PANOS REST API

October 2011

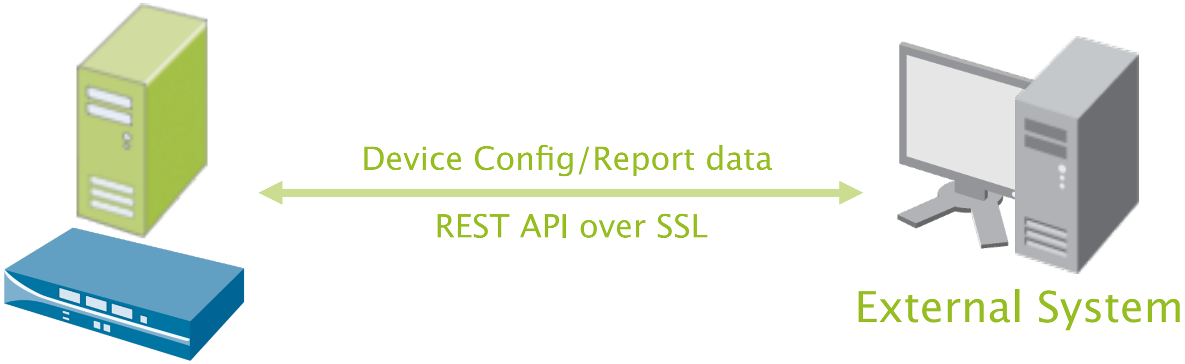
Business Development

paloalto NETWORKS

the network security company™

PANOS REST API

- External system can connect to device management interface or Panorama over SSL
  - Connection is treated as general admin web access
    - *same source address restriction and timeout settings*



- Used to:
  - Read/Write Device or Panorama Configuration
  - Extract report data in XML format
  - Execute Operational Commands
- Requires a key generated with admin ID and password info
  - Or a current authenticated administrative session

PANOS REST API - keygen

- Keygen for API communication

Key generation request example:

https://hostname/api/?type=keygen&user=username&password=password

Key generation response example:

<response status="success”><result><key>**0RgWc42Oi0vDx2WRUIUM6A=**</key></result></response>

PANOS REST API - xpath

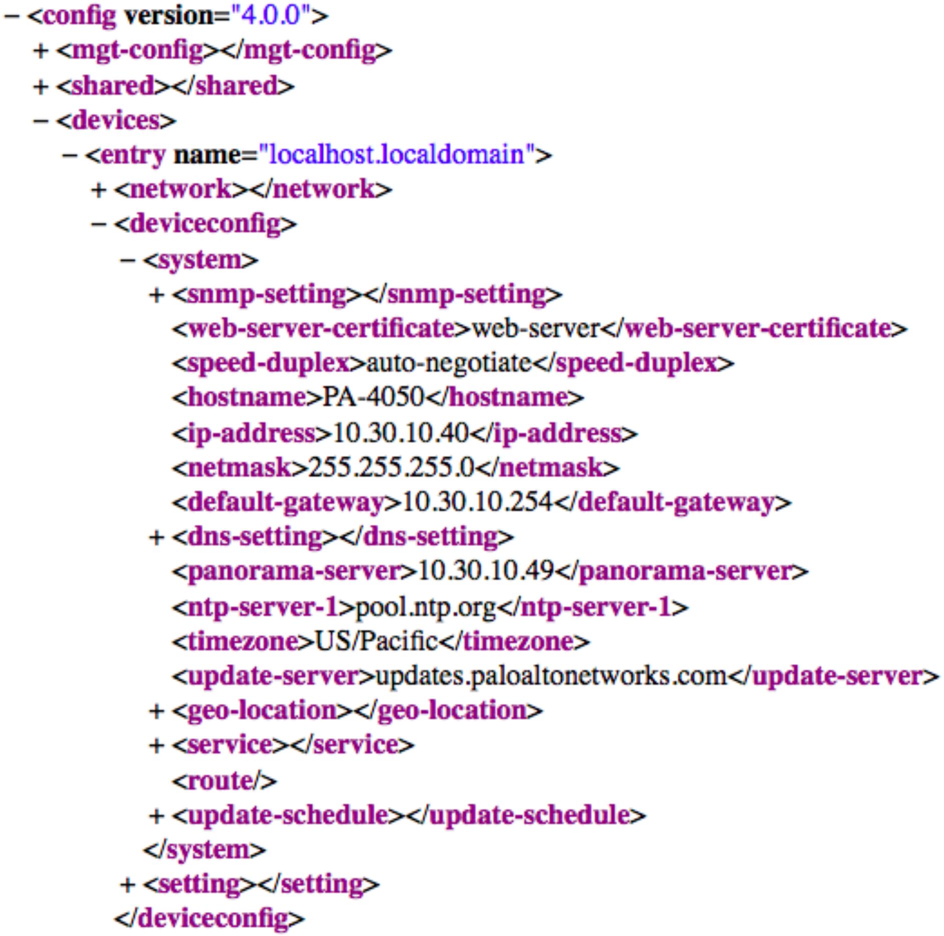
- *xpath*
  - Hierarchical XML path within firewall configuration file

