is dropped	V	V	V	V	—
Reset Server	For TCP, resets the server-side connection. For UDP, the connection is dropped	V	V	V	V	—

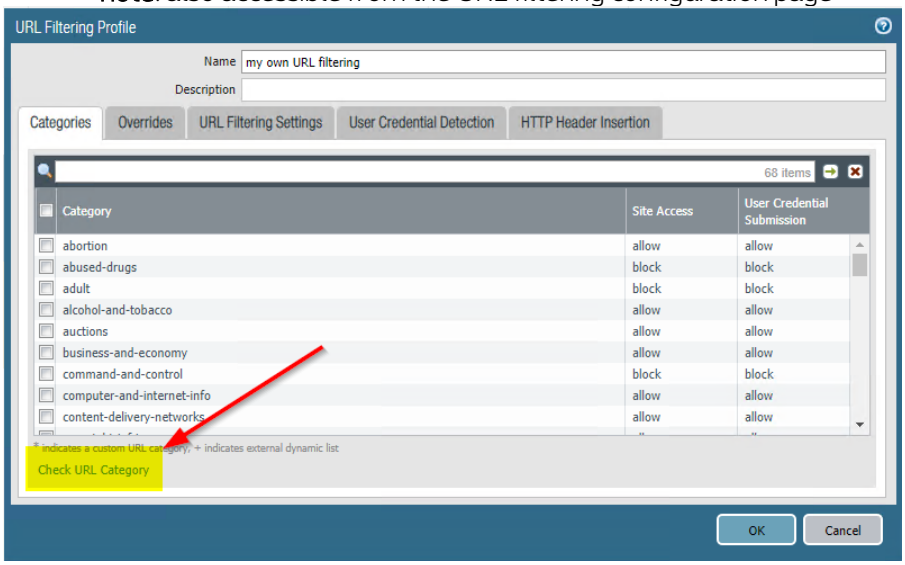
Reset Both	For TCP, resets the connection on both client and server ends. For UDP, the connection is dropped	V	V	V	V	–
Block	Blocks access to the web site. If the Site Access to a URL category is set to block, the User Credential Submission permissions is automatically also set to block.	–	–	–	–	V
Continue	Displays a page to users that to warn them against continuing to access the page. To access the web site, the user must click **Continue**.	–	–	–	–	V
Override	Displays a response page that prompts the user to enter a valid password in order to gain access to the site. Configure URL Admin Override settings (**Device > Setup > Content ID**) to manage password and other override settings.	–	–	–	–	V

For more information about the different custom elements on each profile, please consult the contextual 

5.3.3.3 URL Filtering details

- If you want to find the category of a website, you can use this link : https://urlfiltering.paloaltonetworks.com/

  note: also accessible from the URL filtering configuration page



- The complete list the categories of the PAN-DB URL filtering: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm5hCAC

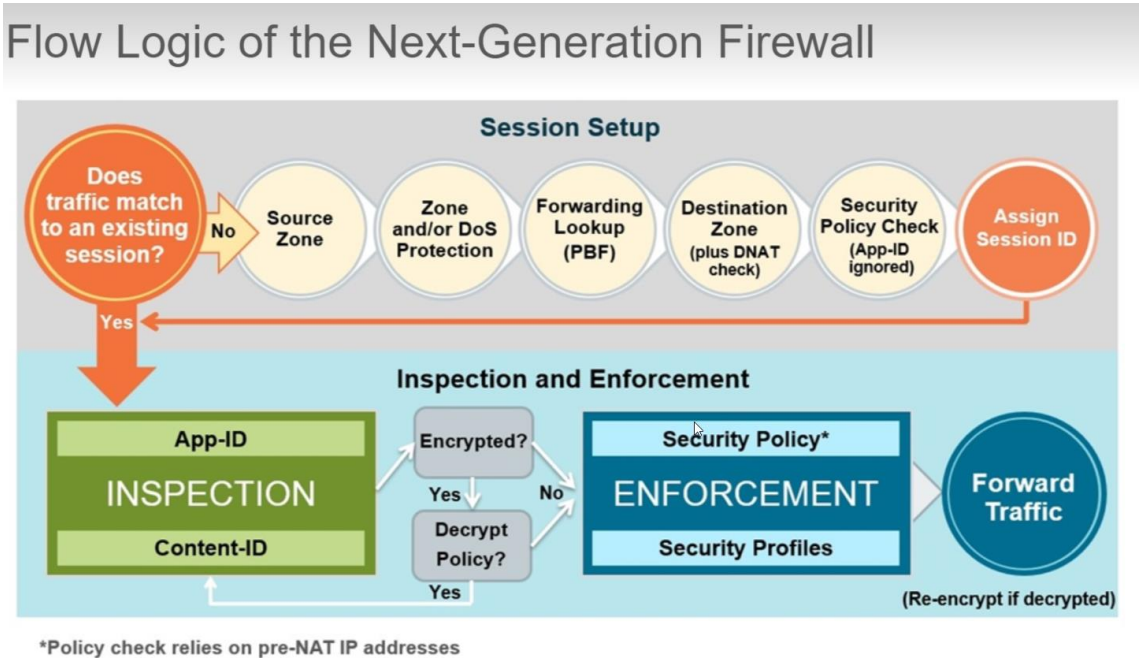
- More details about configuring URL filtering: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering

. For more information about the different custom elements on URL Filtering, please consult the contextual 

