App-ID

SE Boot Camp

PAN-OS 8.0

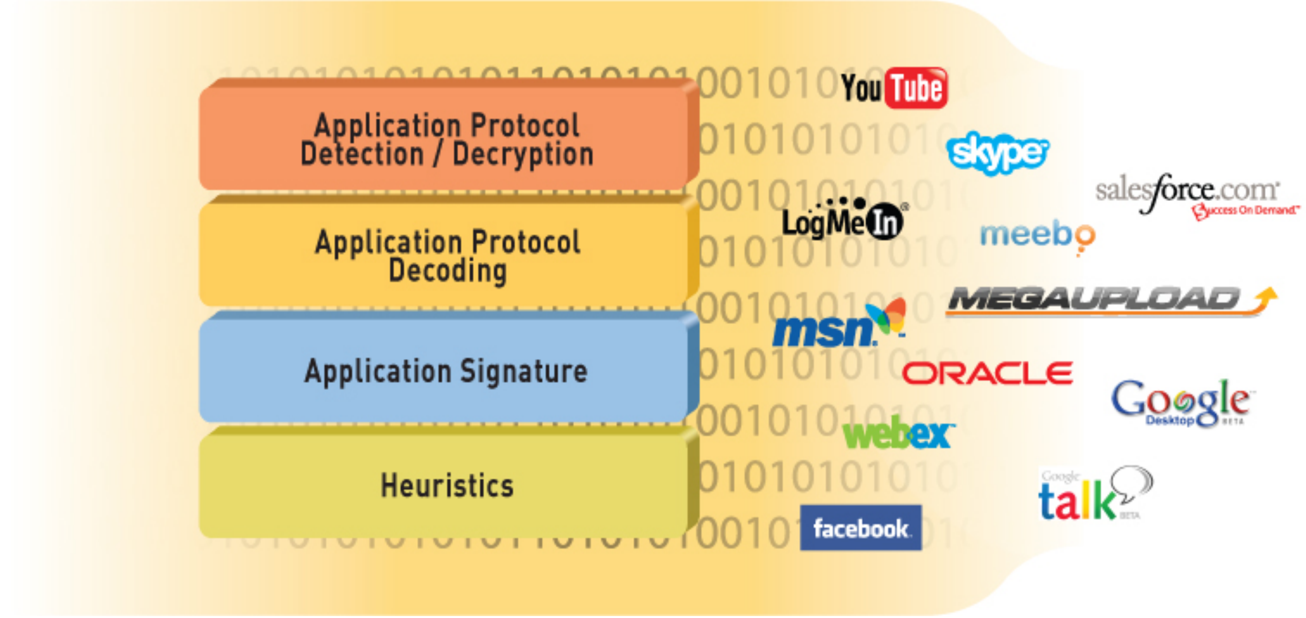
Agenda

- Anatomy of an Application Object
  - Object Elements
  - Application Groups and Filters
- Custom Signatures
  - Components of Signatures

Anatomy of an Application Object

App-ID

- Application identification is at the core of PAN-OS security, QoS, and PBF policies
- Each session contains the information that is necessary to identify the applications traversing the firewall



App-ID Components

Protocol Decoders

- Detect Protocol in Protocol within a session
- Provide context for application signatures

Application Signatures

- Detect Layer 7 signatures within a session

Protocol Decryption

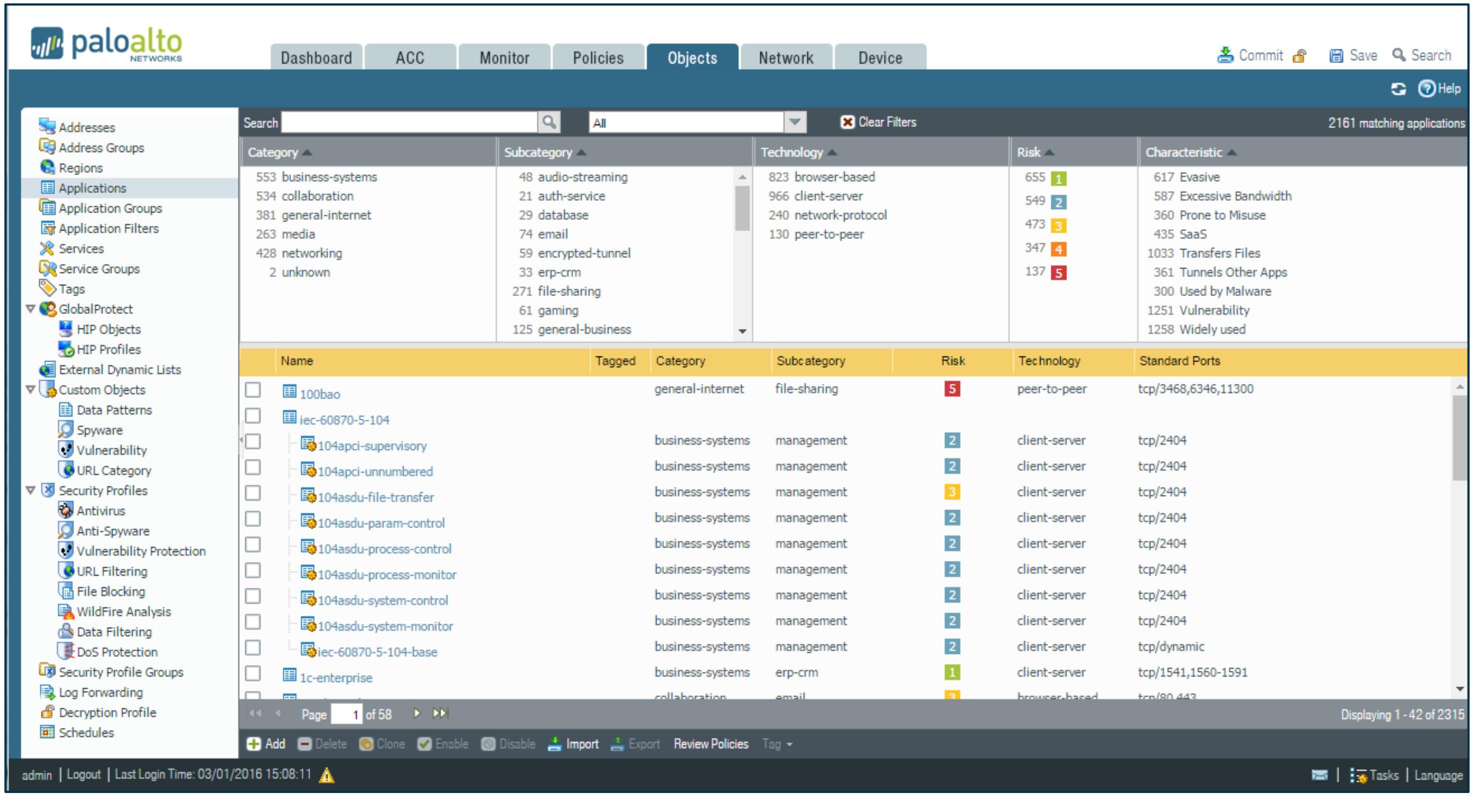
- SSL & SSH decryption

Heuristics

- Look for patterns of communication when no signature exists

Application Database

- Firewall (*Objects >> Applications*)