Image at right depicts XML Device Configuration of a Palo Alto Networks Firewall

The same data can be viewed using the REST API at the following xpath:

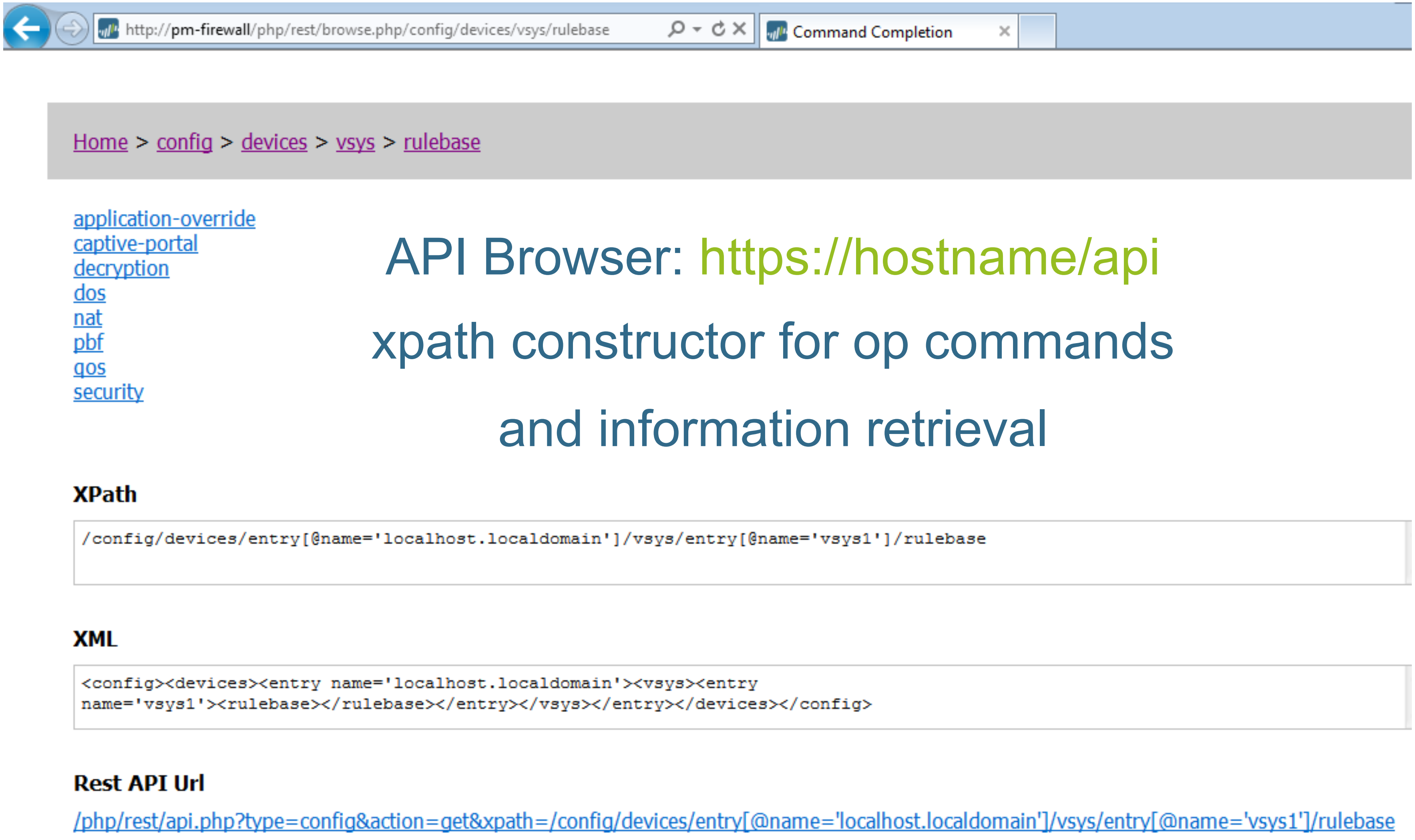
/config/devices/entry/deviceconfig

Utilize xpath to isolate viewing or to manipulate portions of the configuration



```
- <config version="4.0.0">
  + <mgt-config></mgt-config>
  + <shared></shared>
  - <devices>
    - <entry name="localhost.localdomain">
      + <network></network>
      - <deviceconfig>
        - <system>
          + <snmp-setting></snmp-setting>
            <web-server-certificate>web-server</web-server-certificate>
            <speed-duplex>auto-negotiate</speed-duplex>
            <hostname>PA-4050</hostname>
            <ip-address>10.30.10.40</ip-address>
            <netmask>255.255.255.0</netmask>
            <default-gateway>10.30.10.254</default-gateway>
          + <dns-setting></dns-setting>
            <panorama-server>10.30.10.49</panorama-server>
            <ntp-server-1>pool.ntp.org</ntp-server-1>
            <timezone>US/Pacific</timezone>
            <update-server>updates.paloaltonetworks.com</update-server>
          + <geo-location></geo-location>
          + <service></service>
            <route/>
          + <update-schedule></update-schedule>
          </system>
        + <setting></setting>
        </deviceconfig>
```

PANOS REST API - browser


http://pm-firewall/php/rest/browse.php/config/devices/vsys/rulebase
Command Completion

Home > config > devices > vsys > rulebase

- application-override
- captive-portal
- decryption
- dos
- nat
- pbf
- qos
- security

API Browser: https://hostname/api

xpath constructor for op commands

and information retrieval

XPath

```
/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/rulebase
```

XML

```
<config><devices><entry name='localhost.localdomain'><vsys><entry