5.4 Configuration of a NAT Policy.

5.4.1 Palo Alto NAT implementation and theory

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/configure-nat

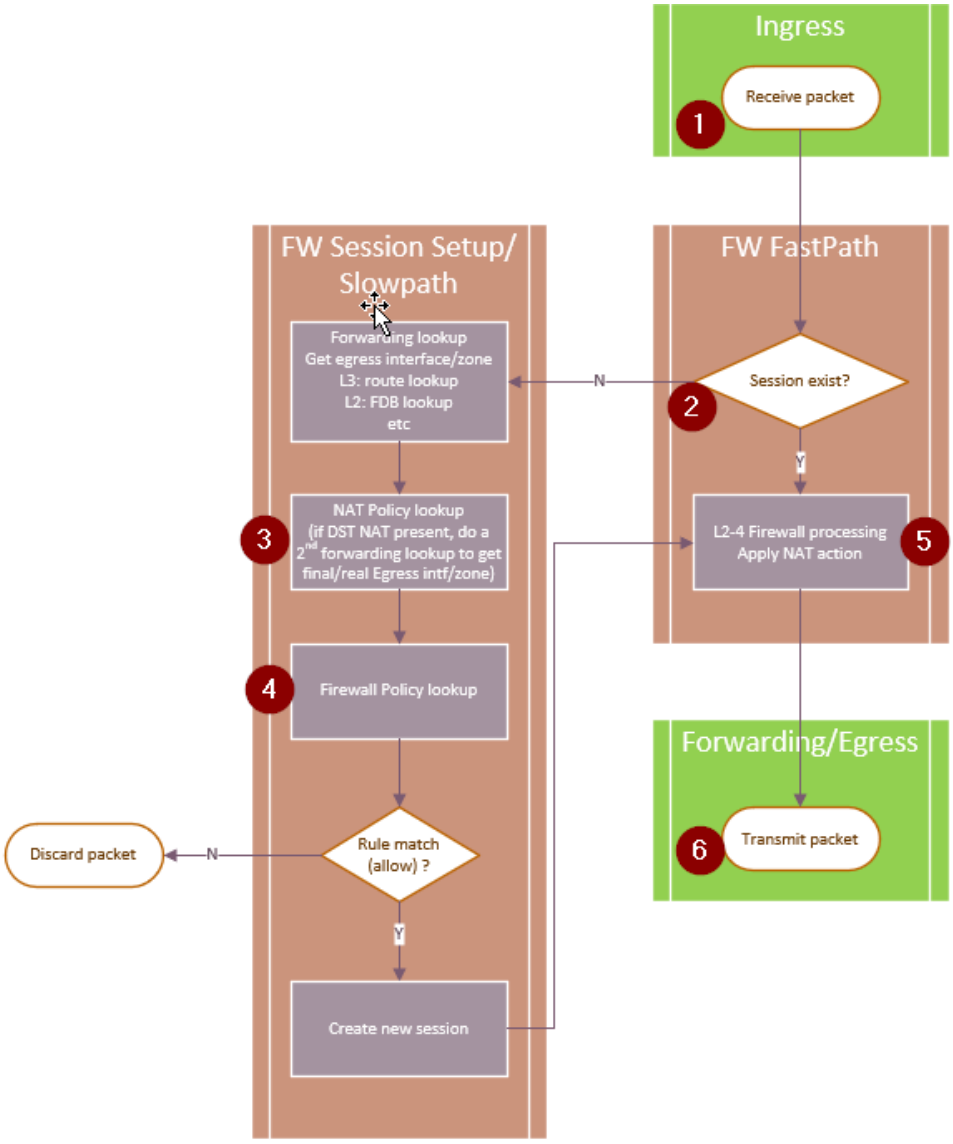


Network Address Translation is, in Palo Alto Firewalls, separated from the firewall filtering rules. Therefore, it is important to understand the firewall's flow logic to correctly define your Firewall policies to use NATIVE or NATted addresses…

NAT rules are based on source and destination zones, source and destination addresses, and application service (such as HTTP). Like security policies, NAT policy rules are compared against incoming traffic in sequence, and the first rule that matches the traffic is applied.

It is then important to organize your NAT rules from the more specific to the less specific, in order to correctly match the traffic.

Note: a default NAT rule is implemented by default by the Proximus templates in order to provide internet access by default. It is of type Dynaminc IP and Port, and matches RFC1918 ranges + FW INSIDE interface range (for testing purposes). This rule should be enough for most needs for what concerns internet access, but if you need something more specific, note that it will always be placed AFTER your own NAT rules, so basically it won't interfere with your own NAT implementations because your rules will always match the traffic first.



1 Packet enters the firewall
2 in case a session does not exist yet (generally the case for a new config)
3 NAT is inspected for route lookup, but NOT applied → this is important in the case of a static NAT entry! See TYPICAL STATIC NAT FROM INTERNET TO SERVERS example
4 the Firewall Policies are checked
5 NAT is applied to the packet
6 Packet is forwarded

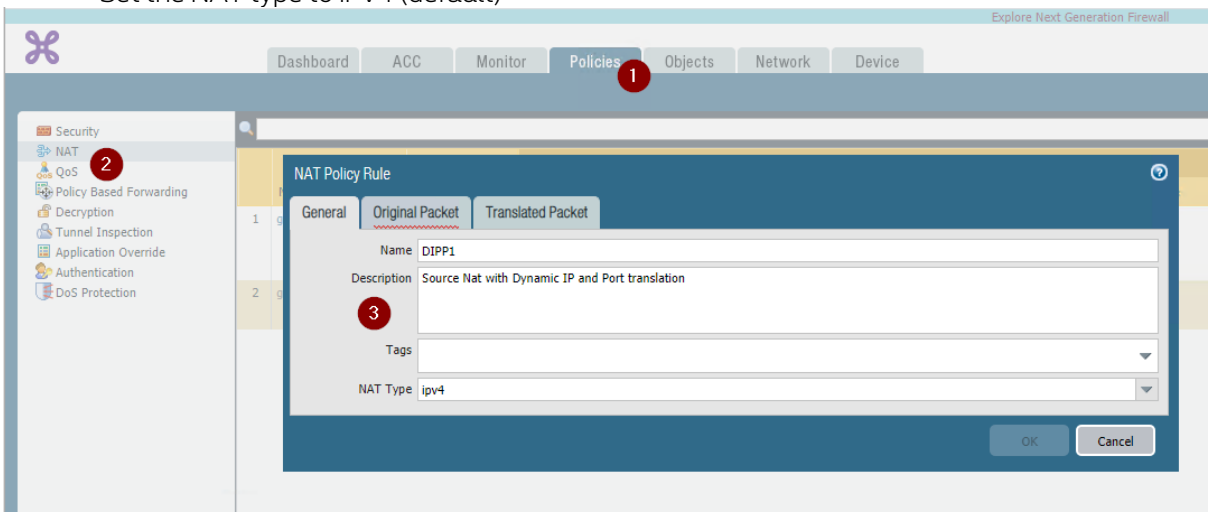
For a complete overview of the firewall's packet processing logic: Day Life of a Packet (Palo Alto KB) (scheme also available in hi-res)

5.4.2 Typical internet access rule (dipp/napt)

- Go to *Policies > NAT >* Add and create a new NAT policy.

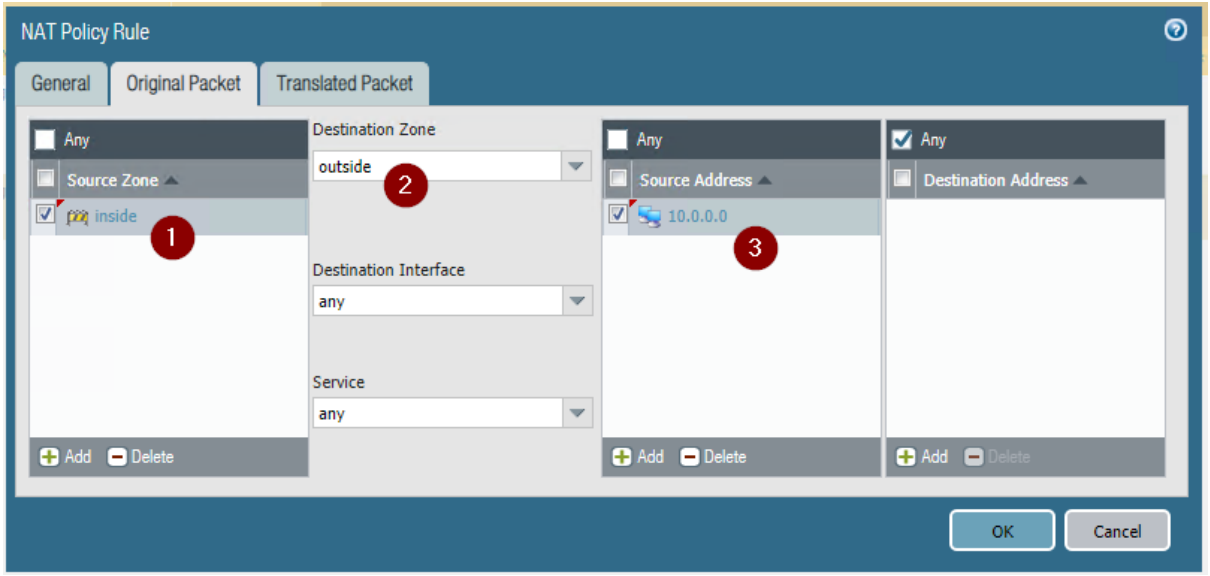
Inside the **General tab**, enter

- A unique name
- A description
- One or more tags
- Set the NAT type to IPv4 (default)