2161 matching applications

Category ▲	Subcategory ▲	Technology ▲	Risk ▲	Characteristic ▲
553 business-systems	48 audio-streaming	823 browser-based	655 1	617 Evasive
534 collaboration	21 auth-service	966 client-server	549 2	587 Excessive Bandwidth
381 general-internet	29 database	240 network-protocol	473 3	360 Prone to Misuse
263 media	74 email	130 peer-to-peer	347 4	435 SaaS
428 networking	59 encrypted-tunnel		137 5	1033 Transfers Files
2 unknown	33 erp-crm			361 Tunnels Other Apps
	271 file-sharing			300 Used by Malware
	61 gaming			1251 Vulnerability
	125 general-business			1258 Widely used

	Name	Tagged	Category	Subcategory	Risk	Technology	Standard Ports
□	100bao		general-internet	file-sharing	5	peer-to-peer	tcp/3468,6346,11300
□	iec-60870-5-104						
□	104apci-supervisory		business-systems	management	2	client-server	tcp/2404
□	104apci-unnumbered		business-systems	management	2	client-server	tcp/2404
□	104asdu-file-transfer		business-systems	management	3	client-server	tcp/2404
□	104asdu-param-control		business-systems	management	2	client-server	tcp/2404
□	104asdu-process-control		business-systems	management	2	client-server	tcp/2404
□	104asdu-process-monitor		business-systems	management	2	client-server	tcp/2404
□	104asdu-system-control		business-systems	management	2	client-server	tcp/2404
□	104asdu-system-monitor		business-systems	management	2	client-server	tcp/2404
□	iec-60870-5-104-base		business-systems	management	2	client-server	tcp/dynamic
□	1c-enterprise		business-systems	erp-crm	1	client-server	tcp/1541,1560-1591
□			collaboration	email	3	browser-based	tcp/80,443

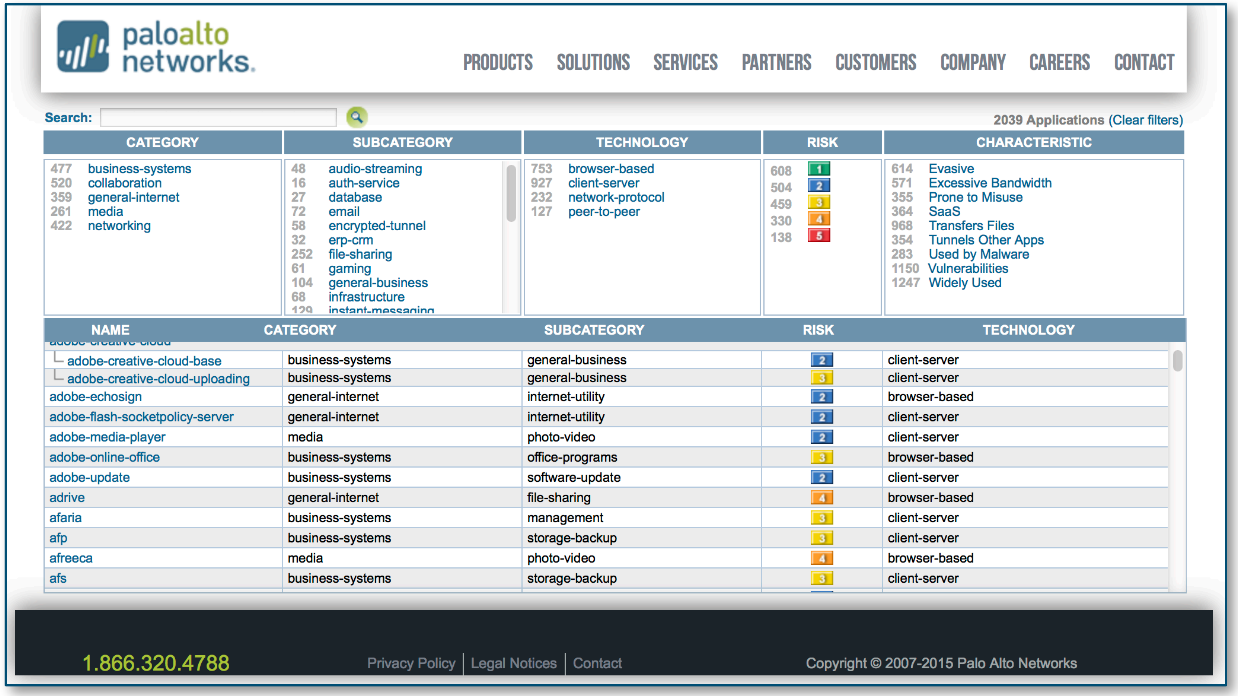
Page 1 of 58

Displaying 1 - 42 of 2315

admin | Logout | Last Login Time: 03/01/2016 15:08:11

Applipedia

- Applipedia (http://applipedia.paloaltonetworks.com)



2039 Applications (Clear filters)

CATEGORY	SUBCATEGORY	TECHNOLOGY	RISK	CHARACTERISTIC
477 business-systems	48 audio-streaming	753 browser-based	608 1	614 Evasive
520 collaboration	16 auth-service	927 client-server	504 2	571 Excessive Bandwidth
359 general-internet	27 database	232 network-protocol	459 3	355 Prone to Misuse
261 media	72 email	127 peer-to-peer	330 4	364 SaaS
422 networking	58 encrypted-tunnel		138 5	968 Transfers Files
	32 erp-crm			354 Tunnels Other Apps
	252 file-sharing			283 Used by Malware
	61 gaming			1150 Vulnerabilities
	104 general-business			1247 Widely Used
	68 infrastructure			
	129 instant-messaging			

