

PAN-OS 4.1

Markus Laaksonen

mlaaksonen@paloaltonetworks.com



the network security company™

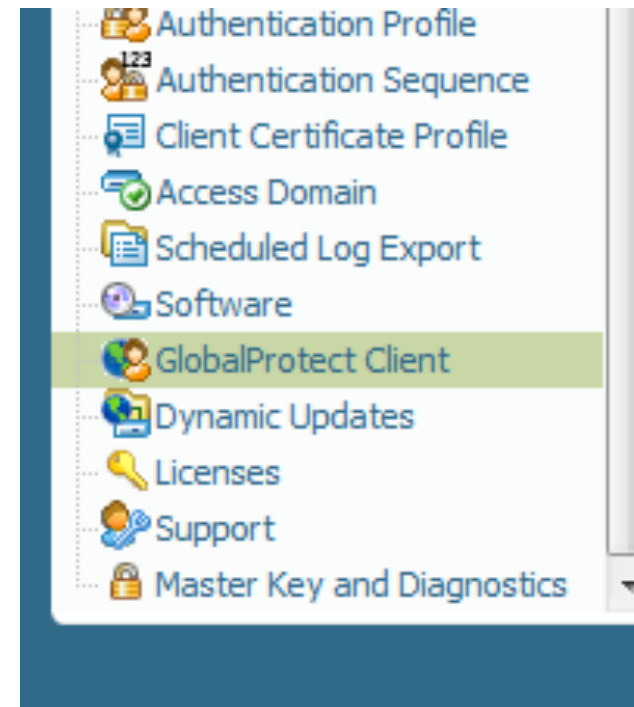
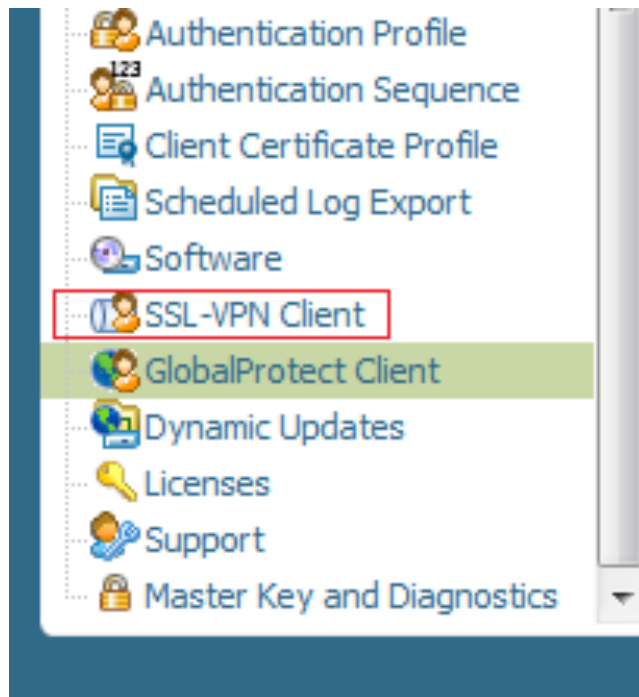
4.1 Feature Summary

- App-ID, User-ID, Content-ID
 - URL category in policy match
 - H.323 NAT/PAT support
 - User-ID redesign
 - *Global Catalog, Direct group mapping, consolidated agent, more*
 - User-ID agent Exchange support
 - Vulnerability and anti-spyware profile refinement
- Networking
 - Multicast routing (IGMP, PIM-SM, PIM-SSM)
 - DHCP client
 - DNS setting propagation
 - NAT in Virtual Wire
- GlobalProtect
 - Gateway/agent unification
 - User group-based client configuration
 - Gateway priority included in closest gateway selection
 - Advanced/basic client view
 - Mac OS support (full support)
 - Apple iOS support (manual connect)
 - Customizable response pages
- Management
 - XML API enhancements, including most operational commands, API browser
 - SSH key-based auth
 - Independent device/network/shared object commit
 - Netflow v9 (all but PA-4000 series)
 - Customizable branding on web interface

GlobalProtect features

Unification of NC and GP

- In 4.1, the feature set of NetConnect has been integrated into GlobalProtect. GlobalProtect in its base functionality now replaces NetConnect.

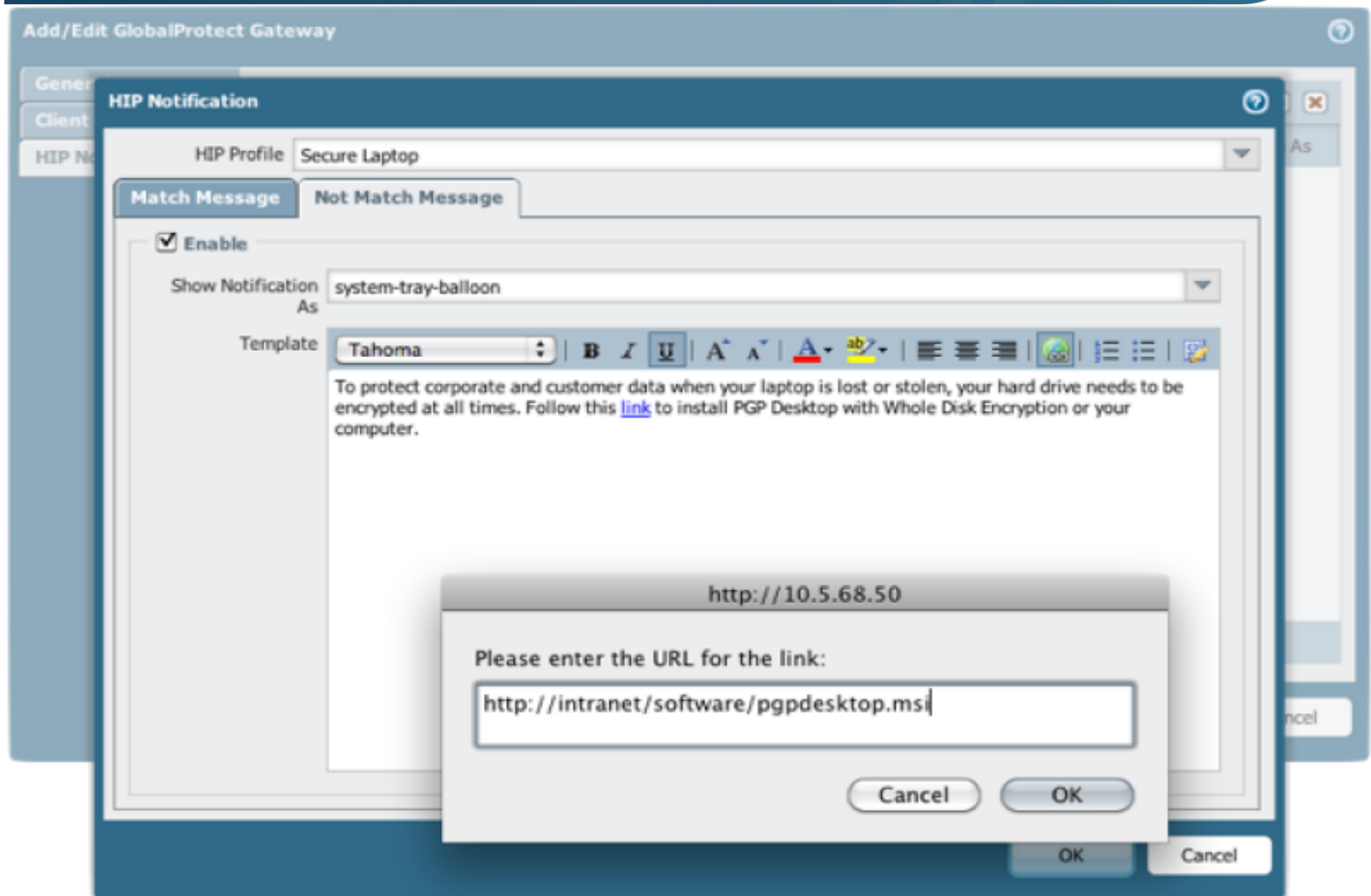


Unification of NC and GP (cont'd)