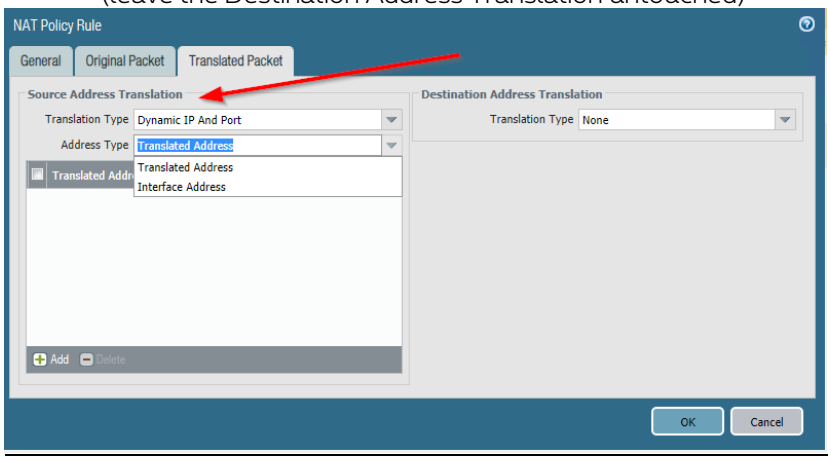
In the **Original Packet tab**, provide

- A source Zone (typically Inside)
- A Destination Zone (typically Outside)
- (optional) One or more source addresses (IP, subnet or pool) that will match the NAT rule



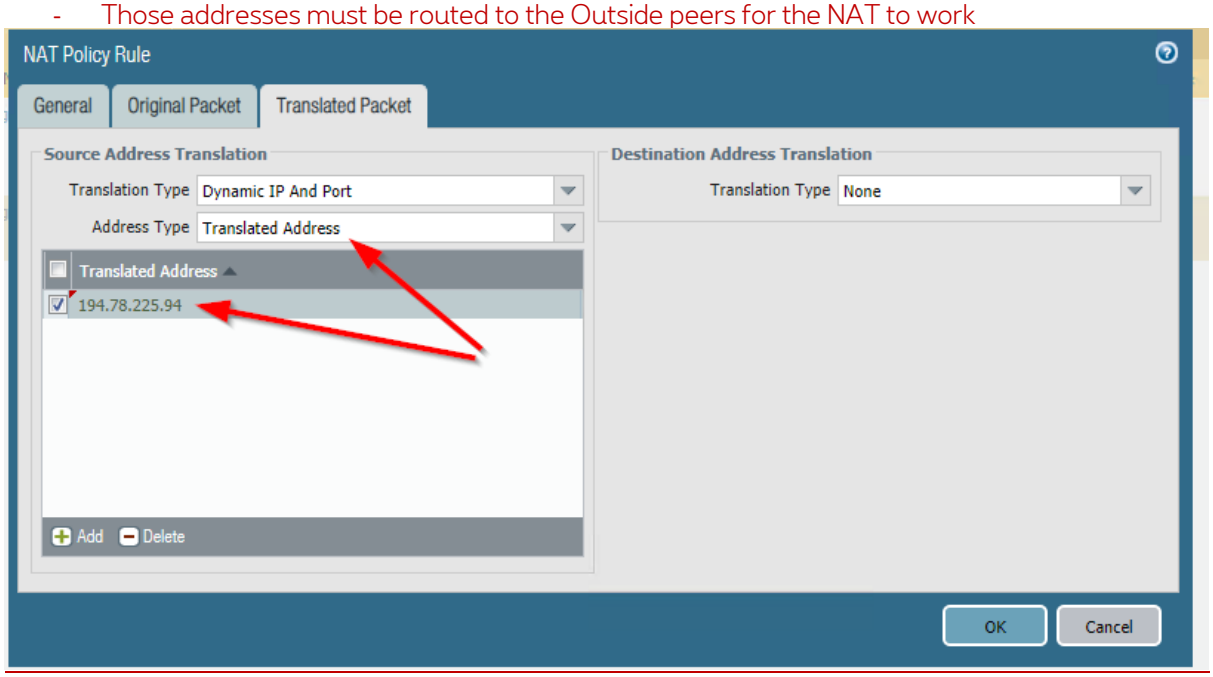
In the **Translated Packet tab**, provide

- The Source Address Translation type = **Dynamic IP and Port**.
- (leave the Destination Address Translation untouched)



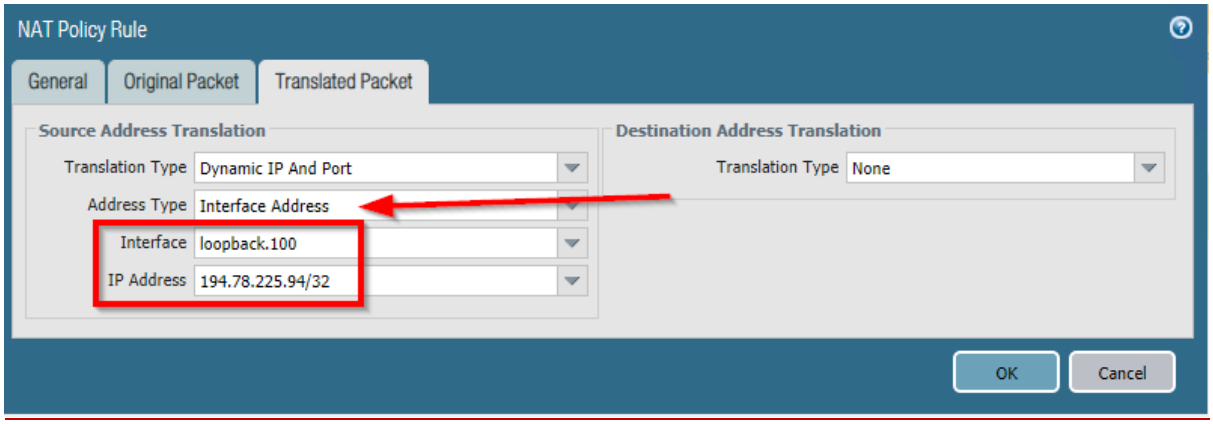
Type1: Translated Address : if using an **IPPack** address

- Add at least 1 IP address in the list, which can be and Address or Address group object created previously.
- Each entry in the list will be used by the NAT rule sequentially. See below more information about the NAT oversubscription
- Those addresses must be routed to the Outside peers for the NAT to work



Type2: Interface Address : if using the IPWAN address

- Only the loopback.100 can be used for NAT
- Do NOT use interfaces ethernet1/1 or ethernet1/2 as NAT address



Note: by default, the NAT oversubscription rate differs depending on the VM model. The NAT Oversubscription is the number of times that the same translated IP and port pair can be used concurrently.