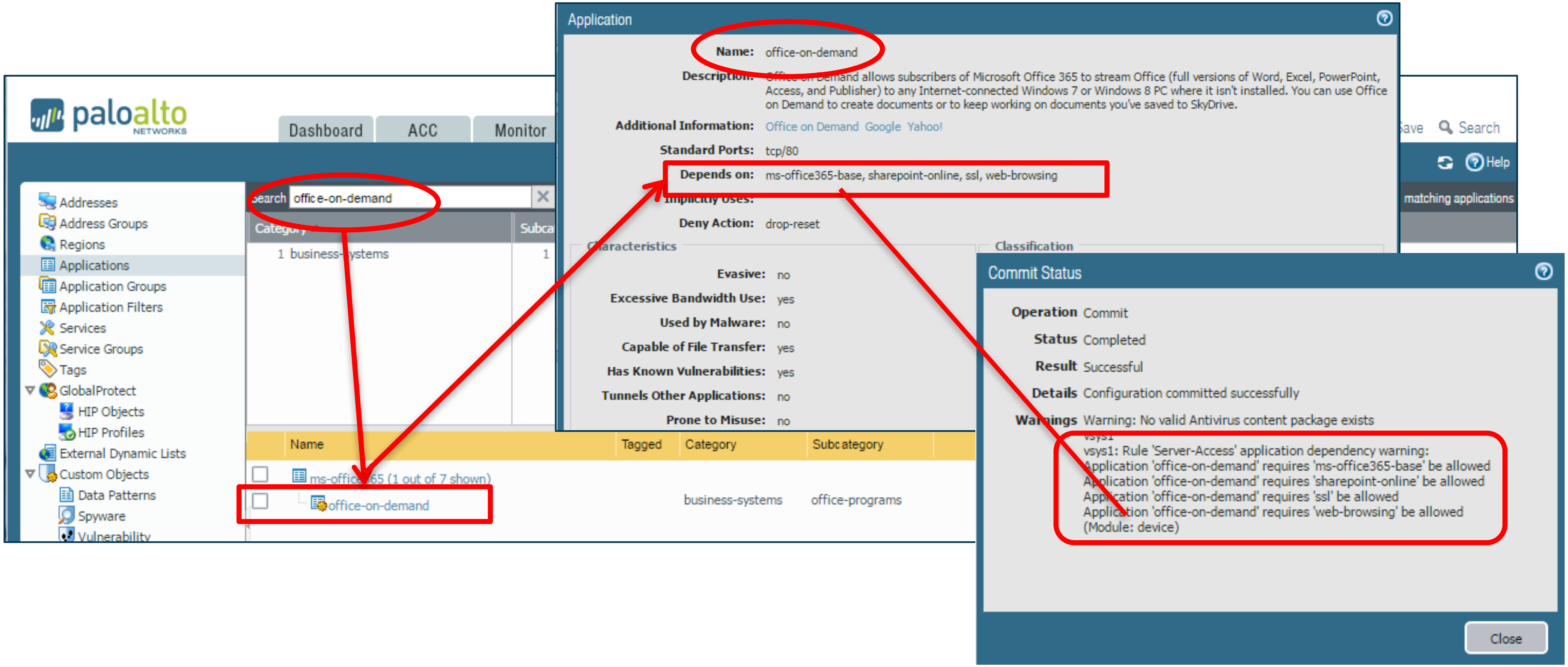
NAME	CATEGORY	SUBCATEGORY	RISK	TECHNOLOGY
adobe-creative-cloud				
└ adobe-creative-cloud-base	business-systems	general-business	2	client-server
└ adobe-creative-cloud-uploading	business-systems	general-business	3	client-server
adobe-echosign	general-internet	internet-utility	2	browser-based
adobe-flash-socketpolicy-server	general-internet	internet-utility	2	client-server
adobe-media-player	media	photo-video	2	client-server
adobe-online-office	business-systems	office-programs	3	browser-based
adobe-update	business-systems	software-update	2	client-server
adrive	general-internet	file-sharing	4	browser-based
afaria	business-systems	management	3	client-server
afp	business-systems	storage-backup	3	client-server
afreeca	media	photo-video	4	browser-based
afs	business-systems	storage-backup	3	client-server

1.866.320.4788

Privacy Policy | Legal Notices | Contact

Copyright © 2007-2015 Palo Alto Networks

Applications that Depend on Applications



Search: office-on-demand

1 business-systems 1

Name	Tagged	Category	Subcategory
□ ms-office365 (1 out of 7 shown)			
□ office-on-demand		business-systems	office-programs

Application

Name: office-on-demand

Description: Office on Demand allows subscribers of Microsoft Office 365 to stream Office (full versions of Word, Excel, PowerPoint, Access, and Publisher) to any Internet-connected Windows 7 or Windows 8 PC where it isn't installed. You can use Office on Demand to create documents or to keep working on documents you've saved to SkyDrive.

Additional Information: Office on Demand Google Yahoo!

Standard Ports: tcp/80

Depends on: ms-office365-base, sharepoint-online, ssl, web-browsing

Implicitly Uses:

Deny Action: drop-reset

Characteristics

Evasive: no

Excessive Bandwidth Use: yes

Used by Malware: no

Capable of File Transfer: yes

Has Known Vulnerabilities: yes

Tunnels Other Applications: no

Prone to Misuse: no

Classification

Commit Status

Operation Commit

Status Completed

Result Successful

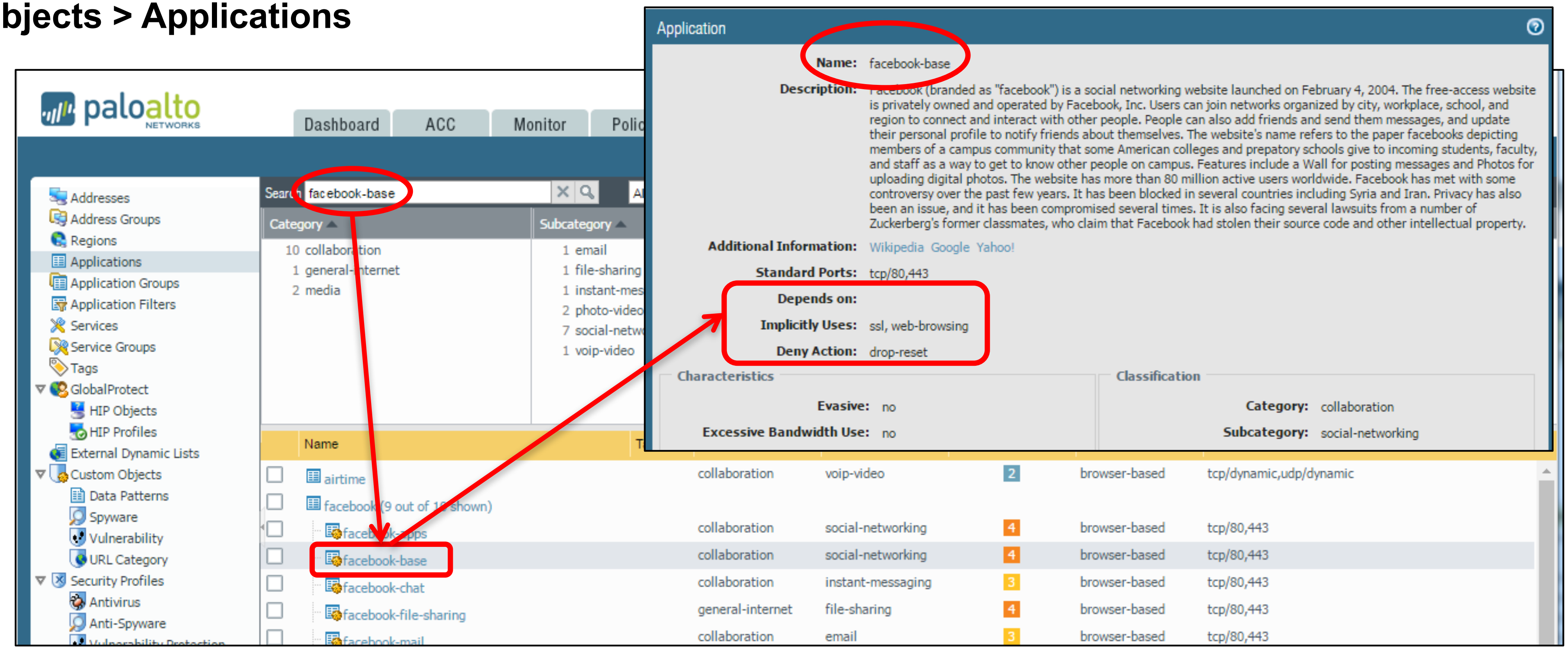
Details Configuration committed successfully

Warnings Warning: No valid Antivirus content package exists

```
vsys1
vsys1: Rule 'Server-Access' application dependency warning:
Application 'office-on-demand' requires 'ms-office365-base' be allowed
Application 'office-on-demand' requires 'sharepoint-online' be allowed
Application 'office-on-demand' requires 'ssl' be allowed
Application 'office-on-demand' requires 'web-browsing' be allowed
(Module: device)
```

Applications with Implicitly Used Applications

Objects > Applications



Application

Name: facebook-base

Description: Facebook (branded as "facebook") is a social networking website launched on February 4, 2004. The free-access website is privately owned and operated by Facebook, Inc. Users can join networks organized by city, workplace, school, and region to connect and interact with other people. People can also add friends and send them messages, and update their personal profile to notify friends about themselves. The website's name refers to the paper facebooks depicting members of a campus community that some American colleges and prepatory schools give to incoming students, faculty, and staff as a way to get to know other people on campus. Features include a Wall for posting messages and Photos for uploading digital photos. The website has more than 80 million active users worldwide. Facebook has met with some controversy over the past few years. It has been blocked in several countries including Syria and Iran. Privacy has also been an issue, and it has been compromised several times. It is also facing several lawsuits from a number of Zuckerberg's former classmates, who claim that Facebook had stolen their source code and other intellectual property.

Additional Information: Wikipedia Google Yahoo!

Standard Ports: tcp/80,443

Depends on:

Implicitly Uses: ssl, web-browsing

Deny Action: drop-reset

Characteristics

Evasive: no

Excessive Bandwidth Use: no

Classification

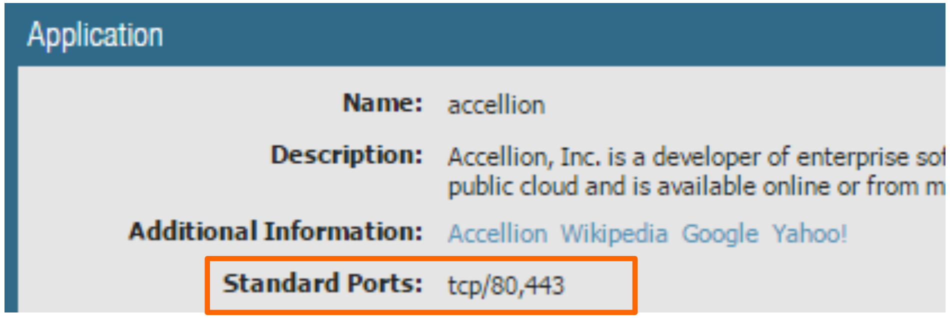
Category: collaboration

Subcategory: social-networking

	Name					
☐	airtime	collaboration	voip-video	2	browser-based	tcp/dynamic,udp/dynamic
☐	facebook (9 out of 10 shown)					
☐	facebook-apps	collaboration	social-networking	4	browser-based	tcp/80,443
☐	facebook-base	collaboration	social-networking	4	browser-based	tcp/80,443
☐	facebook-chat	collaboration	instant-messaging	3	browser-based	tcp/80,443
☐	facebook-file-sharing	general-internet	file-sharing	4	browser-based	tcp/80,443
☐	facebook-mail	collaboration	email	3	browser-based	tcp/80,443

Application Default

- Application-default uses the default port assigned to an application
  - web-browsing – default ports: tcp/80
- Default ports can be viewed in Applipedia or in the Application section of the firewall



Application

Name: accellion

Description: Accellion, Inc. is a developer of enterprise sof public cloud and is available online or from m

Additional Information: Accellion Wikipedia Google Yahoo!