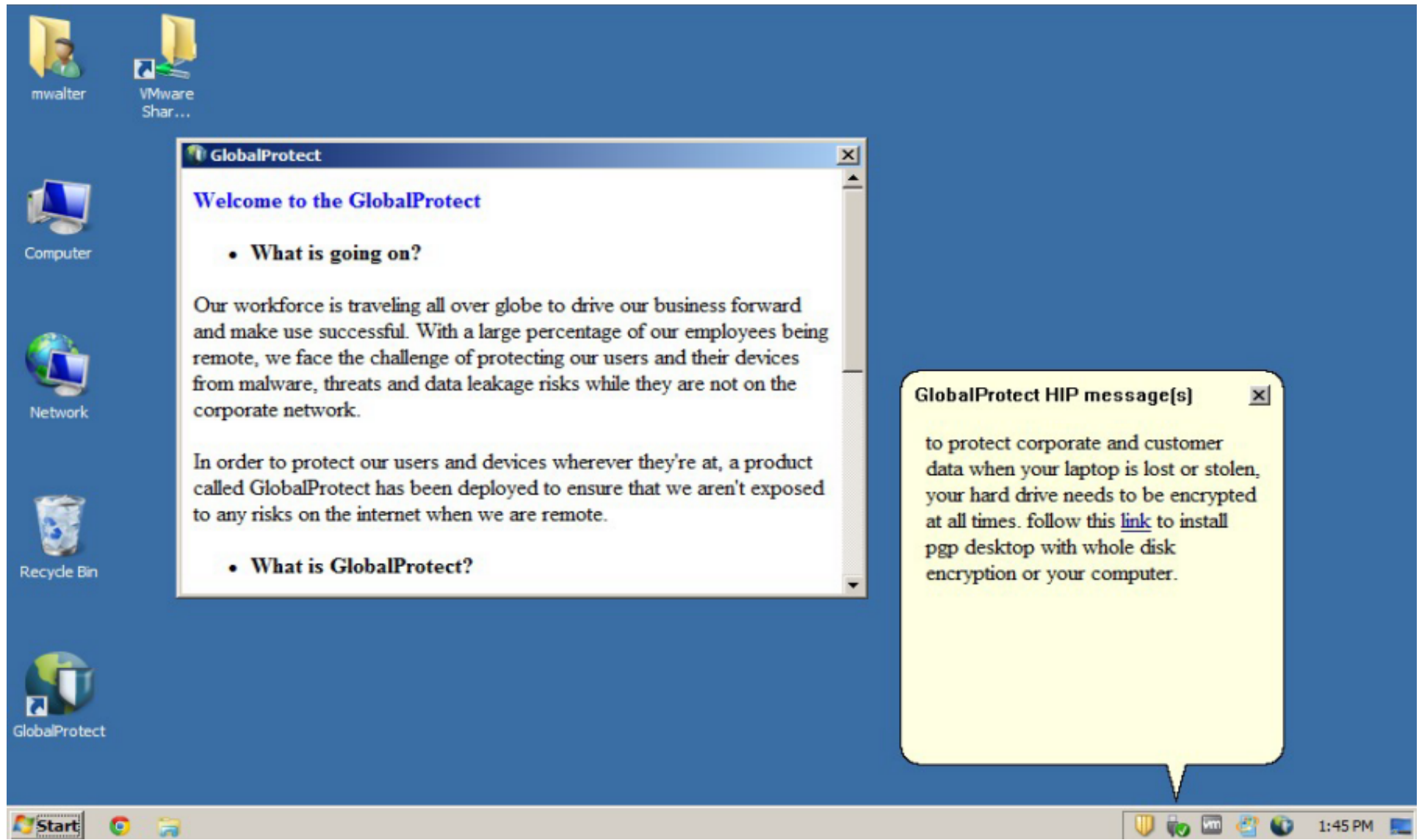
- The advanced functionalities of GlobalProtect, such as Host Information Profiles as well as multi-gateway support remain licensed features while single gateway configurations with no HIP capability will be available without a license.

	GlobalProtect base	GlobalProtect subscription
Multiple gateways	no	yes
HIP Check	no	yes
User override control	yes	yes
SSO	yes	yes
Transparent connection	yes	yes
Third party VPN	yes	yes

Response page enhancements (cont'd)



Response page enhancements (cont'd)



iOS Support & Mac OS X Support



the network security company™

Iphone

Annuler Nouv. config. Enregistrer

L2TP PPTP **IPSec**

CISCO

Description GP GW

Serveur banez.hd.free.fr

Compte cv

Mot de passe ●●●●●●●●●●

Utiliser le certificat ☐

Nom du groupe iphone-group

Secret ●●●●●●●●●●

Configuration

Réseau **VPN**

VPN ☐

Choisissez une configuration...

✓ GP GW
Personnalisé

Ajouter une configuration VPN... >

Activation

SFR 3G **VPN** 23:34 93%

VPN **État**

Serveur banez.hd.free.fr

Temps de connexion 2:11

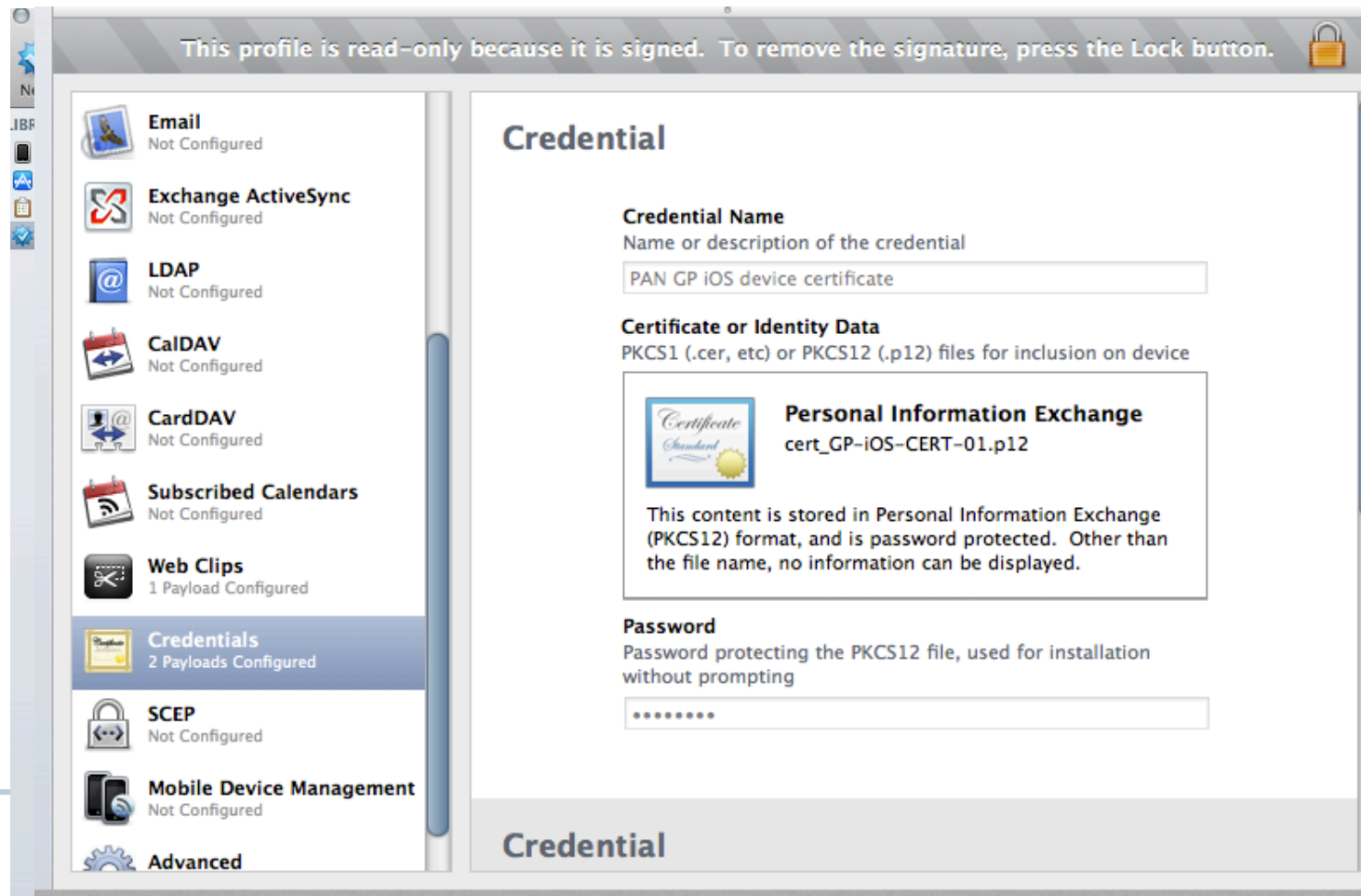
Connecté à 78.241.252.234

Adresse IP 192.168.0.81

Connected !