Do not forget to Commit *your changes !*

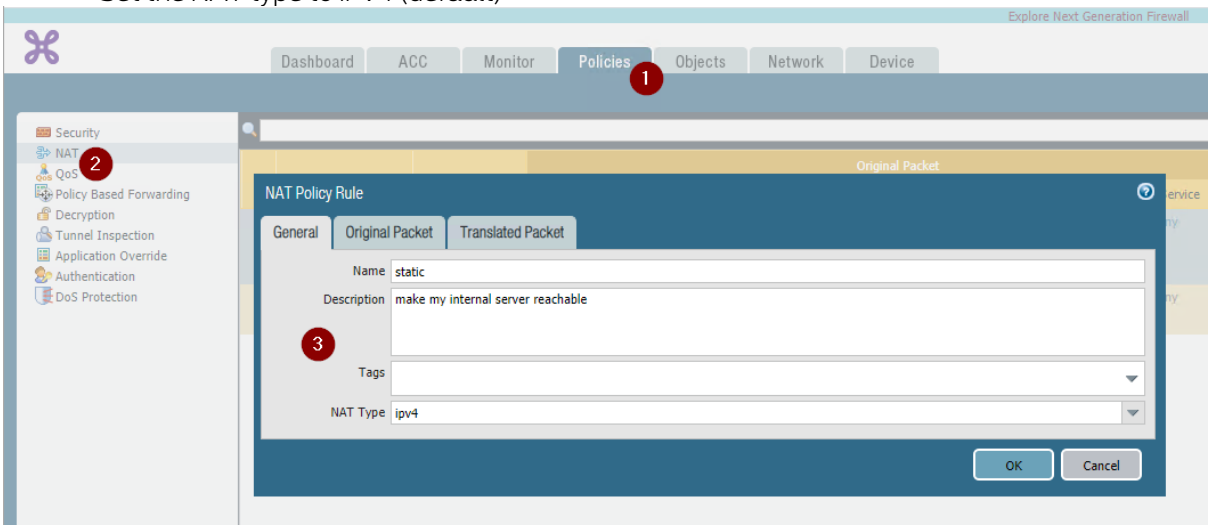
5.4.3 Typical static nat from internet to servers

Static NAT rules do not have precedence over other forms of NAT. Therefore, for static NAT to work, the static NAT rules must be above all other NAT rules in the list on the firewall.

- Go to *Policies > NAT >* Add and create a new NAT policy.

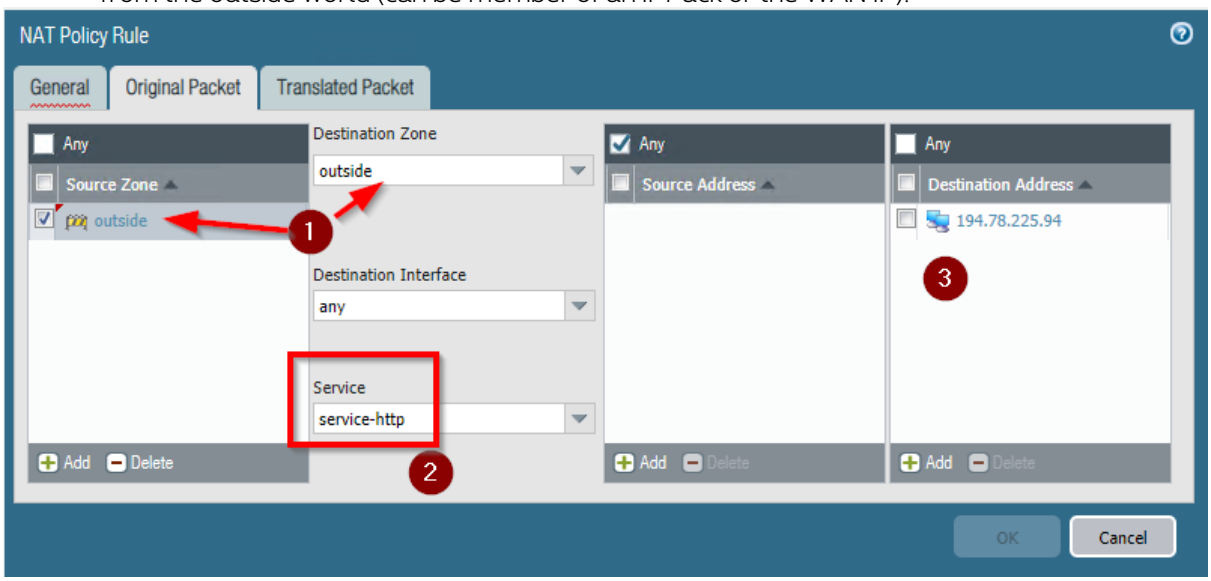
Inside the **General tab**, enter

- A unique name
- A description
- One or more tags
- Set the NAT type to IPv4 (default)



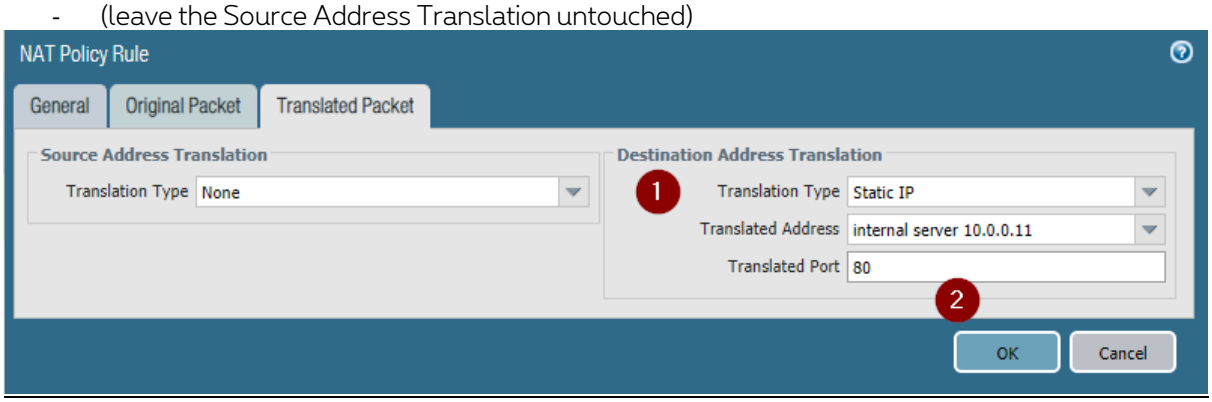
In the **Original Packet tab**, provide

1. The same Source Zone and Destination Zone (typically Outside)
2. The Internet service of your server, otherwise ALL incoming connections will be translated.
3. The Internet address of your server. This is the public address used to reach your server from the outside world (can be member of an IPPack or the WAN IP).



In the **Translated Packet tab**, provide

- The Destination Address Translation type = **Static IP**
- (optional) specify a port or a range or ports. If no port is specified, the original port will be used.
- (leave the Source Address Translation untouched)



Note: your Firewall policy rules will apply to the **real destination zone**, but as destination the **Public IP address** (and port, if translated) of the server, not the internal IP. Review PALO ALTO NAT IMPLEMENTATION AND THEORY for more explanations on the reasons.