Standard Ports: tcp/80,443

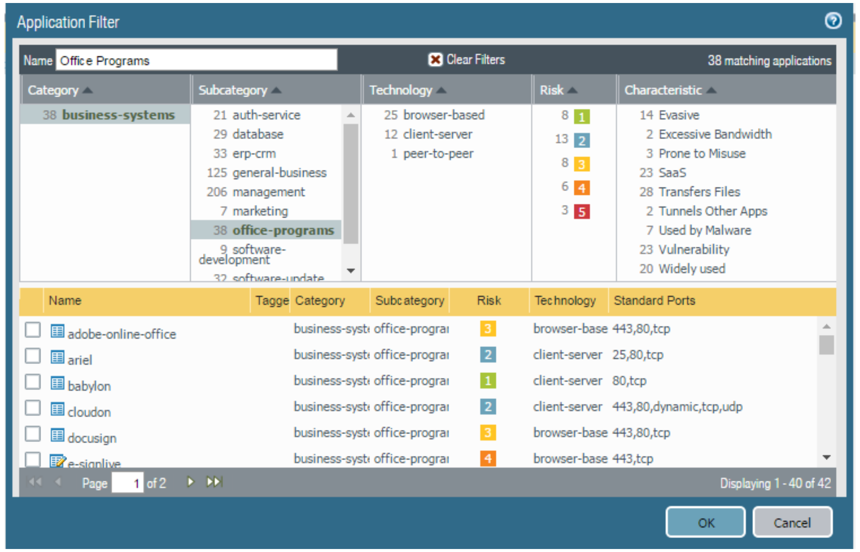
- Security rules use the **Service** column to specify port and protocol to be allowed or blocked:
  - Application-default
  - Any

Unknown Applications

- Applications may show up as “unknown”
  - Typical cause = payload values do not match an existing signature
- What to do with unknown apps:
  - Create security rule controlling unknown TCP/UDP
  - Create security rule with combination of Source Zone/Destination Zone/IP
  - Request app signature from Palo Alto Networks (common and proprietary)
  - Create a custom app signature (discussed later in the module)

Application Filters

- Application Filter
  - Application Filter allows the filtering of applications dynamically
  - You can create a filter by one or more application attributes
    - *Category*
    - *Sub-category*
    - *Technology*
    - *Risk*
    - *Characteristics*
  - When a content update occurs, new applications will be automatically added to the filter based on the filtering criteria



Name: Office Programs

38 matching applications

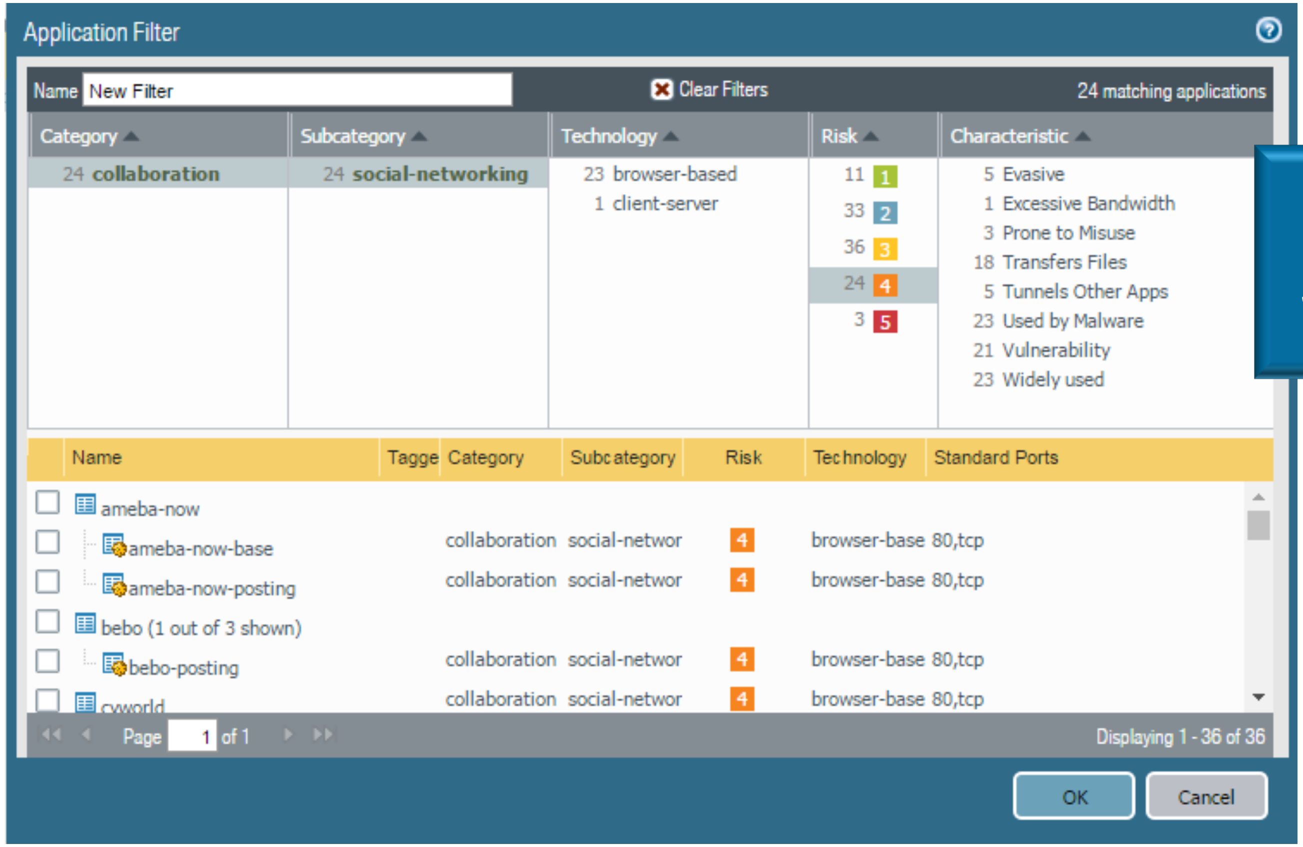
Category	Subcategory	Technology	Risk	Characteristic
38 **business-systems**	21 auth-service	25 browser-based	8 1	14 Evasive
	29 database	12 client-server	13 2	2 Excessive Bandwidth
	33 erp-crm	1 peer-to-peer	8 3	3 Prone to Misuse
	125 general-business		6 4	23 SaaS
	206 management		3 5	28 Transfers Files
	7 marketing			2 Tunnels Other Apps
	38 **office-programs**			7 Used by Malware
	9 software-development			23 Vulnerability
	32 software-update			20 Widely used