Iphone Configuration Utility

- Iphone Configuration Utility helps you in:
 - *Quick Deployment*
 - *Deploy even with non-technical users*
 - *The tool generate a file to send to all users to configure all Iphone settings.*



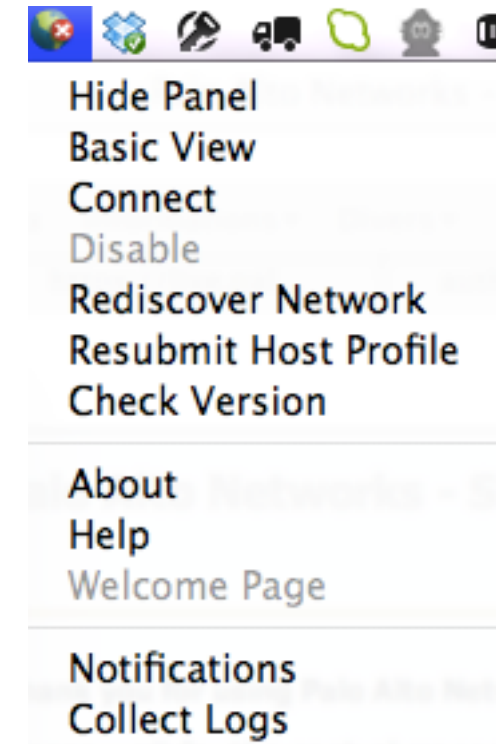
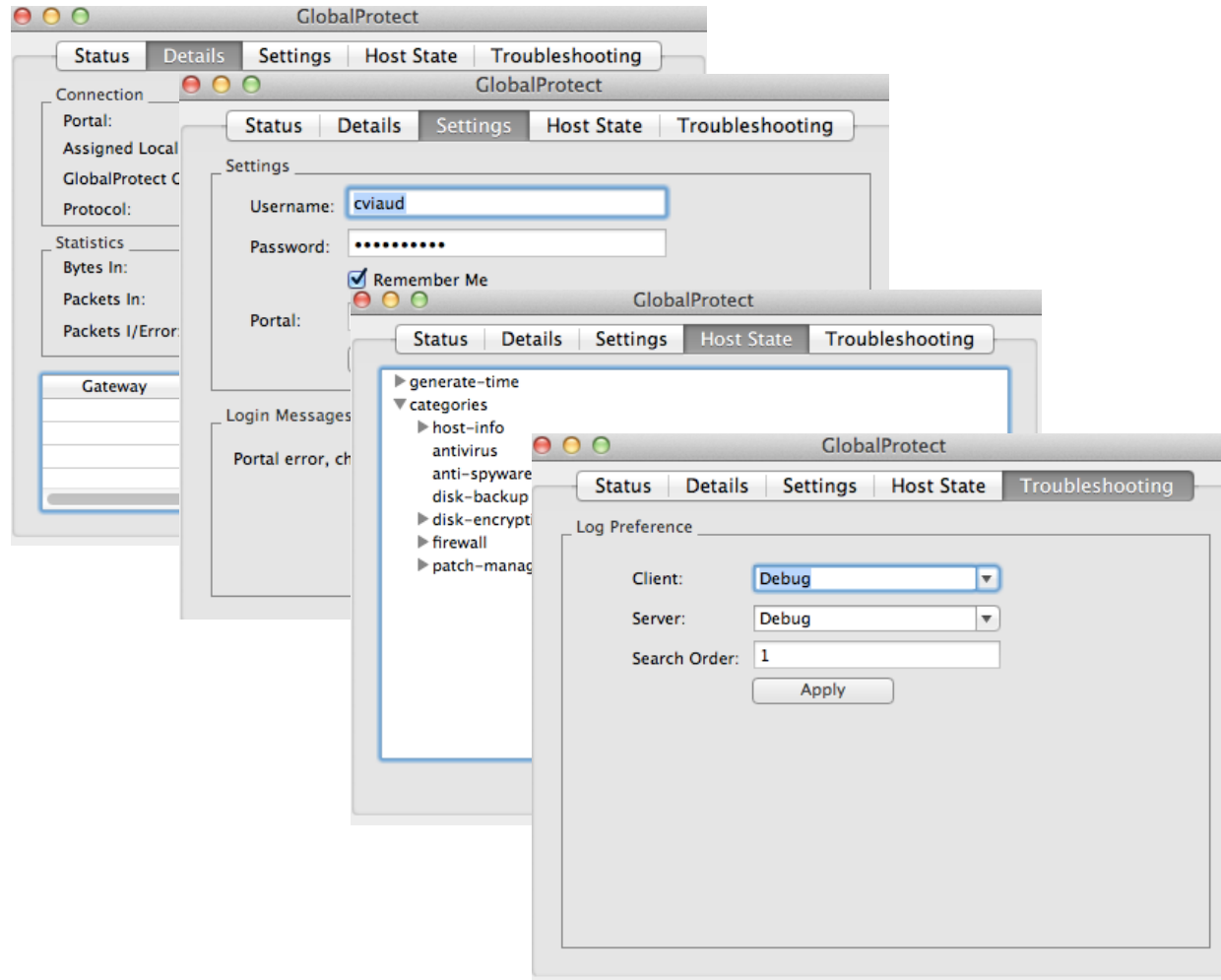
GlobalProtect Mac OS X Support



the network security company™

GlobalProtect Agent

- Same agent as windows



3rd party VPN client with Xauth

- Linux, Android, Windows phone etc.

État : Non connecté

Adresse du serveur : banez.hd.free.fr

Nom du compte : cv

Mot de passe :

Réglages d'authentification...

Se connecter

☒ Afficher l'état VPN dans la barre des menus

Avancé... ?

Auth. des machines :

☒ Secret partagé :

☐ Certificat Choisir...

Nom du groupe : iphone-group

Annuler OK

4.1 Management



the network security company™

UI and Log DB Optimization

- **Web Interface Updates**
 - Performance optimization
 - Completed Web UI update started in 4.0
- **Log Database Enhancements**
 - Performance optimization
 - Scalability enhancements



**Better than he was before.
Better...stronger...faster**

Modern Malware - WildFire

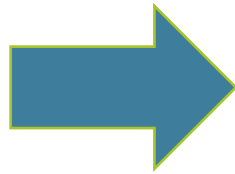


the network security company™

Hackers have changed



From bored “geeks”



To nation states and organized crime

Some recent examples...



epsilon



The 5 steps of modern malware



bait the
end user



exploit



download



back
channel



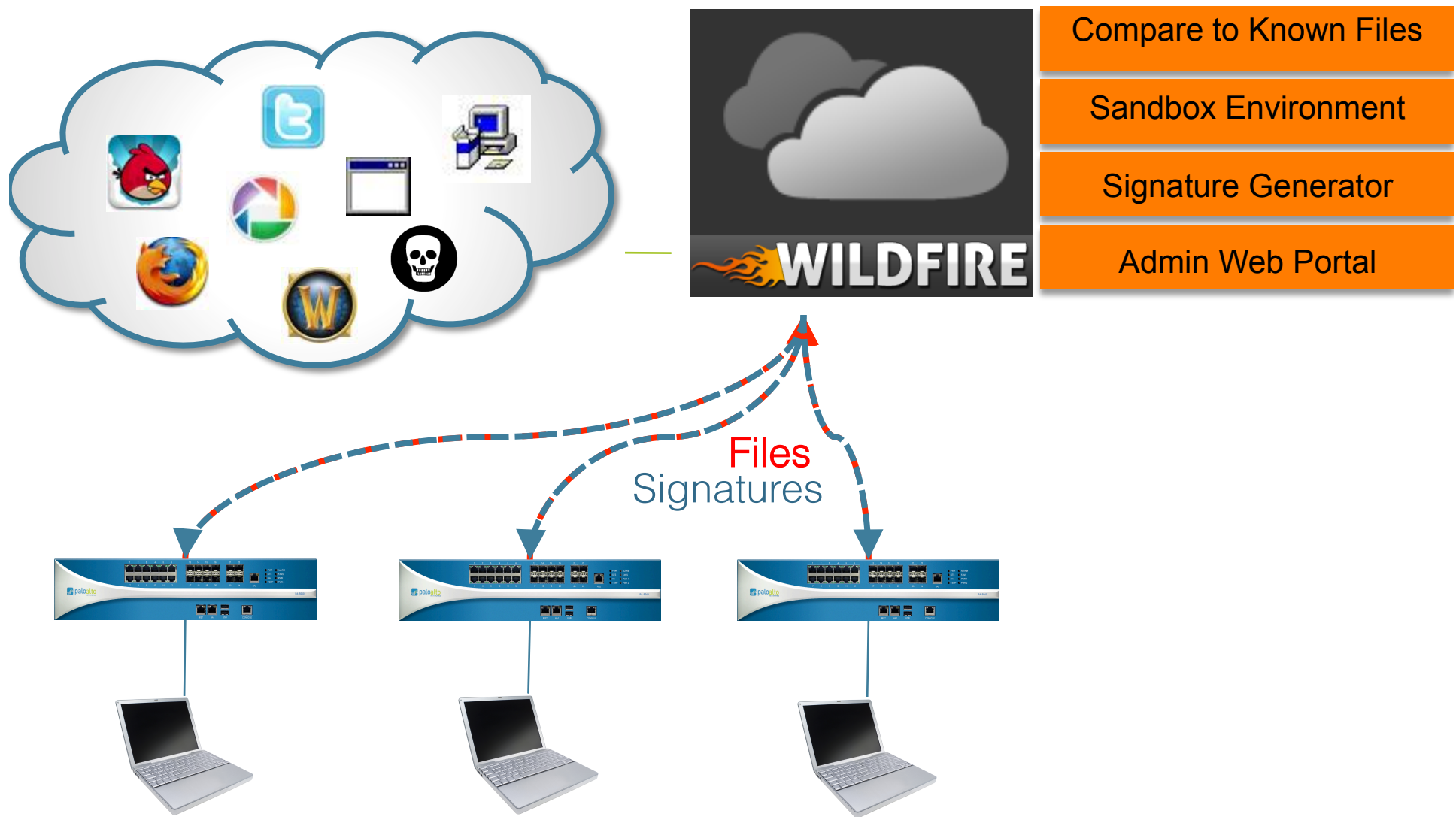
steal

Introducing WildFire

- Identifies unknown malware by direct observation in a cloud-based, virtual sandbox
 - Detects more than 70 malicious behaviors
 - Capture and enforcement performed locally by firewall
 - Sandbox analysis performed in the cloud removes need for new hardware and provides single point of malware visibility
- Automatically generates signatures for identified malware
 - Infecting files and command-and-control
 - Distributes signatures to all firewalls via regular threat updates
- Provides forensics and insight into malware behavior
 - Actions on the target machine
 - Applications, users and URLs involved with the malware



Wildfire Architecture



WildFire Overview/Timing

Available Today

- Malware sandbox
 - Windows XP environment
 - Executable files run and analyzed
- Hosted service in US, Europe (UK), Japan, and Asia (Singapore)
- Signatures delivered via regular AV update process
- Reporting via cloud portal

Future

- Increased OS and application support in virtual environment
- New WildFire subscription service
 - Integrated logging and reporting of WildFire scan results
 - Rapid signature coverage
 - ALL WildFire subscribers will receive rapid signatures for ALL found malware files

WildFire Pricing

- **WildFire Today**

- In 4.1 all WildFire features are available for free.
- Features that are available for free today will continue to be free in the future.