name='vsys1'><rulebase></rulebase></entry></vsys></entry></devices></config>
```

Rest API Url

/php/rest/api.php?type=config&action=get&xpath=/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/rulebase

PANOS REST API - xpath

- Utilize CLI debug mode for determining xpath and syntax
  - Log in to device or Panorama via console or SSH session

```
>debug cli on
>configure
#set vsys vsys1 address demo-obj ip-netmask 1.2.3.4/32
```

Response includes:

```
<request cmd="set" obj="/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/address/entry[@name=’demo-obj']" cookie="0265032970635834"><ip-netmask>1.2.3.4/32</ip-netmask></request>
```

Strip out extraneous XML and cookie:

```
xpath=/config/devices/entry/vsys/entry[@name='vsys1']/address/entry[@name=’demo-obj']&element=<ip-netmask>1.2.3.4/32</ip-netmask>
```

PANOS REST API - xpath

- Same object name, different xpath:
  - Single VSYS or VSYS Specific

    /config/devices/entry/vsys/entry[@name='vsys1']/address/entry [@name=’demo-obj']

  - Shared Objects (Panorama, devices)

    /config/shared/address/entry[@name=’demo-obj’]

  - Panorama Device Group

    /config/devices/entry/device-group/entry[@name='DG1']/address/entry [@name=’demo-obj’]

  - Understand context of where objects and policies belong
    - *Shared objects can be utilized by multiple VSYS within a single device or by many devices managed by Panorama*
    - *VSYS specific objects are only available to that VSYS*
    - *Device Group specific objects are only available to devices that belong to the group*

PANOS REST API - config

- *type = config*
  - Specify the *action* [*show* | *get* | *set* | *edit* | *delete* | *rename* | *move*]

Example, IP Address for an interface (ethernet1/3)

```
xpath=/config/devices/entry/network/interface/ethernet/entry
[@name='ethernet1/3’]
```