	Name	Tagge	Category	Subcategory	Risk	Technology	Standard Ports
□	adobe-online-office		business-syst	office-prograi	3	browser-base	443,80,tcp
□	ariel		business-syst	office-prograi	2	client-server	25,80,tcp
□	babylon		business-syst	office-prograi	1	client-server	80,tcp
□	cloudon		business-syst	office-prograi	2	client-server	443,80,dynamic,tcp,udp
□	docusign		business-syst	office-prograi	3	browser-base	443,80,tcp
□	e-signlive		business-syst	office-prograi	4	browser-base	443,tcp

Page 1 of 2

Displaying 1 - 40 of 42

Application Filter Example



Name New Filter

24 matching applications

Category	Subcategory	Technology	Risk	Characteristic
24 collaboration	24 social-networking	23 browser-based	11 1	5 Evasive
		1 client-server	33 2	1 Excessive Bandwidth
			36 3	3 Prone to Misuse
			24 4	18 Transfers Files
			3 5	5 Tunnels Other Apps
				23 Used by Malware
				21 Vulnerability
				23 Widely used

	Name	Tagge	Category	Subcategory	Risk	Technology	Standard Ports
☐	ameba-now						
☐	ameba-now-base		collaboration	social-networ	4	browser-base	80,tcp
☐	ameba-now-posting		collaboration	social-networ	4	browser-base	80,tcp
☐	bebo (1 out of 3 shown)						
☐	bebo-posting		collaboration	social-networ	4	browser-base	80,tcp
☐	cyworld		collaboration	social-networ	4	browser-base	80,tcp

Page 1 of 1

Displaying 1 - 36 of 36

Filter created using:

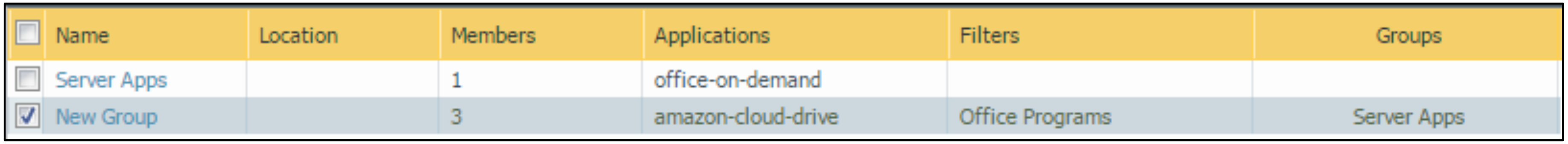
Category: Collaboration

Subcategory: Social-Networking

Risk: 4

Application Groups

- Application Groups
  - Application Group is an object that contains applications you want to treat similarly in a policy
  - Application Groups can contain:
    - Applications
    - Application Filters
    - Application Groups

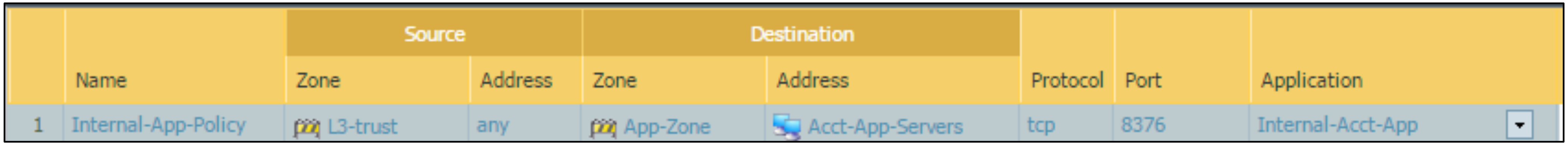


□	Name	Location	Members	Applications	Filters	Groups
□	Server Apps		1	office-on-demand		
☑	New Group		3	amazon-cloud-drive	Office Programs	Server Apps

Application Override Policy

- As an alternative to using custom signatures, use an application override policy to identify legitimate applications.
  - Increase application performance
  - Security policy referencing the App-ID is still needed
  - Policy defines traffic that will *not* go through App-ID processing

Policies > Application Override



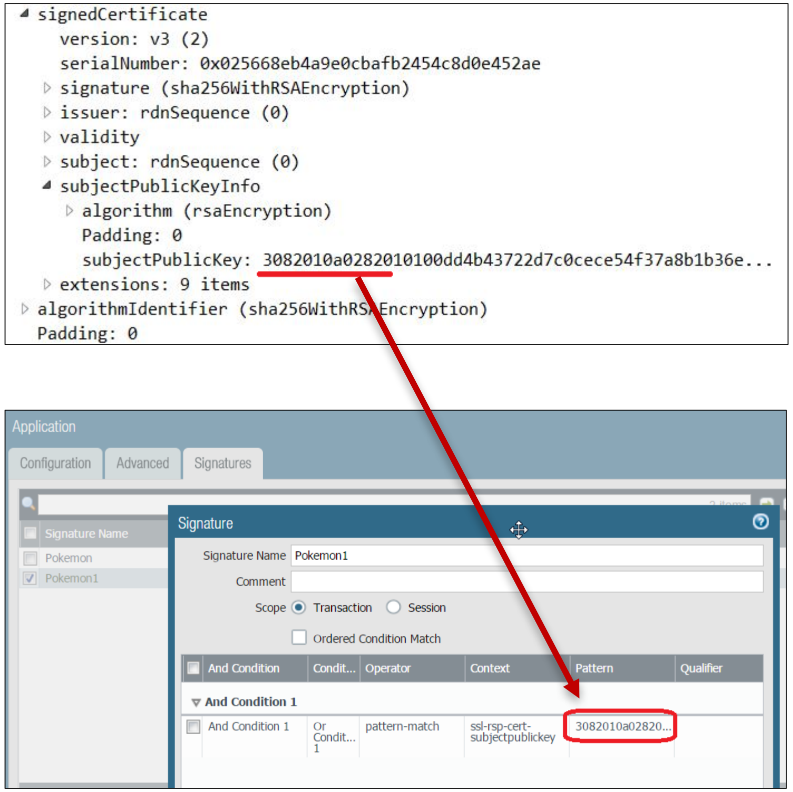
		Source		Destination				
	Name	Zone	Address	Zone	Address	Protocol	Port	Application
1	Internal-App-Policy	L3-trust	any	App-Zone	Acct-App-Servers	tcp	8376	Internal-Acct-App