- **Threat Prevention Subscription**

- Malware signatures are still require a Threat Prevention subscription today and in the future.

- **Future WildFire Subscription**

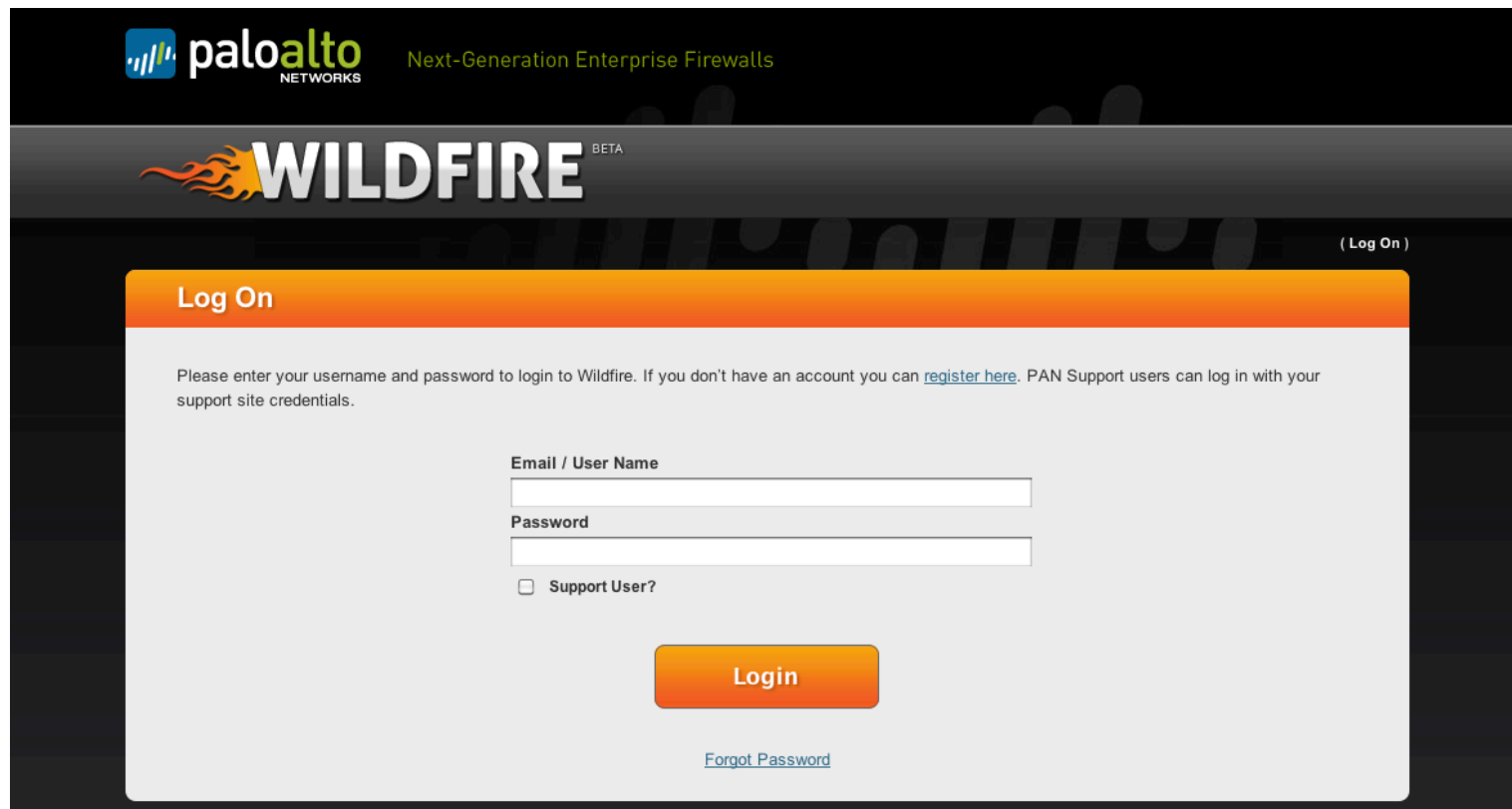
- Future features of WildFire including faster signature delivery and tighter integration with the firewall will require a WildFire subscription.

Interesting Stats From the Beta

- WildFire received more than 35,387 submissions, and more than 7% was found to be malware.
- Of this malware, 57% had no coverage by any AV vendor or had not been seen by Virus Total at the time of discovery
- Hotfile and AIM-Mail had very high rates of targeted with malware outnumbering clean files by 10:1
- 15% of newly discovered malware was found to generate unknown traffic

Wildfire Portal

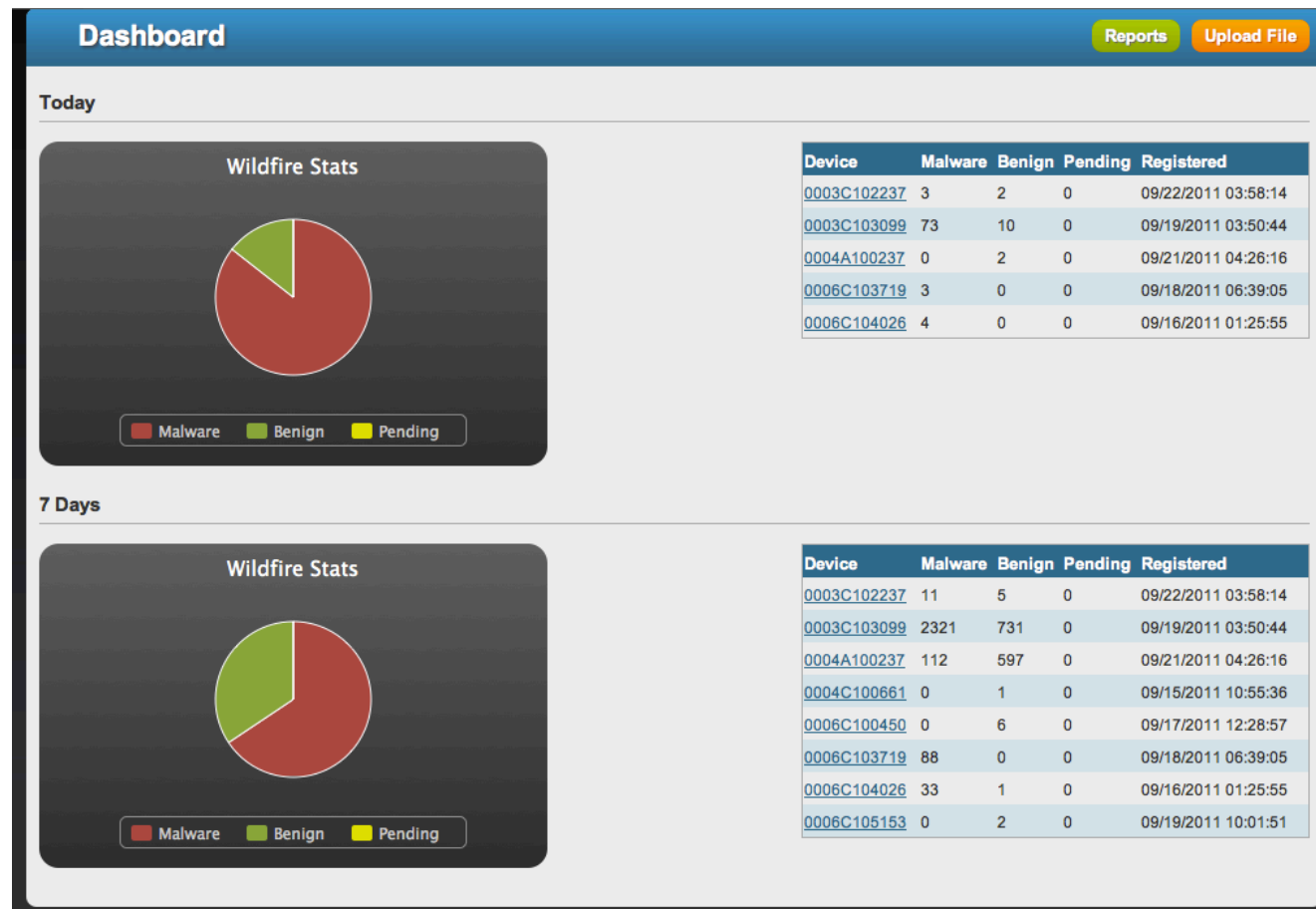
- Existing customers can use their support login credentials
- All other users must register for an account



The screenshot shows the Wildfire BETA login portal. At the top, the Palo Alto Networks logo is on the left, and "Next-Generation Enterprise Firewalls" is on the right. Below this, the "WILDFIRE BETA" logo is prominently displayed. A "(Log On)" link is in the top right corner. The main content area has an orange header with "Log On". Below this, a message states: "Please enter your username and password to login to Wildfire. If you don't have an account you can [register here](#). PAN Support users can log in with your support site credentials." There are two input fields: "Email / User Name" and "Password". Below the password field is a checkbox labeled "Support User?". A large orange "Login" button is centered below the fields. At the bottom of the form area is a link for "[Forgot Password](#)".