Example:

	Name	Source		Destination		Application	Action
		Zone	Address	Zone	Address		
10	access to my server	outside	any	insid...	194.78.225.94	web-browsing	Allow

Do not forget to Commit *your changes*

6. Teleworking (Global Protect)

Customer subscribing to this service can provide a remote access to theirs users. The service is proposed with 2 flavors: **Local Authentication** and **Authentication using Active Directory Services**

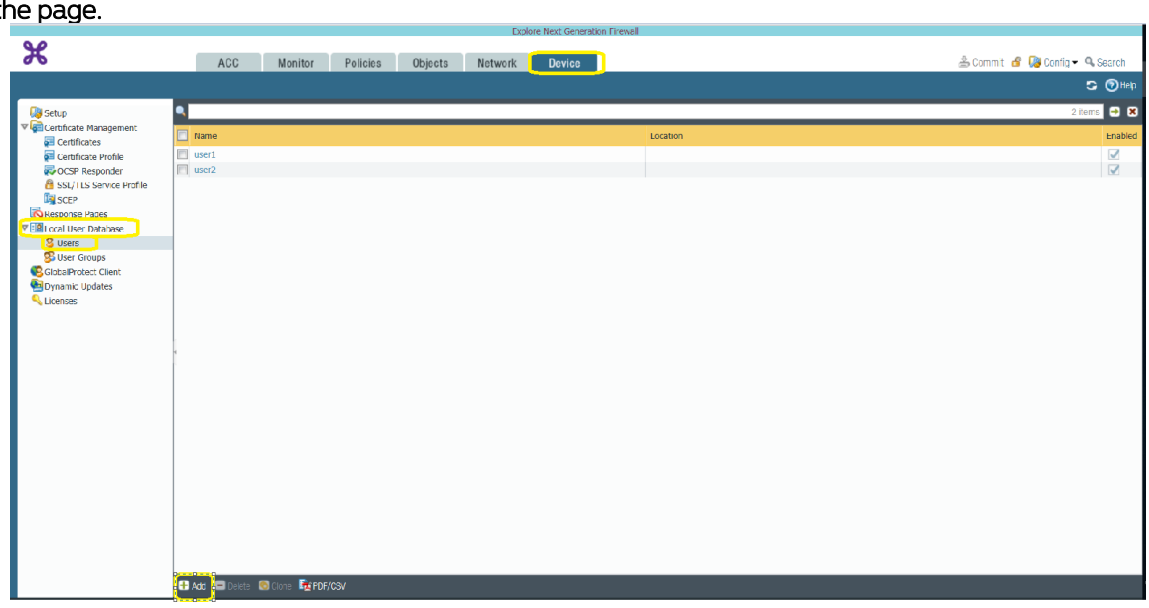
The **Local Authentication** is sold per pack of 5 consecutive users, which usernames and passwords must be configured in the firewall for authentication.

The **Active Directory** relies on AD (LDAP) configuration between the firewall and the AD server of the customer in order to allow access to the Teleworking service. There is no limit in consecutive users in this case. This flavour is not part of the self-managed package and must be configured with the help of an Explore engineer.

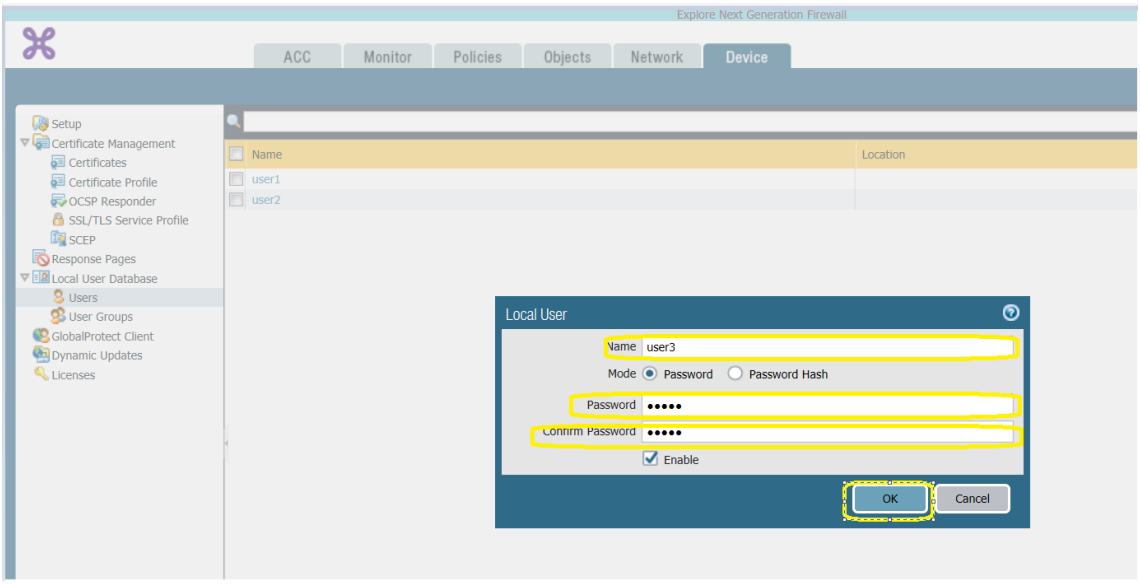
6.1 How to define users and passwords on the NGFW

STEP 1: add users

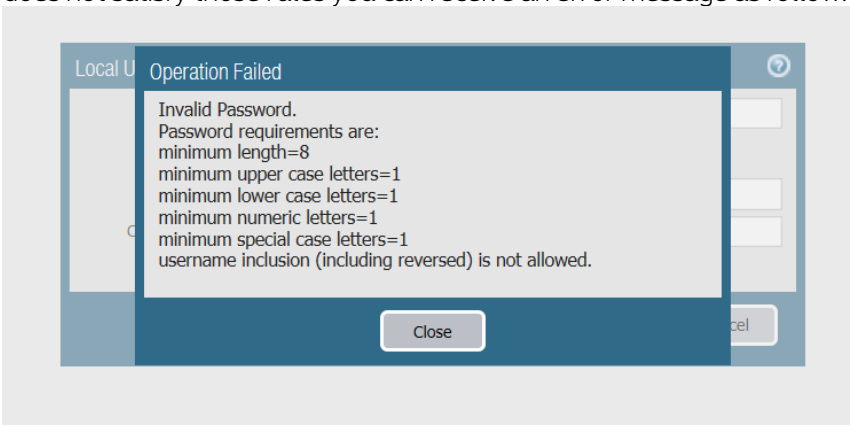
- Select Device > Local user Database > Users. And then select the Add or Clone in the bottom of the page.