"Name" is displayed in ACC, logs, and reports

Custom Signatures

Custom Signatures

- Custom Application Signatures
  - Identify proprietary applications
  - Achieve granularity of visibility and control over traffic
  - Identify ephemeral applications (“short-lived”)
    - March Madness, World Cup, Olympic Games
  - Nested applications
  - QoS for custom/proprietary traffic



```
◢ signedCertificate
    version: v3 (2)
    serialNumber: 0x025668eb4a9e0cbafb2454c8d0e452ae
  ▷ signature (sha256WithRSAEncryption)
  ▷ issuer: rdnSequence (0)
  ▷ validity
  ▷ subject: rdnSequence (0)
  ◢ subjectPublicKeyInfo
    ▷ algorithm (rsaEncryption)
      Padding: 0
      subjectPublicKey: 3082010a0282010100dd4b43722d7c0cece54f37a8b1b36e...
  ▷ extensions: 9 items
▷ algorithmIdentifier (sha256WithRSAEncryption)
  Padding: 0
```

□	Signature Name
□	Pokemon
☑	Pokemon1

Signature Name: Pokemon1

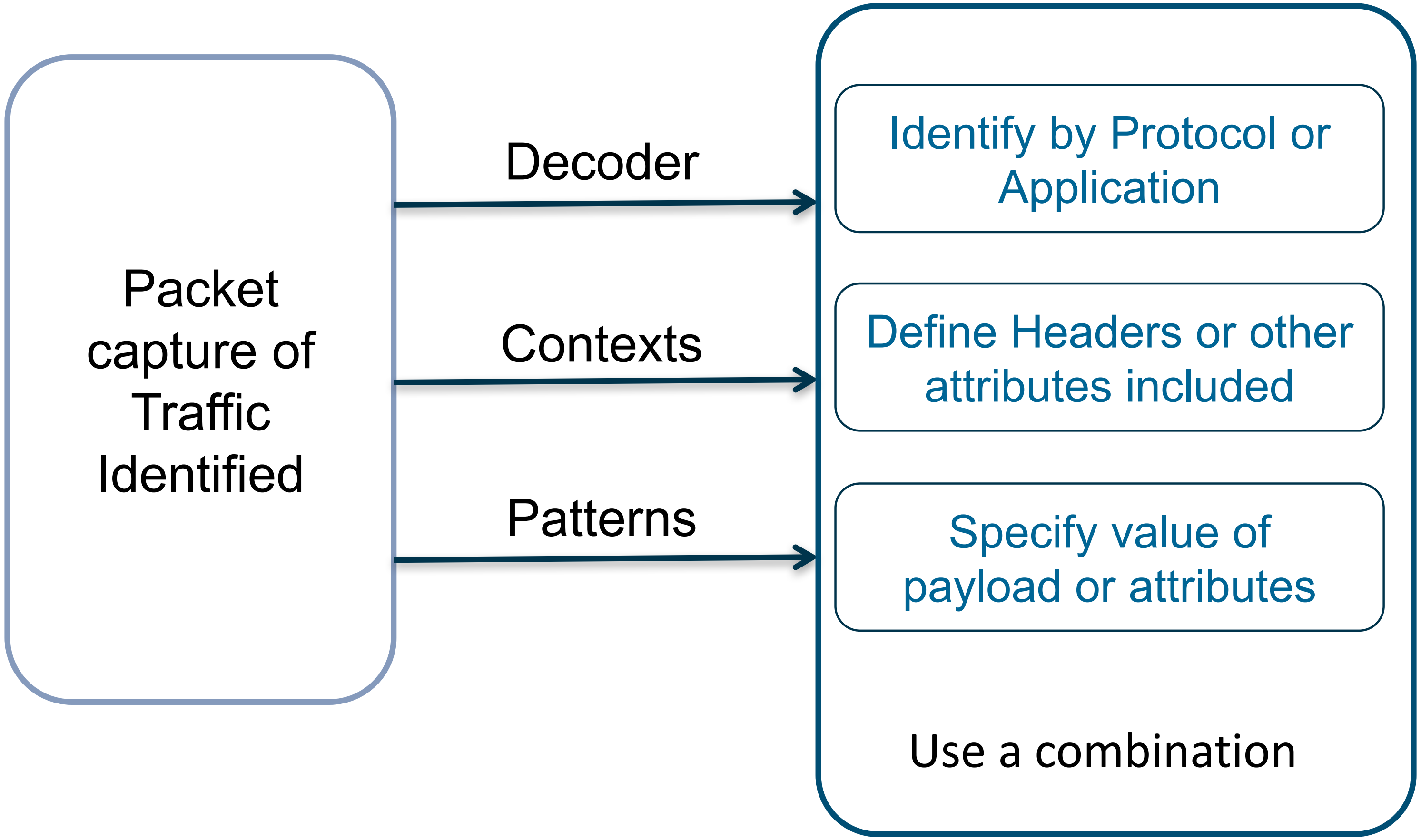
Comment:

Scope ● Transaction ○ Session

□ Ordered Condition Match

□	And Condition	Condit...	Operator	Context	Pattern	Qualifier
	▽ **And Condition 1**					
□	And Condition 1	Or Condit... 1	pattern-match	ssl-rsp-cert-subjectpublickey	3082010a02820...	

How do Custom App-IDs work?



Packet capture of Traffic Identified

Decoder

Contexts

Patterns

Identify by Protocol or Application

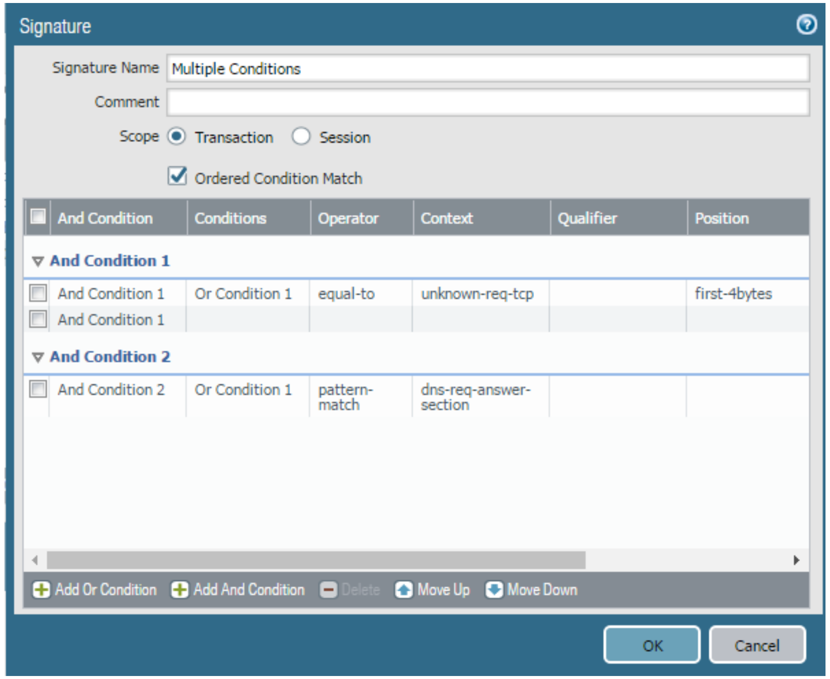
Define Headers or other attributes included

