App-ID

EDU-210 Version A
PAN-OS® 9.0

IDENTIFY AND CONTROL APPLICATIONS

- Application identification (App-ID) overview
- Using App-ID in a Security policy
- Identifying unknown application traffic
- Migrating to an App-ID-based Security policy
- Updating App-ID

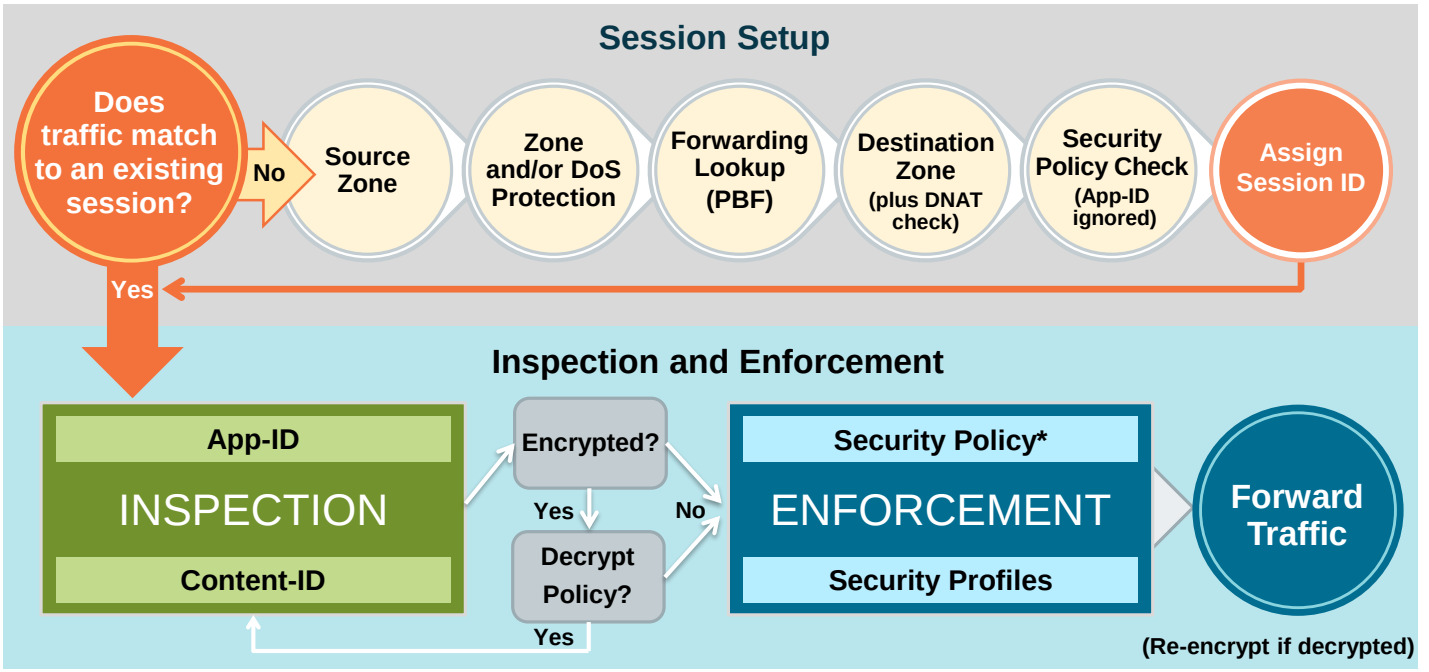
Agenda

After you complete this module, you should be able to:

- Define application identification
- Describe the four major technologies to help identify applications
- Configure application filters and application groups
- Detect unidentified applications traversing the firewall
- Migrate a port-based rule to an App-ID based rule
- Configure scheduling of updates to App-ID

After you complete this module, you should be able to:
- Define application identification
- Describe the four major technologies to help identify applications
- Configure application filters and application groups
- Detect unidentified applications traversing the firewall
- Migrate a port-based rule to an App-ID based rule
- Configure scheduling of updates to App-ID

Flow Logic of the Next-Generation Firewall



* Policy check relies on pre-NAT IP addresses

After the initial packet processing is complete, the Palo Alto Networks firewall examines the traffic to accurately apply the Security policy rules. Though the firewall can classify traffic by port as does a traditional firewall, the next-generation firewall is designed to examine the application associated with the traffic to provide more granular control over data on your network.