- Give a name to the user and click OK



Note: Proximus enforce certain rules for password definition. If your password does not satisfy those rules you can receive an error message as follow:

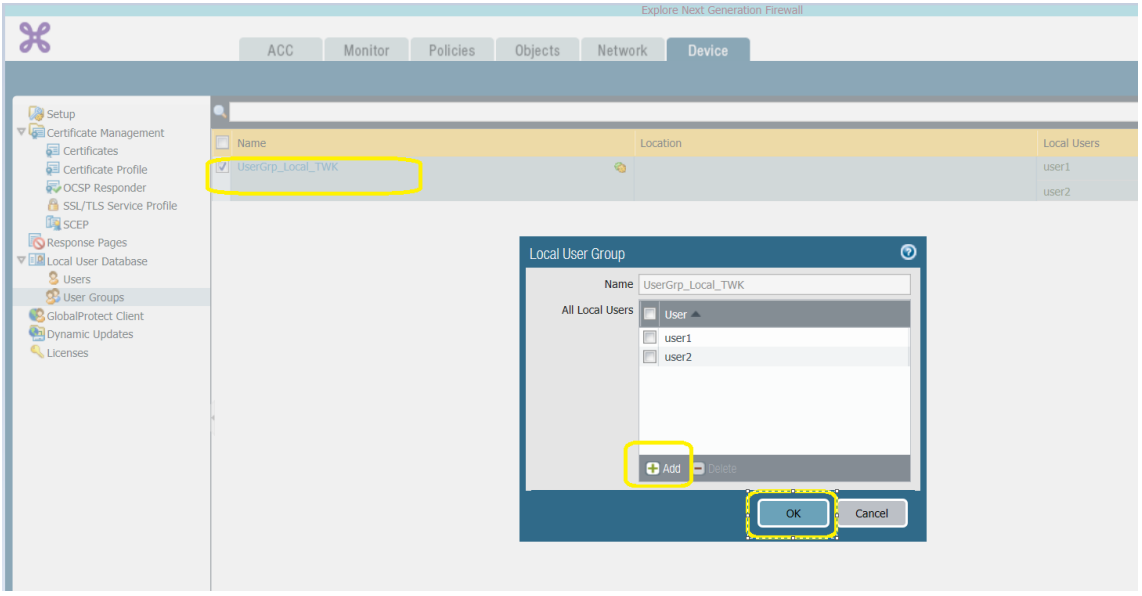


- Add other users as needed.

  You can configure as many users as needed but remember that the amount of consecutive connections depends on your subscription at Proximus (packs of 5).

STEP 2: add the users to the predefined group

- Select **Device > Local user Database > User Groups**. There is already a predefined group in which the customer needs to add their users: **UserGrp_Local_TWK**



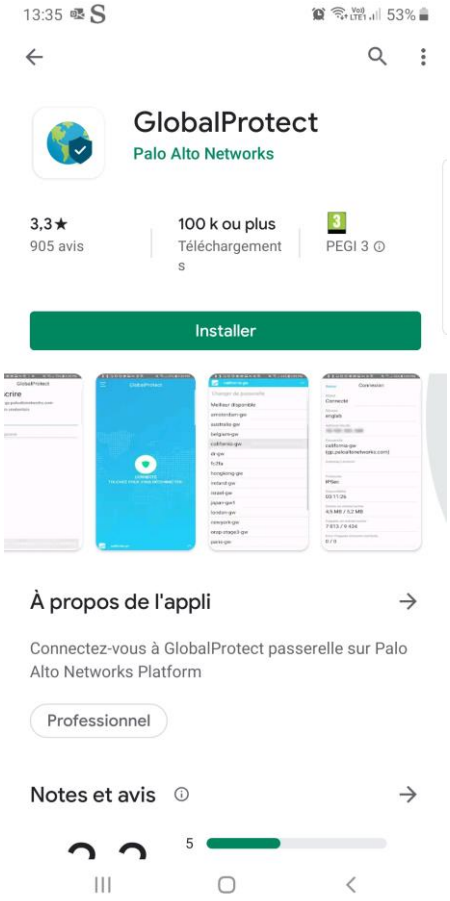
STEP 3: commit your changes

6.2 Installation of the client software

Global Protect requires a client software to be installed in order to establish the connectivity the firewall. This must be achieved once for every device (and requires administrative rights to do so). There are several ways to install the software, depending on the Operating System you will be using.

Android, (Apple) IOS or Windows Mobile: you must download the app from the corresponding app store.

Example with Android



Windows & MAC: you may connect to the firewall portal to download the app. Follow below instructions:

- **Launch a web browser and connect to the portal.**
  The URL to use for the first connection into the portal will be provided by Proximus if you subscribed to this service. The format is https://<cust_shortname>..teleworking.proximus.com (replace <cust_shortname> by the name provided for your Explore contract).

  Note : The supported browsers could be found on the following link.

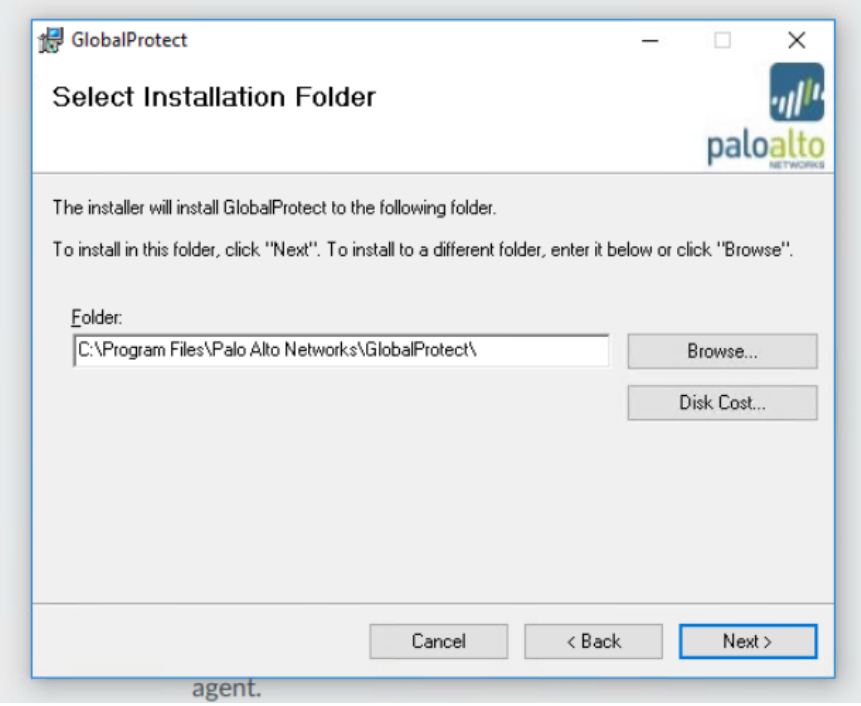
  https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/globalprotect-clientless-vpn/supported-technologies#

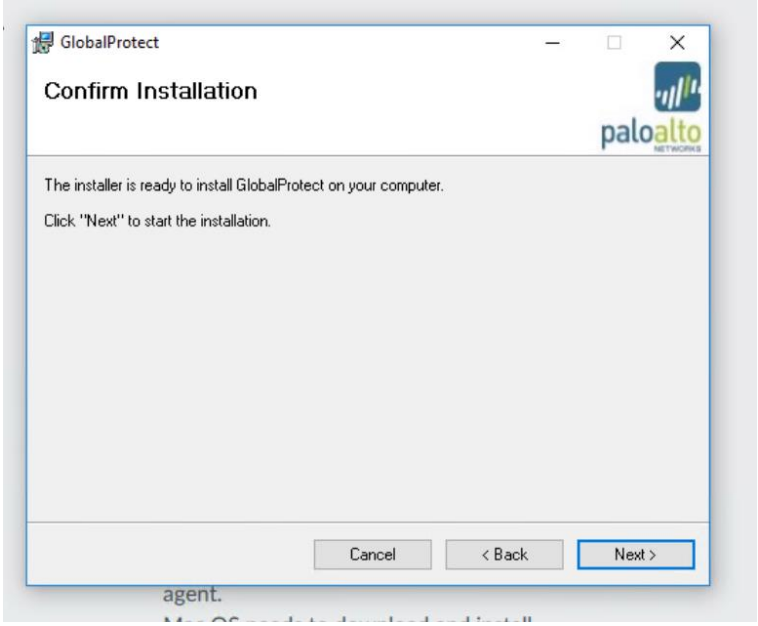
  - On the portal login page, enter your username and password and then click **LOG IN**.