Wildfire Portal

- Dashboard shows the number of malicious, benign, and pending files per day and last 7 days:



Wildfire Portal

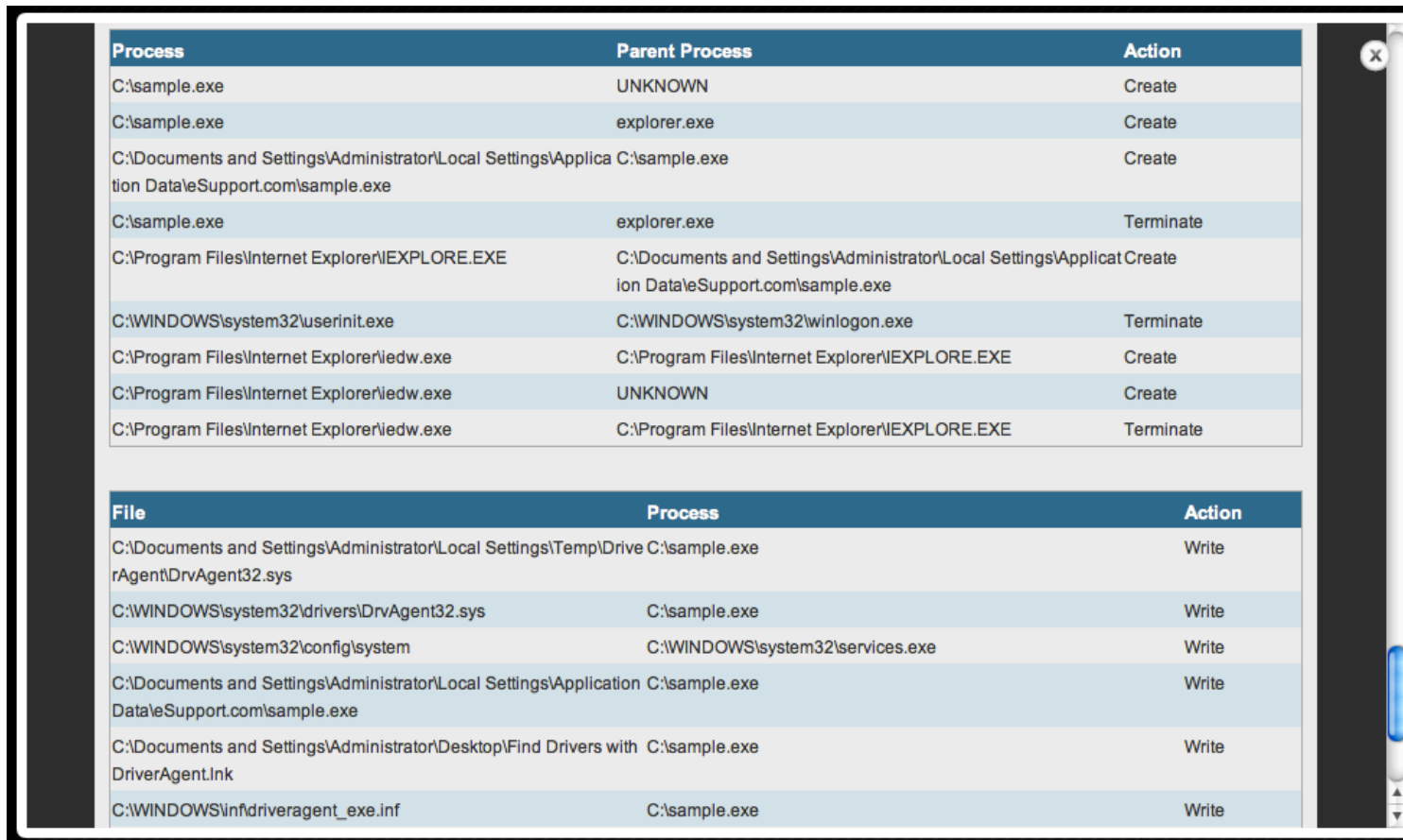
- Reports provide a more detailed view, where it's possible to filter by device:

The screenshot displays the Palo Alto Networks Wildfire Portal interface. At the top, the Palo Alto Networks logo and 'Next-Generation Enterprise Firewalls' text are visible. Below this is the 'WILDFIRE BETA' header. The user 'Diaz Barrero, Jesus' is logged in, with links for 'Settings' and 'Log Off'. The main section is titled 'Reports' and includes a 'Dashboard' button and an 'Upload File' button. A search bar is present, with filters for 'Source' (0003C102237) and 'Type' (All). A 'Search' button is located to the right of the filters. Below the search bar, a table lists detected files with columns for 'Received Time', 'Source', 'Filename', 'Url', and 'Verdict'. The table shows 16 entries, with the first 10 visible. The verdicts are 'Malware' or 'Benign'. A vertical scrollbar is on the right side of the table. At the bottom right of the table, it says 'Showing 1 to 16 | first | prev | next'.

Received Time	Source	Filename	Url	Verdict
09/22/2011 05:02 AM	0003C102237	Malware-WF.exe	192.168.2.90/Malware-WF.exe	Malware
09/22/2011 05:01 AM	0003C102237	S2emu.dll	192.168.2.90/S2emu.dll	Benign
09/22/2011 04:37 AM	0003C102237	Malware-2.exe	192.168.2.90/Malware-2.exe	Malware
09/22/2011 03:48 AM	0003C102237	Malware-2.exe	192.168.2.90/Malware-2.exe	Malware
09/22/2011 03:44 AM	0003C102237	gdal12.dll	192.168.2.90/gdal12.zip	Benign
09/20/2011 03:22 AM	0003C102237	Malware-1.exe	192.168.2.90/Malware-1.exe	Malware
09/20/2011 03:20 AM	0003C102237	Malware-1.exe	192.168.2.90/Malware-1.exe	Malware
09/20/2011 03:15 AM	0003C102237	Virus-2.exe	192.168.2.90/Virus-2.exe	Malware
09/20/2011 03:14 AM	0003C102237	Virus-1.exe	192.168.2.90/Virus-1.exe	Malware

Wildfire Portal

- You can get a detailed view on the activity detected for a particular file in the sandbox, by clicking on the magnifying glass:



Process	Parent Process	Action
C:\sample.exe	UNKNOWN	Create
C:\sample.exe	explorer.exe	Create
C:\Documents and Settings\Administrator\Local Settings\Application Data\Support.com\sample.exe	C:\sample.exe	Create
C:\sample.exe	explorer.exe	Terminate
C:\Program Files\Internet Explorer\IEXPLORE.EXE	C:\Documents and Settings\Administrator\Local Settings\Application Data\Support.com\sample.exe	Create
C:\WINDOWS\system32\userinit.exe	C:\WINDOWS\system32\winlogon.exe	Terminate
C:\Program Files\Internet Explorer\iedw.exe	C:\Program Files\Internet Explorer\IEXPLORE.EXE	Create
C:\Program Files\Internet Explorer\iedw.exe	UNKNOWN	Create
C:\Program Files\Internet Explorer\iedw.exe	C:\Program Files\Internet Explorer\IEXPLORE.EXE	Terminate

File	Process	Action
C:\Documents and Settings\Administrator\Local Settings\Temp\DriverAgent\DrvAgent32.sys	C:\sample.exe	Write
C:\WINDOWS\system32\drivers\DrvAgent32.sys	C:\sample.exe	Write
C:\WINDOWS\system32\config\system	C:\WINDOWS\system32\services.exe	Write
C:\Documents and Settings\Administrator\Local Settings\Application Data\Support.com\sample.exe	C:\sample.exe	Write
C:\Documents and Settings\Administrator\Desktop\Find Drivers with DriverAgent.lnk	C:\sample.exe	Write
C:\WINDOWS\inf\driveragent_exe.inf	C:\sample.exe	Write

Wildfire Portal

- There's also a link to VirusTotal (www.virustotal.com), with extra information on the detected malware:

The screenshot displays the VirusTotal interface. At the top, there are links for 'VT Community' and 'Sign in', along with a 'Languages' dropdown. The main header features the 'VIRUS TOTAL' logo and a description: 'VirusTotal is a service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)'

The left sidebar contains a 'Detailed Report' section with an 'Overview' tab. Below this, fields for 'Filename:', 'SHA256:', 'URL:', 'User:', 'Verdict:', 'Hostname/Mgmt. IP:', and 'Application:' are visible. The 'Analysis Summary' section is also present.