Application identification (App-ID) overview

Using App-ID in a Security policy

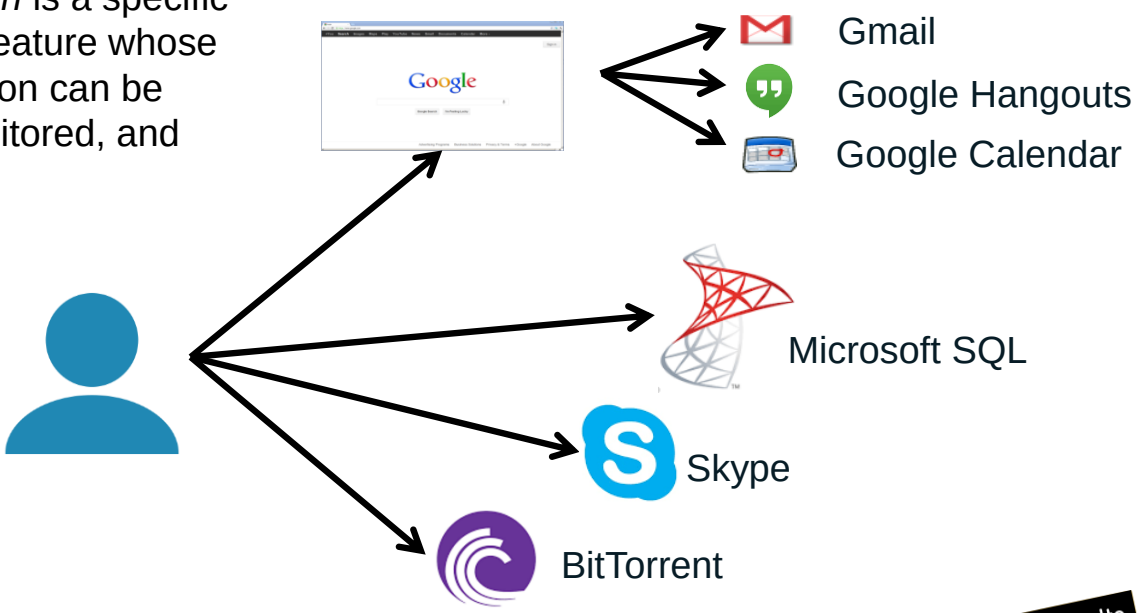
Identifying unknown application traffic

Migrating to an App-ID-based Security policy

Updating App-ID

What Is an Application?

- An *application* is a specific program or feature whose communication can be labeled, monitored, and controlled.



The term *application* does not have an industry-accepted definition in the way that *session* or *packet* does. In Palo Alto Networks terms, an application is a specific program or feature whose communication can be labeled, monitored, and controlled. Applications can be delivered through a web browser, a client-server model, or a decentralized peer-to-peer design.

Applications include business tools and services that must be allowed, and entertainment or personal services that might need to be blocked.

What Is App-ID?

- Multiple techniques to label traffic by application rather than just port

Port-based security rule

				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	FTP	egress	universal	inside	any	any	any	outside	any	any	service-ftp	Allow

Application-based security rule

				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	FTP	egress	universal	inside	any	any	any	outside	any	ftp	application-default	Allow

App-ID uses multiple identification mechanisms to determine the exact identity of applications traversing the firewall.

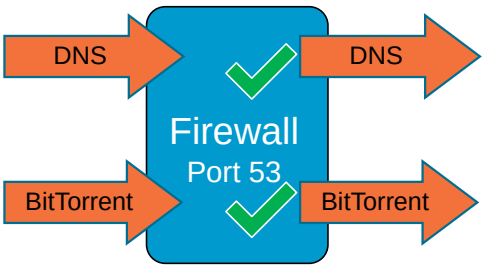
Accurate traffic classification is the primary function of any firewall, with the result becoming the basis of the Security policy. Security rules within a Palo Alto Networks firewall can specify applications to allow or block. Traditional firewalls classify traffic by port and protocol, which at one point was a satisfactory mechanism for securing the network perimeter. However, today's applications can easily bypass a port-based firewall by hopping ports, using SSL and SSH encrypted traffic, sneaking across port 80, or using non-standard ports. App-ID is the Palo Alto Networks traffic classification mechanism that addresses the traffic classification limitations that plague traditional firewalls.

In the example, the port-based Security policy rule allows any traffic from the private zone to the public zone as long as it is going to ports 20 and 21 (as defined in the service service-ftp). The actual traffic might or might not be FTP traffic. The application-based Security policy rule allows only FTP traffic from the private zone to the public zone that is going to ports 20 and 21 (as defined by the service setting of application-default).