Show the current IP Address for interface ethernet1/3 from running config

```
https://hostname/api/?type=config&action=show&key=keyvalue&
xpath=devices/entry/network/interface/ethernet/entry[@name='ethernet1/3’]/
layer3/ip
```

```
<response status="success”><result><ip><entry name="192.168.10.1/24"/></ip></
result></response>
```

PANOS REST API - config

- *type = config*
  - Specify the *action* [*show* | *get* | *set* | *edit* | *delete* | *rename* | *move*]

Add another IP Address to interface ethernet1/3 in the candidate configuration

```
https://hostname/api/?type=config&action=set&key=keyvalue&xpath=/
config/devices/entry/network/interface/ethernet/entry[@name='ethernet1/3']/
layer3/ip&element=<entry name='1.2.3.4/24'/>
```

```
<response status="success" code="20”><msg>command succeeded</msg></
response>
```

Commit your candidate configuration to make the change live

```
https://hostname/api/?
type=commit&action=set&key=keyvalue&cmd=<commit></commit>
```

```
<response status="success" code="19"> <result> <msg> <line>Commit job
enqueued with jobid 9</line> </msg> <job>9</job> </result> </response>
```

PANOS REST API - report

- *type = report*
  - Specify the *reporttype* [*dynamic* | *predefined* | *custom*]
  - Specify *reportname*
  - Can specify the *period* OR *starttime* & *endtime* *optional

Example : Get Application Top 3 data from ACC

https://hostname/api/?type=report&reporttype=dynamic&
reportname=top-app-summary&period=last-hour&topn=3&key=keyvalue

```
<response status="success"> <report reportname="top-app-summary" logtype="trsum">
<result name="Top applications" logtype="trsum" start="2011/10/10 16:58:02" start-
epoch="1318291082" end="2011/10/10 17:58:01" end-epoch="1318294681" generated-
at="2011/10/10 17:58:02" generated-at-epoch="1318294682"> <entry> <app>yahoo-
toolbar</app> <risk-of-app>2</risk-of-app> <bytes>2746868295</bytes>
<sessions>406209</sessions> </entry> <entry> <app>web-browsing</app> <risk-of-
app>4</risk-of-app> <bytes>2489995505</bytes> <sessions>218078</sessions> </entry>
<entry> <app>ssl</app> <risk-of-app>4</risk-of-app><bytes>1700670245</bytes>
<sessions>100718</sessions> </entry></result></report></response>
```

PANOS REST API - report

- *type = report*
  - Specify the *reporttype* [*dynamic* | *predefined* | *custom*]
  - Specify *reportname*
  - Can specify the *period* OR *starttime* & *endtime* *optional

“top-attackers-summary” data from dynamic report

https://hostname/api/?type=report&reporttype=dynamic&reportname=top-attackers-summary&key=keyvalue

```
<response status="success"><report name="Top Attackers" logtype="thsum" start="2011/10/10 19:34:43" start-epoch="1318300483" end="2011/10/10 20:34:42" end-epoch="1318304082" generated-at="2011/10/10 20:34:43" generated-at-epoch="1318304083"><entry><src>172.16.2.101</src><resolved-src>172.16.2.101</resolved-src><srcuser/><sessions>1114</sessions></entry><entry><src>172.16.1.100</src><resolved-src>172.16.1.100</resolved-src><srcuser/><sessions>745</sessions></entry></report></response>
```

PANOS REST API – op

Operational Commands

- Setting, Showing, Clearing runtime parameters

```
https://hostname/api/?key=keyvalue&type=op&cmd=<show><resource><limit><session/></limit></resource></show>
```

```
<response cmd=“status” status="success”><result>current session 0 max session 2097152</result></response>
```

- Saving and loading configuration to/from disk

```
https://hostname/api/?key=keyvalue&type=op&cmd=<save><config><to>abc.xml</to></config></save>
```

```
<response status="success”><result>Config saved to abc.xml.</result></response>
```

PANOS REST API – op

- Commit

  https://hostname/api/?key=keyvalue&type=commit&force=yes

  <response status="success" code=”20”><msg>**command succeeded**</msg></response>

- Support for Packet Capture (PCAP) File Listings and Exports

  https://hostname/api/?key=keyvalue&type=export&category=application-pcap&from=20100504/2-2200-722971.pcap&to=out.pcap