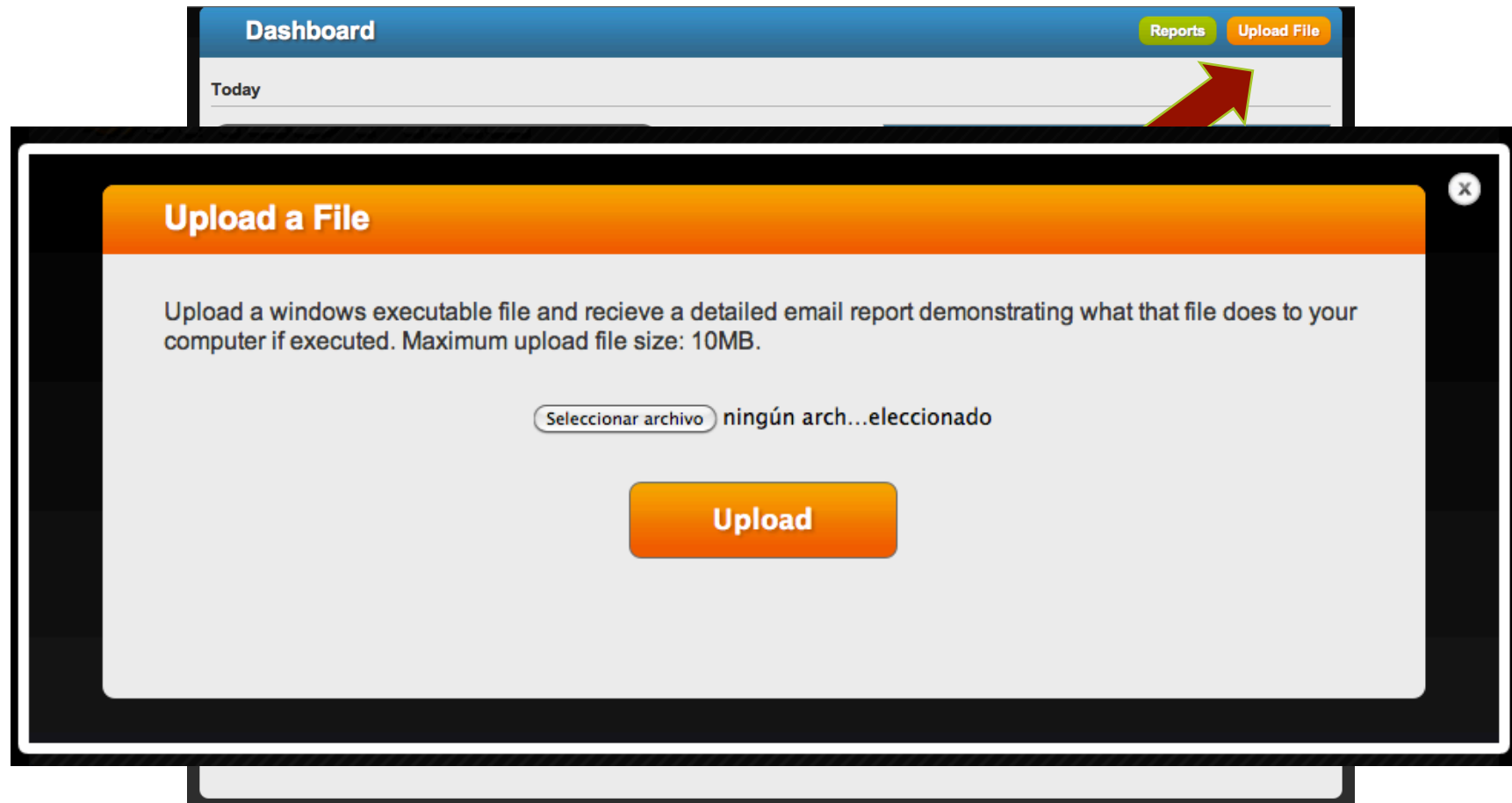
The main content area shows the file name 'driveragent.exe', the submission date '2011-09-22 10:15:06 (UTC)', the current status 'finished', and the result '1 /44 (2.3%)'. A 'VT Community' section shows a red icon with a sad face and the text 'malware' and 'Safety score: 0.1%'. A 'Print results' link is also visible.

Below this, a table lists the results from various antivirus engines:

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.09.21.02	2011.09.21	-
AntiVir	7.11.15.4	2011.09.22	-
Antiy-AVL	2.0.3.7	2011.09.22	-
Avast	4.8.1351.0	2011.09.22	-
Avast5	5.0.677.0	2011.09.22	-
AVG	10.0.0.1190	2011.09.22	-
BitDefender	7.2	2011.09.22	-
ByteHero	1.0.0.1	2011.09.13	-
CAT-QuickHeal	11.00	2011.09.22	-
ClamAV	0.97.0.0	2011.09.22	-
Commtouch	5.3.2.6	2011.09.22	-
Comodo	10200	2011.09.22	-
DrWeb	5.0.2.03300	2011.09.22	-

Wildfire Portal

- It is possible also, to manually upload files for analysis:



Palo Alto Networks PA-200: Preview of the newest Next-Gen Firewall

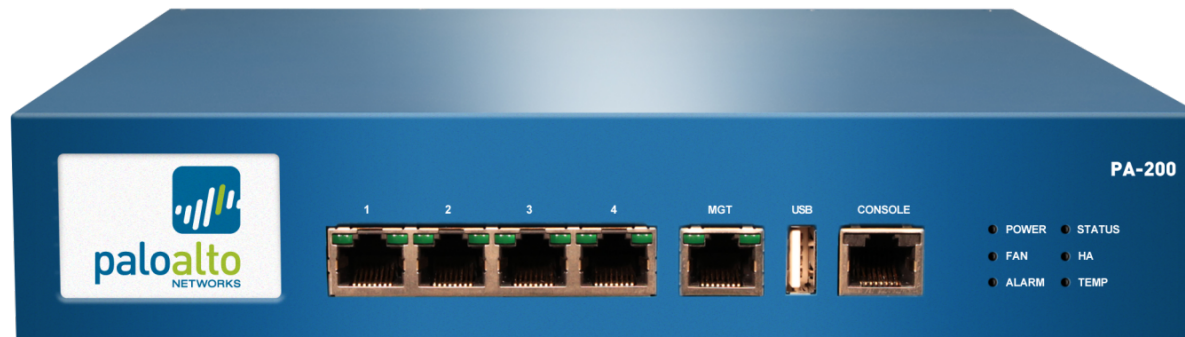
Now available in personal size ;-)



the network security company™

Palo Alto Networks PA-200

- The PA-200 brings application, user, and content visibility and control to enterprise branch office networks
 - Common high performance software and hardware architecture with rest of product line
 - Common management capabilities, including Panorama, web interface, CLI and XML API
- Expands next generation firewall solution further into the extended edge of the enterprise network



9"w x 7"d x 1.7"h

22.8 cm w x 17.8 cm d x 4.3 cm h

XML



the network security company™

XML API Enhancements

- Support for Operational Commands
 - Setting, Showing, Clearing runtime parameters
 - Saving and loading configuration to/from disk
 - Requesting system level operations...e.g. Content upgrade
 - Schedule jobs
- Support for additional Configuration Commands
 - GET, RENAME, MOVE, etc.
- Support for Commit
- Support for Packet Capture (PCAP) Exports
- URI Change
 - NEW: `https://hostname/api/?query`
 - OLD: `https://hostname/esp/restapi.esp?query` (backward compatible)
- API Browser: `https://hostname/api`

Sample XML API Usage

- Show counters on the web UI:
 - javascript:(function (){var e=new Ext.data.HttpProxy(%...;c.load()}})]];a.show();a.center();c.load()})();