Port-Based Versus Next-Generation Firewalls

Traditional Firewalls

Firewall Rule: ALLOW Port 53



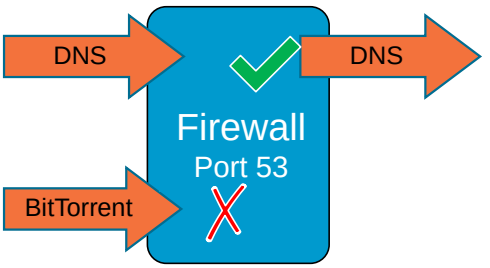
Packet on port 53: Allow

Packet on port 53: Allow

Visibility: Port 53 allowed

Palo Alto Networks Firewalls with App-ID

Firewall Rule: ALLOW DNS



DNS = DNS: Allow

BitTorrent ≠ DNS: Deny

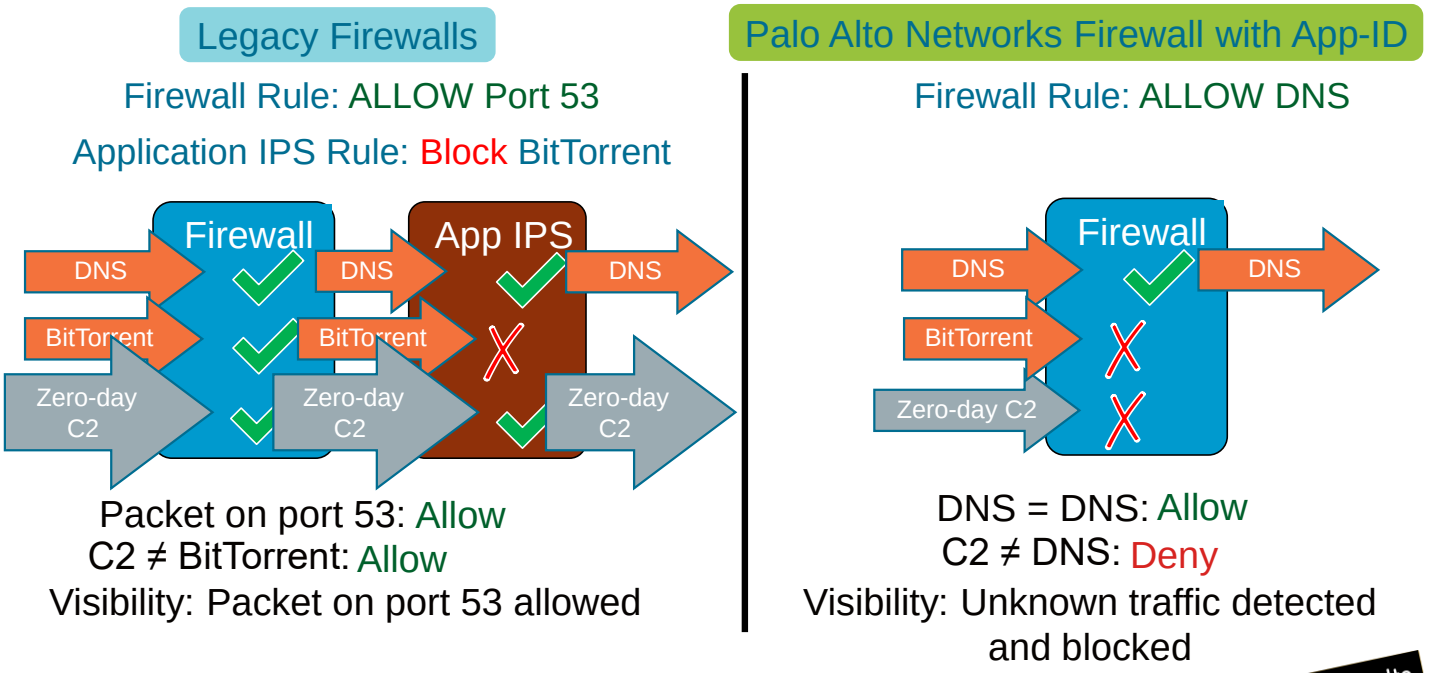
Visibility: BitTorrent detected and blocked

Traditional firewalls use port blocking to control traffic. To allow a service such as DNS that uses port 53, the traditional firewall is configured to allow port 53 traffic.