  Download of **out.pcap** will automatically commence

- Requesting system level operations…e.g. Content upgrade

  https://hostname/api/?key=keyvalue&type=op&cmd=<show><operational-mode></operational-mode></show>

  <response status="success”><result>**normal**</result></response>

PANOS REST API - examples

- *Easy to use in a web browser*

  Get a key:

  https://10.xx.10.50/api/?type=keygen&user=admin&password=admin

  Backup your config:

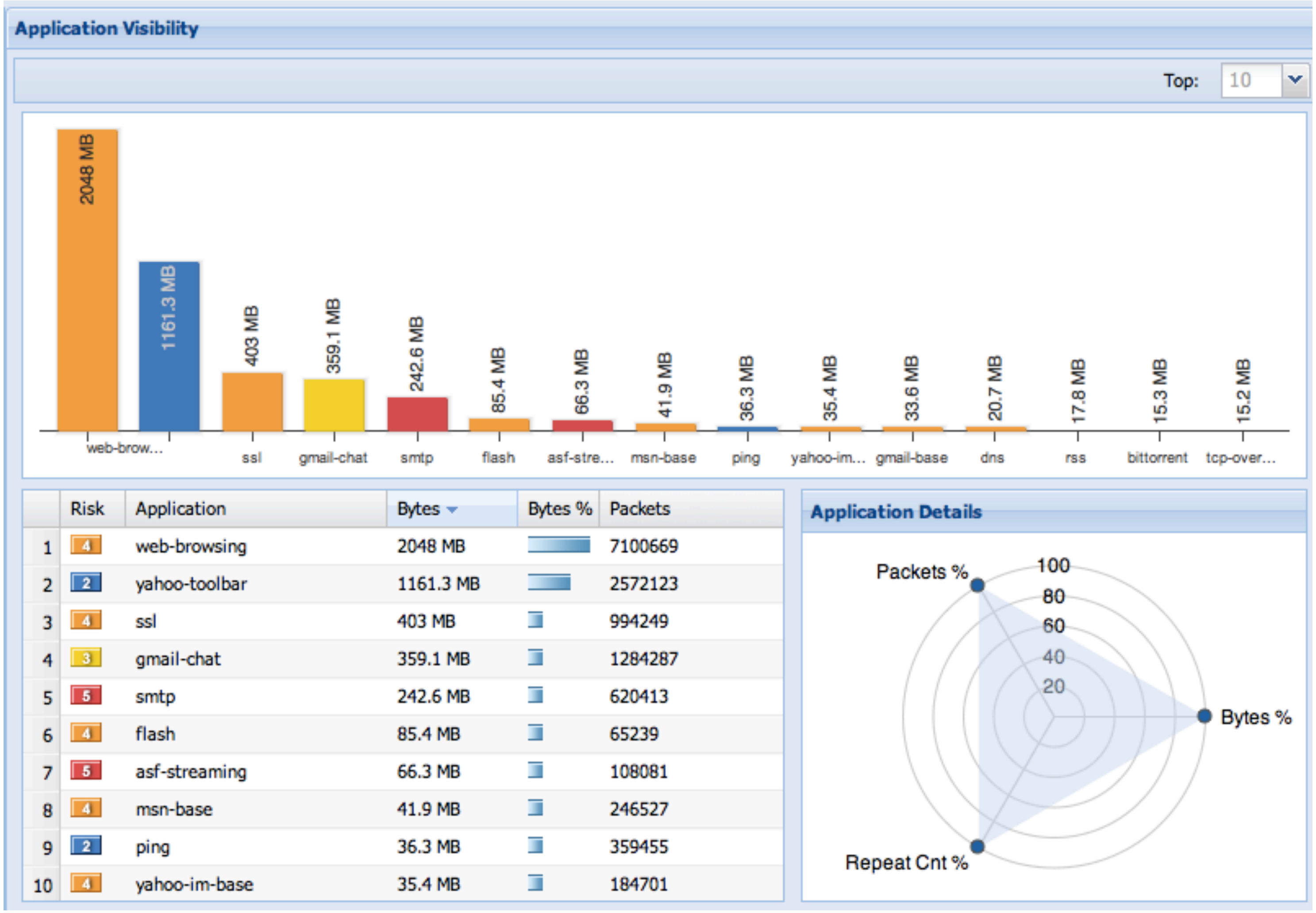
  https://10.xx.10.50/api/?type=config&action=show&key=0RgWc42Oi0vDx2WRUIUM6A=