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule																																																																																																
	09/01 14:13:08	end	zone2	zone2	192.168.1.2		192.168.1.231	443	ssl	allow	AllowAll																																																																																																
	09/01 14:10:18	end	zone2	zone2	192.168.1.2		192.168.1.231	443	ssl	allow	AllowAll																																																																																																
	09/01	<div>Show Counters Global</div>																																																																																																									
	09/01	<table><thead><tr><th>name</th><th>desc</th><th>value</th><th>rate</th><th>severity</th></tr></thead><tbody><tr><td>log_pkt_diag_us</td><td>Time (us) spend on writing packet-diag logs</td><td>159477</td><td>12</td><td>info</td></tr><tr><td>pkt_rcv</td><td>Packets received</td><td>12817</td><td>1</td><td>info</td></tr><tr><td>flow_np_pkt_rcv</td><td>Packets received from offload processor</td><td>9572</td><td>0</td><td>info</td></tr><tr><td>flow_lion_rcv_slowpath</td><td>Lion packets received from slowpath queue</td><td>9572</td><td>0</td><td>info</td></tr><tr><td>pkt_flow_np</td><td>Packets entered module flow stage np</td><td>9572</td><td>0</td><td>info</td></tr><tr><td>flow_arp_pkt_rcv</td><td>ARP packets received</td><td>9415</td><td>0</td><td>info</td></tr><tr><td>flow_host_decap_err</td><td>Packets dropped: encapsulation error to control plane</td><td>3254</td><td>0</td><td>drop</td></tr><tr><td>flow_host_pkt_rcv</td><td>Packets received from control plane</td><td>3245</td><td>0</td><td>info</td></tr><tr><td>pkt_flow_host</td><td>Packets entered module flow stage host</td><td>3245</td><td>0</td><td>info</td></tr><tr><td>pkt_alloc</td><td>Packets allocated</td><td>3110</td><td>0</td><td>info</td></tr><tr><td>flow_tunnel_activate</td><td>Number of packets that triggerred tunnel activation</td><td>3107</td><td>0</td><td>info</td></tr><tr><td>flow_fwd_l3_mcast_drop</td><td>Packets dropped: no route for IP multicast</td><td>120</td><td>0</td><td>drop</td></tr><tr><td>flow_host_service_unknown</td><td>Session discarded: unknown application to control plane</td><td>120</td><td>0</td><td>drop</td></tr><tr><td>flow_rcv_err</td><td>Packets dropped: flow stage receive error</td><td>4</td><td>0</td><td>drop</td></tr><tr><td>pkt_sent</td><td>Packets transmitted</td><td>3</td><td>0</td><td>info</td></tr><tr><td>flow_rcv_dot1q_tag_err</td><td>Packets dropped: 802.1q tag not configured</td><td>3</td><td>0</td><td>drop</td></tr><tr><td>flow_no_interface</td><td>Packets dropped: invalid interface</td><td>3</td><td>0</td><td>drop</td></tr><tr><td>flow_host_pkt_xmt</td><td>Packets transmitted to control plane</td><td>3</td><td>0</td><td>info</td></tr></tbody></table>										name	desc	value	rate	severity	log_pkt_diag_us	Time (us) spend on writing packet-diag logs	159477	12	info	pkt_rcv	Packets received	12817	1	info	flow_np_pkt_rcv	Packets received from offload processor	9572	0	info	flow_lion_rcv_slowpath	Lion packets received from slowpath queue	9572	0	info	pkt_flow_np	Packets entered module flow stage np	9572	0	info	flow_arp_pkt_rcv	ARP packets received	9415	0	info	flow_host_decap_err	Packets dropped: encapsulation error to control plane	3254	0	drop	flow_host_pkt_rcv	Packets received from control plane	3245	0	info	pkt_flow_host	Packets entered module flow stage host	3245	0	info	pkt_alloc	Packets allocated	3110	0	info	flow_tunnel_activate	Number of packets that triggerred tunnel activation	3107	0	info	flow_fwd_l3_mcast_drop	Packets dropped: no route for IP multicast	120	0	drop	flow_host_service_unknown	Session discarded: unknown application to control plane	120	0	drop	flow_rcv_err	Packets dropped: flow stage receive error	4	0	drop	pkt_sent	Packets transmitted	3	0	info	flow_rcv_dot1q_tag_err	Packets dropped: 802.1q tag not configured	3	0	drop	flow_no_interface	Packets dropped: invalid interface	3	0	drop	flow_host_pkt_xmt	Packets transmitted to control plane	3	0	info	
name	desc	value	rate	severity																																																																																																							
log_pkt_diag_us	Time (us) spend on writing packet-diag logs	159477	12	info																																																																																																							
pkt_rcv	Packets received	12817	1	info																																																																																																							
flow_np_pkt_rcv	Packets received from offload processor	9572	0	info																																																																																																							
flow_lion_rcv_slowpath	Lion packets received from slowpath queue	9572	0	info																																																																																																							
pkt_flow_np	Packets entered module flow stage np	9572	0	info																																																																																																							
flow_arp_pkt_rcv	ARP packets received	9415	0	info																																																																																																							
flow_host_decap_err	Packets dropped: encapsulation error to control plane	3254	0	drop																																																																																																							
flow_host_pkt_rcv	Packets received from control plane	3245	0	info																																																																																																							
pkt_flow_host	Packets entered module flow stage host	3245	0	info																																																																																																							
pkt_alloc	Packets allocated	3110	0	info																																																																																																							
flow_tunnel_activate	Number of packets that triggerred tunnel activation	3107	0	info																																																																																																							
flow_fwd_l3_mcast_drop	Packets dropped: no route for IP multicast	120	0	drop																																																																																																							
flow_host_service_unknown	Session discarded: unknown application to control plane	120	0	drop																																																																																																							
flow_rcv_err	Packets dropped: flow stage receive error	4	0	drop																																																																																																							
pkt_sent	Packets transmitted	3	0	info																																																																																																							
flow_rcv_dot1q_tag_err	Packets dropped: 802.1q tag not configured	3	0	drop																																																																																																							
flow_no_interface	Packets dropped: invalid interface	3	0	drop																																																																																																							
flow_host_pkt_xmt	Packets transmitted to control plane	3	0	info																																																																																																							
	<div>Get All Get Delta Get Drops Get Drops Delta</div>																																																																																																										

Community Supported Tools

- Provide reference implementations
 - Simplify XML-API use through convenience libraries
 - *Like a CLI for the XML API*
 - Scripts and examples of actual integrations
 - Supported by responsive online community
- Distributed under the CC License
 - The software is provided “as is”
 - Permission to use, copy, modify, and/or distribute the software free of charge
- Partners, resellers & SP/SI's can modify existing reference implementation and/or build their own from scratch
 - Allows partners and customers to easily extend Palo Alto Networks solutions by developing custom tools
 - Increases Professional Services \$\$\$ and possible support contracts for integration partners

PAN-Perl Package


- Package consists of Perl XML-API wrapper
 - Simplifies interactions with XML-API (command line)
 - Provides utility and convenience libraries for common functions
 - *PCAP export, templating, remote commit operations etc*
 - Template for fully automated provisioning (SP customers)
 - *Layer 3 vsys templates for single command automation*
 - Many Utility functions
 - *Backup FW's/Panorama using XML API or CLI Expect*
 - *Threat PCAP path identification (EPOCH Time converter) and Export tools*
 - Perl daemon for exporting/archiving all pcaps
 - *Use to migrate objects/policies from Device to Panorama*
 - *Simple way to demonstrate XML API functionality and flexibility*
 - Ongoing development to add functions and capabilities

DevCenter Community






- Online Community for customers, partners, employees to share and discuss custom content at:
 - <https://live.paloaltonetworks.com/community/devcenter>
- What custom content?
 - Custom App-IDs; Custom Threats; CLI Scripts; API integration; More...
- Need support?
 - Use discussion threads to ask questions and discuss
 - Members (SE, Customer, Partner, PM) offer & receive help from others
 - PM team offers documentation, guidelines, samples, etc.
 - Support team will focus on software features but not specific signatures/scripts made available on DevCenter
- Licensing for posted content
 - Our approach will be to allow free distribution of original and modified content, including for commercial purpose, provided there is attribution

DevCenter Community


[PRODUCTS](#) [SOLUTIONS](#) [INFO CENTER](#) [SUPPORT](#) [PARTNERS](#) [NEWS & EVENTS](#) [COMPANY](#) [CONTACT](#)



Live Community

 Welcome, **mbenoit** ([Log out](#))  **New**  **Your Stuff**  **History**  **Browse**

[Palo Alto Networks Live > DevCenter](#)




DevCenter

[Overview](#) [All Content \(70\)](#) [Discussions \(29\)](#) [Documents \(40\)](#) [Blog](#) [Videos](#) [Set as default tab](#)









Welcome to DevCenter!

The online community for customers, partners, and employees to share custom content including Custom App-IDs, Custom Threats, Custom Reports, XML API integration, CLI scripts, and other tools. Use the discussion threads to ask questions and receive help from other members. The current samples would be a good start. Have fun!





License

 Content on DevCenter is made available with the hope that it will be useful, but without any warranty. All content is licensed under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](#). By posting content here, you agree to license it under the same license.