The Palo Alto Networks next-generation firewall is configured to allow the DNS service. If you configure the firewall Security policy rule to use the *application-default* port, then the firewall allows only DNS traffic on port 53 and denies all other non-DNS traffic on this port. In this way, the Palo Alto Networks firewall protects the network from evasive applications that switch ports or use non-standard ports.

This protection is not available on a network protected by a traditional port-based firewall. On a port-based firewall, DNS would be allowed on port 53, but so would other evasive applications attempting to use port 53, such as BitTorrent in the example here. In such an environment the network would be completely unprotected.

Zero-Day Malware: IPS Versus App-ID

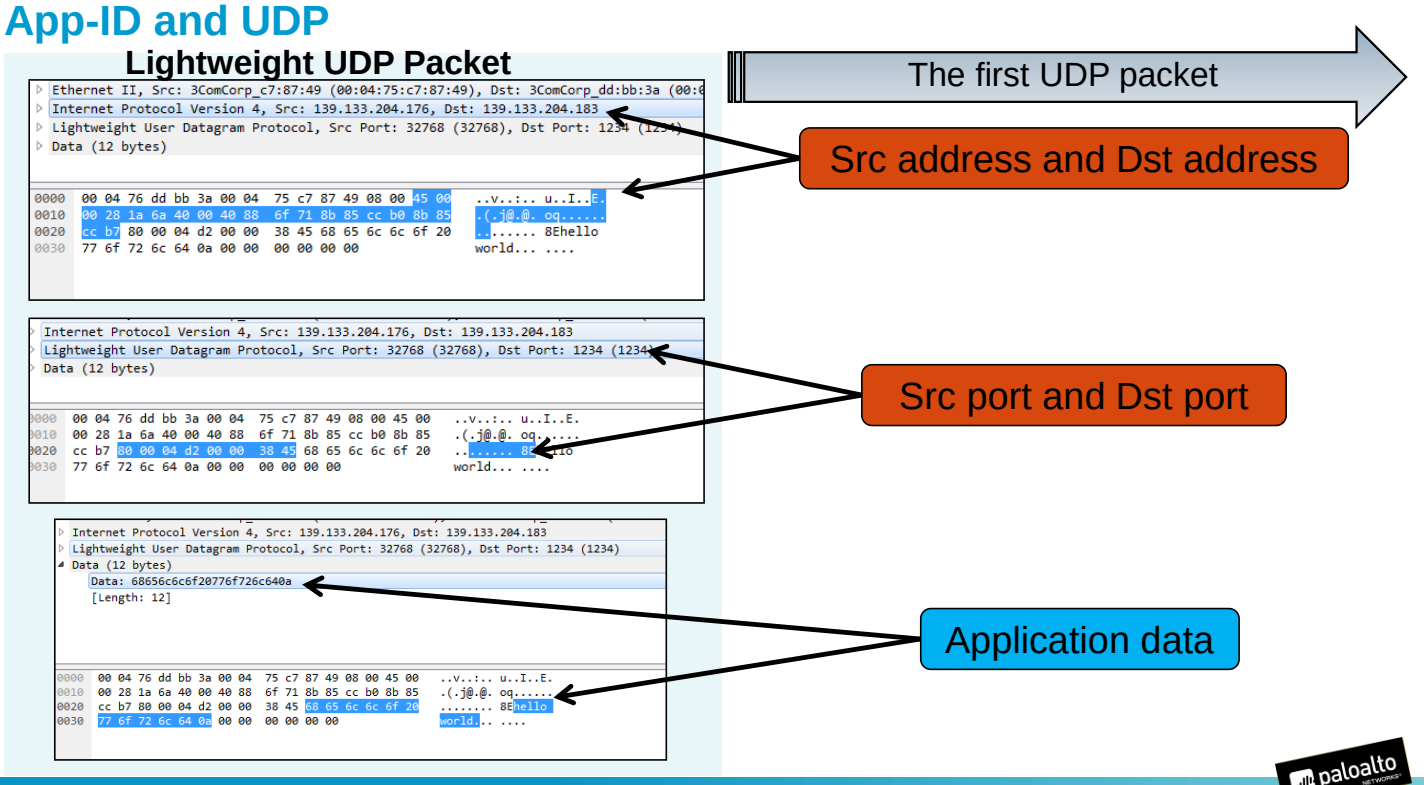


The previous example described a well-behaved, known threat. The situation changes if the threat is unknown, like a zero-day virus.