  Generate a report:

  https://10.xx.10.50/api/?type=report&reporttype=dynamic&reportname=top-app-summary&period=last-hour&topn=5&key=0RgWc42Oi0vDx2WRUIUM6A=

PANOS REST API - examples

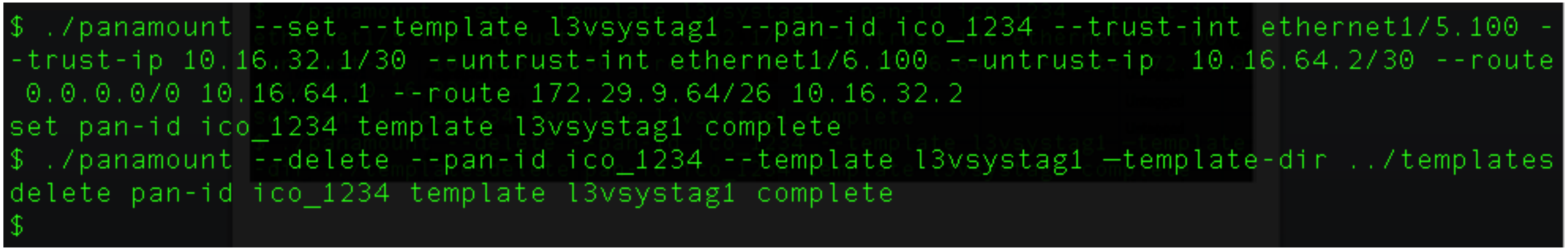
- Example of API Based Custom Reporting Web Application



	Risk	Application	Bytes	Bytes %	Packets
1	4	web-browsing	2048 MB	▬	7100669
2	2	yahoo-toolbar	1161.3 MB	▬	2572123
3	4	ssl	403 MB	▬	994249
4	3	gmail-chat	359.1 MB	▬	1284287
5	5	smtp	242.6 MB	▬	620413
6	4	flash	85.4 MB	▬	65239
7	5	asf-streaming	66.3 MB	▬	108081
8	4	msn-base	41.9 MB	▬	246527
9	2	ping	36.3 MB	▬	359455
10	4	yahoo-im-base	35.4 MB	▬	184701

PANOS REST API - examples

- Automated Provisioning for Virtual or Multi-Tennant Environments



```
$ ./panamount --set --template l3vsystag1 --pan-id ico_1234 --trust-int ethernet1/5.100 -
-trust-ip 10.16.32.1/30 --untrust-int ethernet1/6.100 --untrust-ip  10.16.64.2/30 --route
 0.0.0.0/0 10.16.64.1 --route 172.29.9.64/26 10.16.32.2
set pan-id ico_1234 template l3vsystag1 complete
$ ./panamount --delete --pan-id ico_1234 --template l3vsystag1 —template-dir ../templates
delete pan-id ico_1234 template l3vsystag1 complete
$
```

- PAN-perl Package available on DevCenter
  - https://live.paloaltonetworks.com/docs/DOC-1910
  - Includes convenience libraries, templates, sample integrations

For More Information: DevCenter

- Online Community for customers, partners, employees to share and discuss custom content at:
  - https://live.paloaltonetworks.com/community/devcenter
- Custom Content and Information
  - API integration, Custom App-IDs, Custom Signatures, CLI Scripts, etc.
  - DevCenter community offers documentation, guidelines, samples, etc.
- Support?
  - For issues with API's or PANOS components, open ticket with Support
  - For scripts, etc. Support is best effort by DevCenter community members
  - Use discussion threads to ask questions
    - *Members (SEs, Customers, Partners, PMs, Support) offer & receive help from each other*
- Licensing for posted content
  - free distribution of original and modified content, including for commercial purpose with attribution

paloalto
NETWORKS

the network security company™