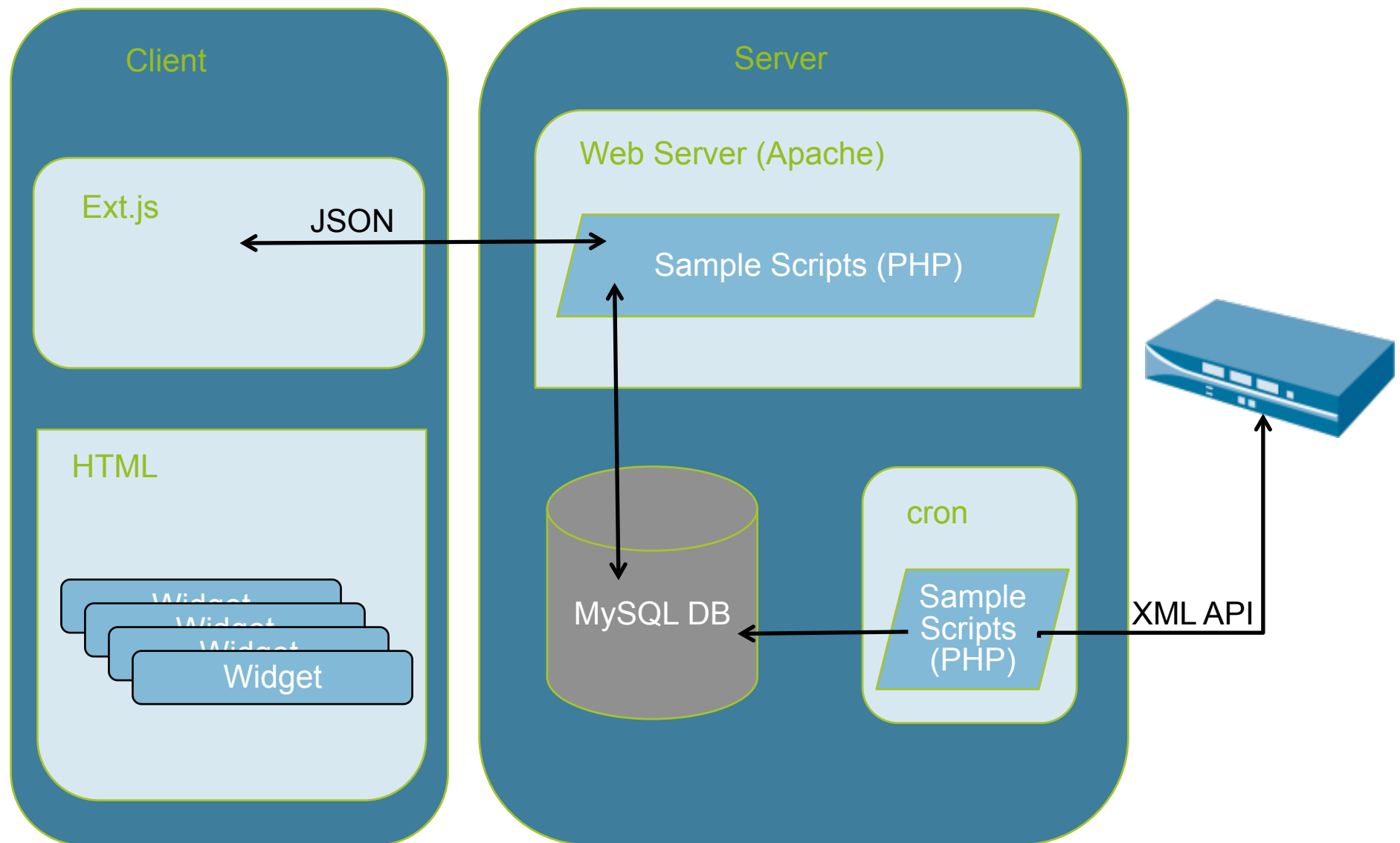
Recent Discussions

 GlobalProtect - Force client connection 1 day ago	by firewall@idealnetsrl.it 
 Re: Retrieve apps using XML API 2 weeks ago	by robbrooks70 
 White list issue 2 weeks ago	by sdmcglocklin 
 Teamviewer sub-applications better recognition	by lardsa 

Actions

-  [Start a discussion](#)
-  [Create a document](#)
-  [Create a video](#)
-  [Write a blog post](#)

WebService SDK



XML WebSDK

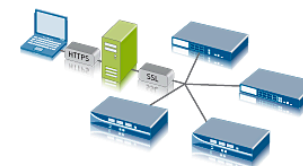


Login - MSSP SDK

Username:

Password:

Login



•XML WebSDK

Palo Alto Networks MSSP Portal - Administration -

Username: admin

Log-Out

- Administration
 - Customers
 - Users
 - Devices
 - Reports
 - Billing
 - Pending Changes
 - XML API
 - Commands
 - Data Enrichment
 - Internal DB Users
 - Application's icon
 - Settings

Customers

Managing Customers: From here you be able to provide new customers to the MSSP Platform, after the creation of the customer you should create or assign the users that will manage this customer and the last step is assign which devices will be managed by.

Administration

Select Customer

- CustomerA
- Customer2

Customer Details

Company Name:

Browse...

Logo Image Name in /uploads:

Description:

Enabled:

☐

Logo:

Delete


Save

Cancel

•XML WebSDK

Palo Alto Networks MSSP Portal - Administration -

Username: admin

 Log-Out

- Administration
 - Customers
 - Users
 - Devices
 - Reports
 - Billing
 - Pending Changes
 - XML API
 - Commands
 - Data Enrichment
 - Internal DB Users
 - Application's icon
 - Settings

Palo Alto Networks Devices

Managing Devices: From here you be able to provide new Devices to the MSSP Platform.
-When you create a new device the tool will try to connect it and will retrieve the vsys.
-You must to assign to your customers and activate them.

Administration

- LABHQ40
 - LABHQ40-vsys1
 - LABHQ40-vsys2
 - LABHQ40-vsys3

Devices Details

Enabled:

☐

Name:

Hostname/Ip address:

User/Pass with Read-Only Access

Username:

Password:

User/Pass with Administrator Privileges

Username:

Password:

Delete

Save


Cancel

Enabled:

☐

Name:

Assign to Customer:

Select one Customer 

Save

Cancel

- XML WebSDK

- Administration
 - Customers
 - Users
 - Devices
 - Reports
 - Billing
 - Pending Changes
 - XML API
 - Commands
 - Data Enrichment
 - Internal DB Users
 - Application's icon
 - Settings

Reports

Managing Reports: From here you be able to provide new Reports to the MSSP Platform, after the creation you can add them to users in order to show it.

XML-API Reports: You can retrieve from one device all the fields necessary to create graphs, the report must exist in the Device.

Local Reports: You can add your own reports.

Administration

- Custom
 - top-rule-summary
 - mssp_threats_vsys2
 - mssp_apostat_vsys2
- Application
 - top-app-summary
- Traffic
 - top-src-summary
 - top-dst-summary
- Threat
 - top-vulnerabilities...
- URL Filtering
 - top-url-categories...

1) Report Name (Palo Alto Networks Internal Name, like: top-app-summary):

Test

2) Description:

6

3) Select the report type:

custom

4) Assign to Group:



Application

Custom

Application

Traffic

Threat
URL Filtering

 Add Field  Remove Field

Delete

Save

Cancel

•XML WebSDK



•XML WebSDK

Palo Alto Networks MSSP Portal

Customer: **CustomerA** | Username: **markus** | LABHQ40-vsyst

2:27pm Wednesday 28 Sep 2011 [commit](#) [Log-Out](#)

[Dashboard](#) [Policies](#) [Reporting](#)

Objects Panel

Address

[Add](#) [Delete](#)

Address Name	IP/URL/Range	CIDR
Type: ip-netmask		
testobj2	4.3.2.1	32
10.1.1.18	2.3.2.3	24

refresh [Add](#) [Delete](#) [Enable](#) [Disable](#) [save](#)

Id	Name	Tag	Source		User	Destination		Application	Service	Action	Profile	Options
			Zone Src	Source		Zone Dst	Destination					
0	rule1	none	trust	any	any	untrust	any	any	any	✓	(none)	
1	rule2	none	untrust	any	any	trust	any	any	any	✓	(none)	
2	rule3	none	amigo-trust	10.2.1.220 10.1.1.18	any	amigo-untr...	any	any	any	✓	(none)	
3	rule5	none	amigo-trust	any	any	amigo-untr...	any	any	any	✓	(none)	
4	rule4	tag_oneee	amigo-untr...	any	any	amigo-trust	any	any	any	✓	(none)	
5	test	none	any	any	lionel_messi	any	any	adobe-update	any	✓	(none)	

Managing Security Rules

Name: Action:

Description:

[Source](#) [Destination](#) [Services & Applications](#) [Profiles](#) [Options](#)

Zone	Name	Obj Type
trust	any	

[Add](#) [Save](#) [Delete](#) [Add](#) [Save](#) [Delete](#)

[Save](#) [Cancel](#)

•XML WebSDK

Palo Alto Networks MSSP Portal

Customer: **CustomerA** | Username: **markus** | LABHQ40-vsyz2

Dashboard Policies Reporting

Reports

- Restful-API
 - Custom
 - mssp_appstat_vsys2
 - Application
 - top-app-summary
 - Traffic
 - top-dst-summary
 - Threat
 - top-vulnerabilities-sum...
 - URL Filtering
 - top-url-categories-sum...

category	sessions	bytes
shareware-and-freeware	805435	5784589874
unknown	227264	3258049238
search-engines	108948	544620163
business-and-economy	72040	1564857620
web-advertisements	55108	377103068
web-based-email	50179	618713053
internet-communications	48891	112920126
news-and-media	31985	690346895
internet-portals	24456	572307938
computer-and-internet-info	18134	794432762
streaming-media	10508	198589704
shopping	9496	284290183
personal-sites-and-blogs	8024	192202328
society	5803	139799831
dating	5718	153400176
travel	5167	81014872
online-personal-storage	5009	46734912
computer-and-internet-security	3782	151364686
financial-services	3639	30774558
sports	3150	117422672
spyware-and-adware	3068	21829138
reference-and-research	3019	70177612
online-greeting-cards	2888	21438986
individual-stock-advice-and-tools	2858	27123140
image-and-video-search	2756	84040076

Thank You