Specify value of payload or attributes

Use a combination

Terminology

- Scope
  - How signature is applied to traffic
  - **Transaction** (ex. HTTP request and response)
  - **Session** (ex. match on different requests within the same session)
- Ordered Condition Match
  - Useful when signatures have multiple conditions
  - Matches are done from top to bottom
- And / Or Conditions
  - Uses Boolean conditions
  - “And” = all conditions must match; used for narrow searches
  - “Or” = only one condition must match; used for broader searches



Signature

Signature Name: Multiple Conditions

Comment:

Scope: ● Transaction ○ Session

☑ Ordered Condition Match

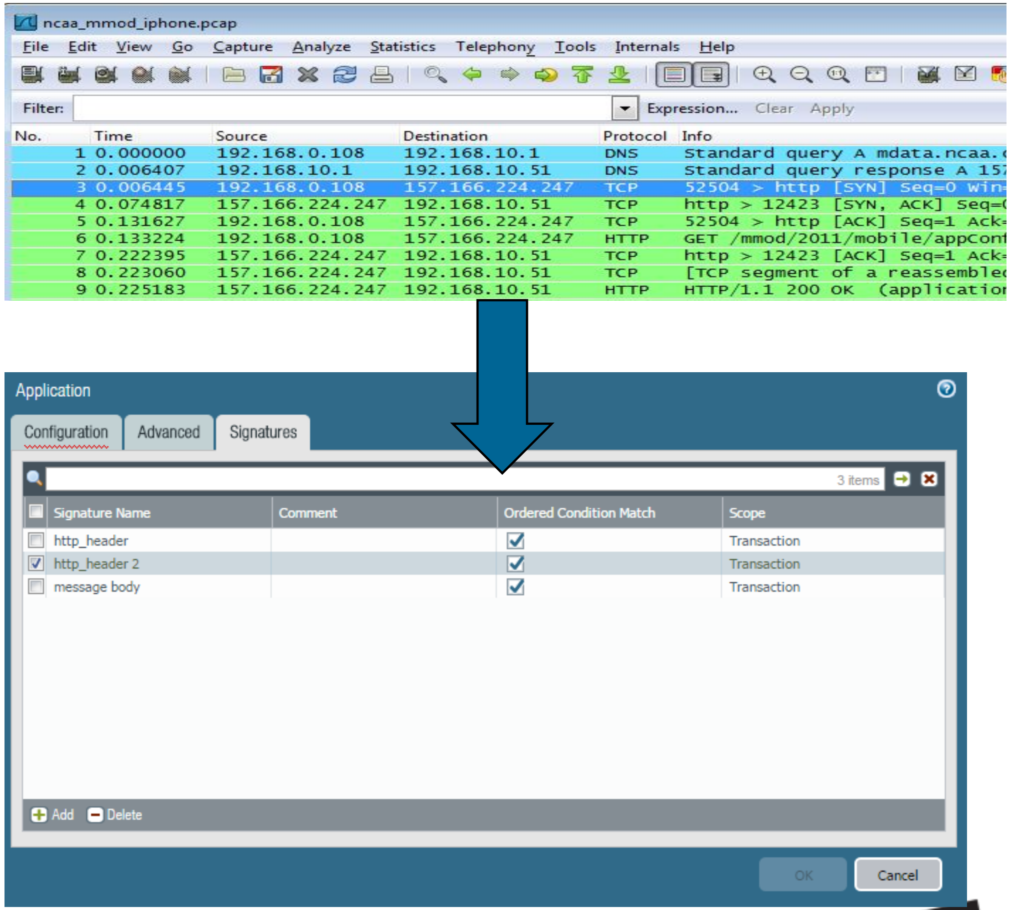
□	And Condition	Conditions	Operator	Context	Qualifier	Position
	▽ **And Condition 1**					
□	And Condition 1	Or Condition 1	equal-to	unknown-req-tcp		first-4bytes
□	And Condition 1					
	▽ **And Condition 2**					
□	And Condition 2	Or Condition 1	pattern-match	dns-req-answer-section		

Create a Custom App-ID

1. Capture comprehensive packet trace
   - Client-side and Server-side sessions
   - Capture Session Start

2. Find a unique identifier and create the signature
   - Protocol / Application (http)
   - Decoder context (http-req-headers)
   - Pattern (Chrome/)

3. Commit



ncaa_mmod_iphone.pcap
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.108	192.168.10.1	DNS	Standard query A mdata.ncaa.c
2	0.006407	192.168.10.1	192.168.10.51	DNS	Standard query response A 157
3	0.006445	192.168.0.108	157.166.224.247	TCP	52504 > http [SYN] Seq=0 Win=
4	0.074817	157.166.224.247	192.168.10.51	TCP	http > 12423 [SYN, ACK] Seq=0
5	0.131627	192.168.0.108	157.166.224.247	TCP	52504 > http [ACK] Seq=1 Ack=
6	0.133224	192.168.0.108	157.166.224.247	HTTP	GET /mmod/2011/mobile/appconf
7	0.222395	157.166.224.247	192.168.10.51	TCP	http > 12423 [ACK] Seq=1 Ack=
8	0.223060	157.166.224.247	192.168.10.51	TCP	[TCP segment of a reassembled
9	0.225183	157.166.224.247	192.168.10.51	HTTP	HTTP/1.1 200 OK (application

□	Signature Name	Comment	Ordered Condition Match	Scope
□	http_header		☑	Transaction
☑	http_header 2		☑	Transaction
□	message body		☑	Transaction