  - After the authentication of the user, it will be asked to download and install the Global Protect agent. (Windows and MAC).

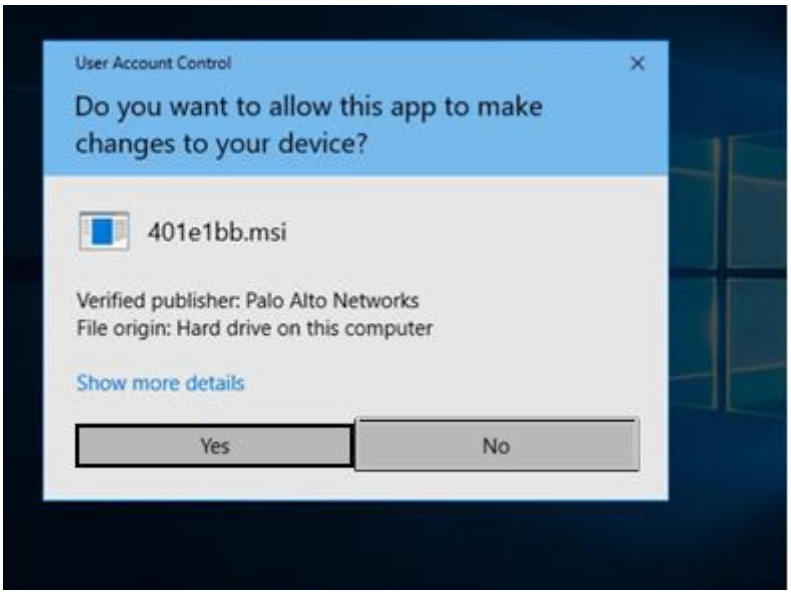
    To begin the download, click the software link that corresponds to the operating system running on your computer. If you are not sure whether the operating system is 32-bit or 64-bit, ask your system administrator before you proceed.

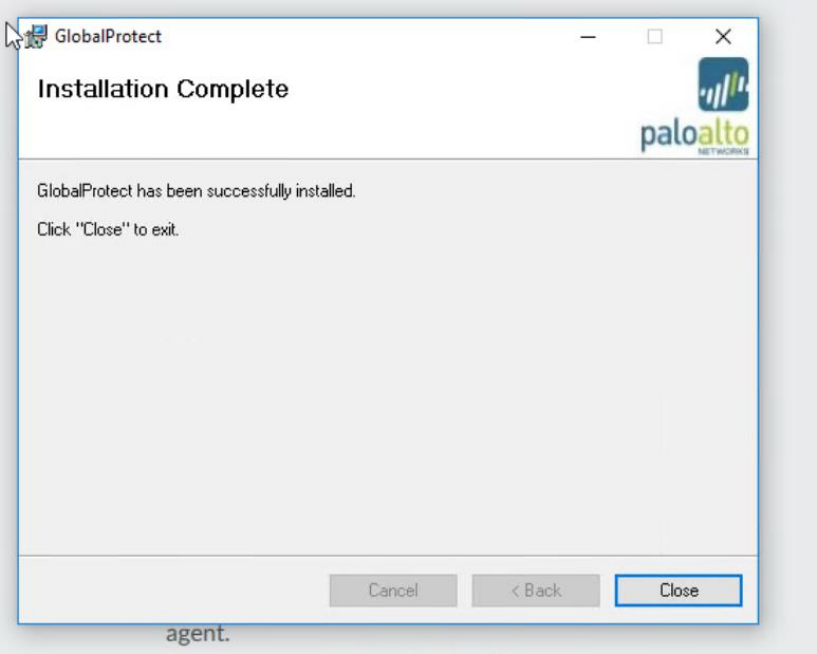
- Follow the following steps for the installation of the agent.
    - Open the software installation file.
    - When prompted, Run the software.
    - When prompted again, Run the GlobalProtect Setup Wizard.





- Allow the application changes to your device. Administrator privileges are required to install the Global Protect client for the first time.

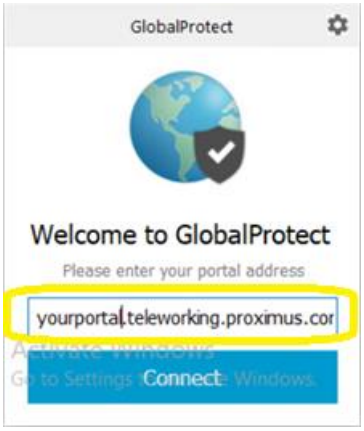




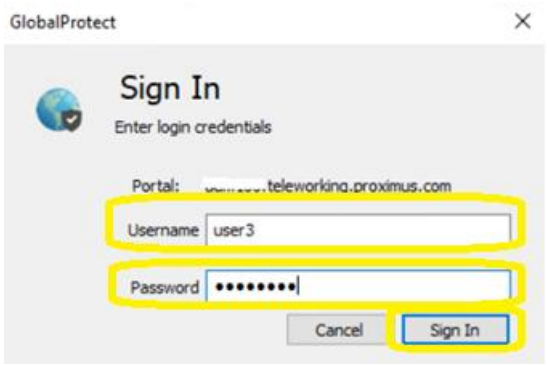
- After the installation of the agent, close the wizard.
  you will be able to launch the agent and to connect to the gateway.

6.3 First connection for a Teleworker

- Launch the Global Protect Agent
  Enter the the link to your teleworking portal as provided by Proximus.
  (e.g. https://yourportal.teleworking.proximus.com/ where 'yourportal' is replaced by your company's portal name).

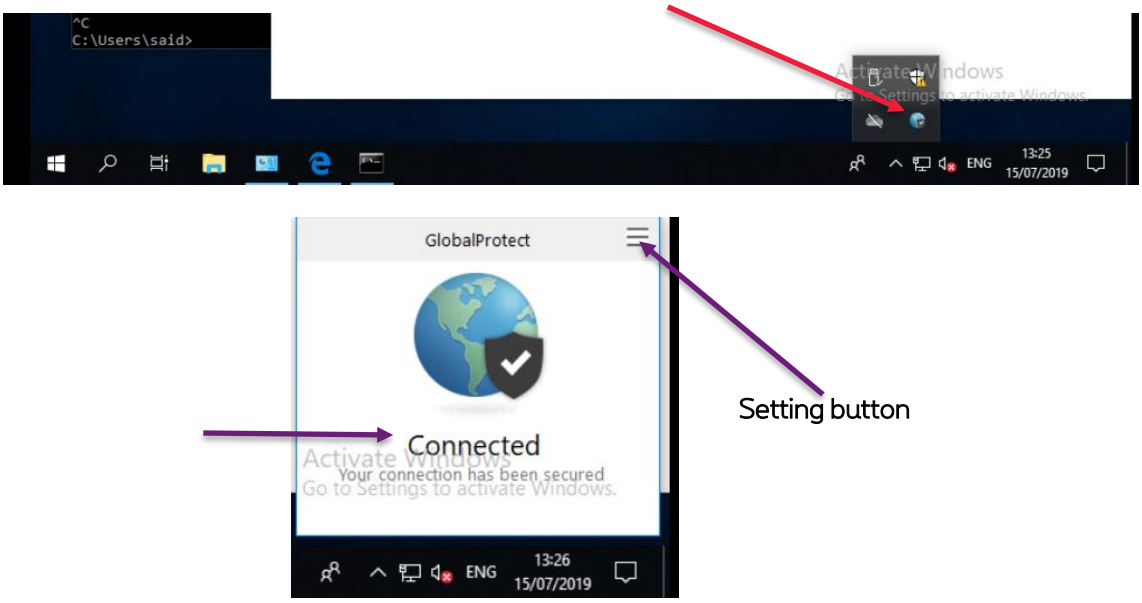


Enter your username and password. (provided by your administrator)
And then click connect to initiate the connection.

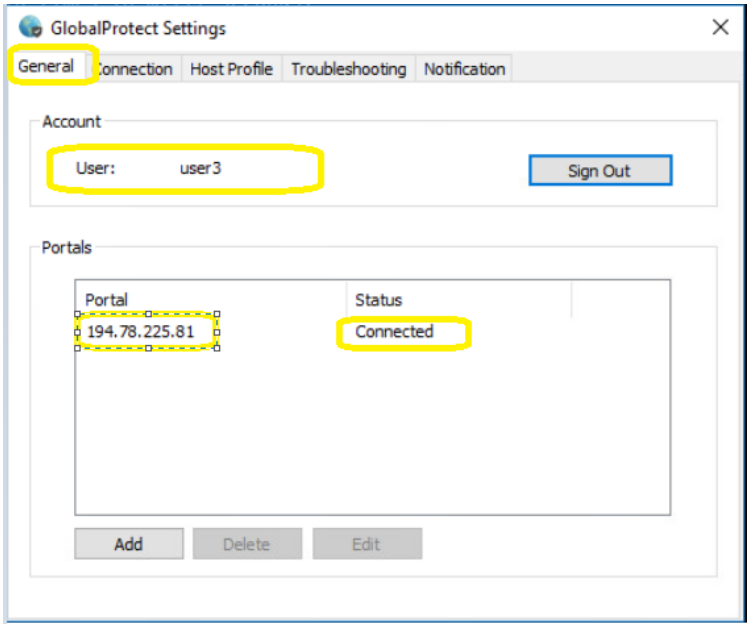


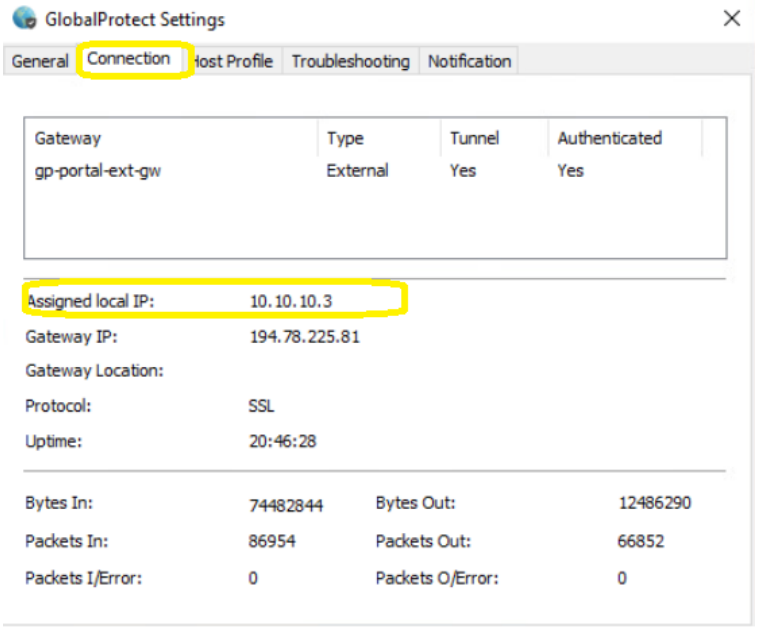
If authentication is successful, you are connected to your corporate network, and the status panel displays the Connected or Connected - Internal status. If your administrator sets up a Global Protect welcome page, it displays after you log in successfully.

To check your connectivity status, click on the Global Protect icon of your laptop and see if the status is set to “connected”.



You can also verify the configuration of the client agent by clicking on the setting button.





Important! you shall verify the firewall policies between the Teleworking Zone and both the Inside and Outside zones to make sure all required accesses are allowed.

7. Want to know more?

7.1 Palo Alto useful websites

https://knowledgebase.paloaltonetworks.com/ contains a lot of useful information about specific configuration needs. Just enter the keywords and look for a solution, you'll certainly find it!

https://eu.wildfire.paloaltonetworks.com/wildfire/dashboard gives an overview of Wildfire activity all over Europe (remove leading "eu." From the URL for a worldwide version), check other firewalls file subscriptions (or yours, based on Serial#).

https://live.paloaltonetworks.com/ a community for all Palo Alto users.

7.2 Palo Alto trainings

Though your firewall has been mostly pre-configured by Proximus, you might want to know more about such device for the self-management part. There is of course no obligation to follow these trainings advises.

In order to access the trainings, you must have a valid account to Palo Alto's education website https://www.paloaltonetworks.com/services/education

As Proximus service provider, we can advise you to some specific e-learning modules that will **focus** on the **self-management activites** you would be required to do.

Remember that your firewall is not a genuine Palo Alto device anymore, so certain features might not be available or look the same way as described in the training. Note also that we run today version 8.1.7 of PanOS.

Training 1: FIREWALL 8.1 ESSENTIALS: CONFIGURATION AND MANAGEMENT (EDU-110) E-LEARNING
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/edu-110-8x-datasheet.pdf

Modules to follow:

- Next Generation Security Practices
- WildFire
- User-ID
- **Security and NAT policies**
- **App-ID**
- Content-ID
- **Monitoring and Reporting**
- URL Filtering

Training 2: FIREWALL 8.1: OPTIMIZING FIREWALL THREAT PREVENTION (EDU-114) E-LEARNING

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/edu-114-8x-datasheet.pdf

Modules to follow:

- Module 1: The Cyber-Attack Lifecycle
- Module 2: Blocking Packet and Protocol-based Attacks
- Module 3: Blocking Threats from Known-Bad sources
- **Module 4: Blocking Threats Using App-ID**
- Module 5: Blocking Threats Using Custom Applications
- **Module 8: Blocking Threats in Allowed Traffic**
- **Module 11: Viewing Threat and Traffic Information**

8. Glossary

App-id	Palo Alto function that permits to recognize applications based on signature (database)
Wildfire	Palo Alto security feature requiring a specific license. Wildfire is a sandbox system that permits to identify zero-day threats by the mean of several investigation techniques available in the cloud
GlobalProtect	Palo Alto solution for remote access (Teleworking).