In the application IPS blade server example, the zero-day virus using port 53 is allowed through the firewall because it is using an allowed port and it is not BitTorrent. The unknown traffic is allowed by the IPS because it has not been specifically blacklisted by the IPS. This problem is inherent with application block policies; the device cannot block what the device does not know. Not only does the zero-day malware get through, but also no logs are generated to identify this occurrence.

The Palo Alto Networks firewall is configured to allow only DNS application traffic. Even if the zero-day malware is unknown to PAN-OS® software, it still is not allowed to pass because it has not been specifically identified as the DNS application. Also, the blocked traffic is logged, making the occurrence known for further analysis.

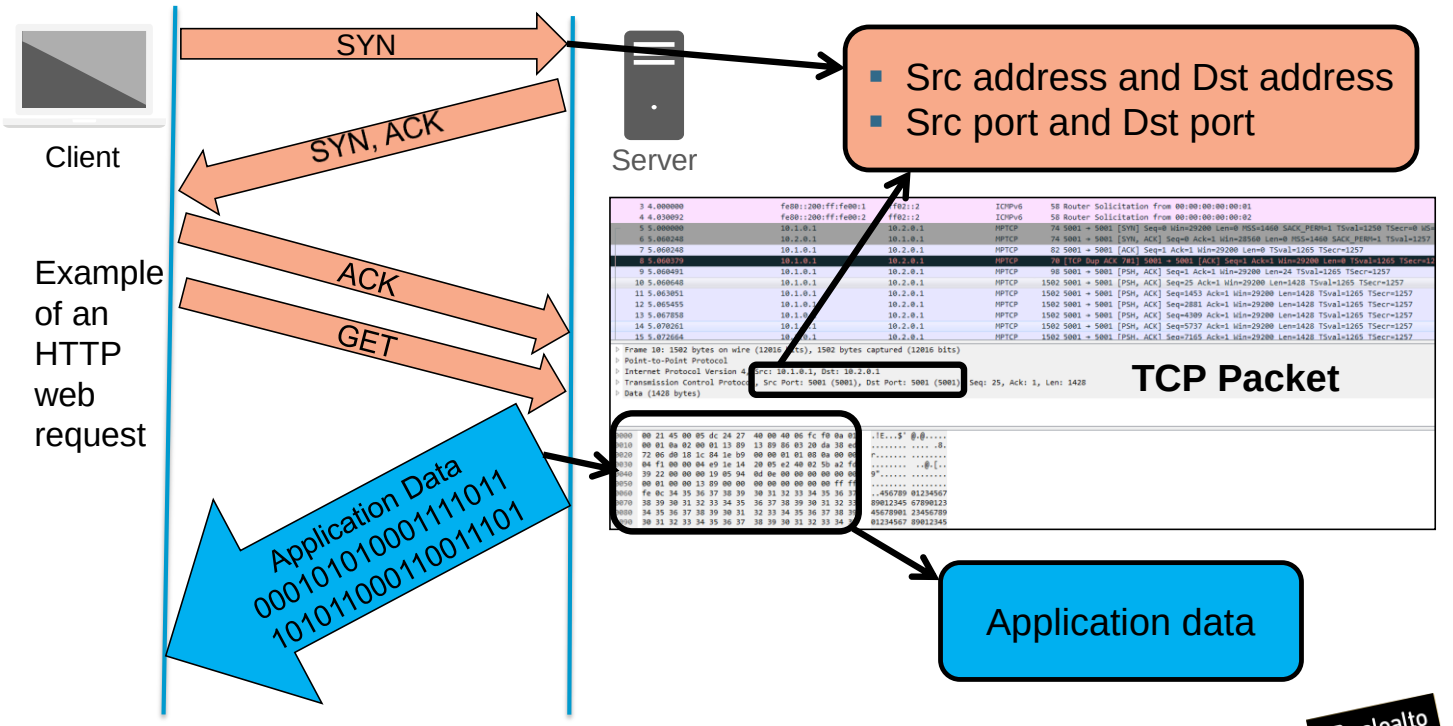
App-ID and UDP



A Palo Alto Networks firewall examining UDP packets often must examine only a single UDP packet to identify the application. In most cases, all the information that the firewall needs is contained in the first packet. This example shows a single Lightweight UDP packet. The packet contains all source and destination addressing information. It also includes the application data that will be used to identify the traffic so that it can be processed by the Security policy.

Note: The Lightweight User Datagram Protocol (UDP-Lite) is very similar to UDP, but it also can serve applications in error-prone network environments that prefer to have partially damaged payloads delivered rather than discarded. When this feature is not used, UDP-Lite is basically identical to UDP.

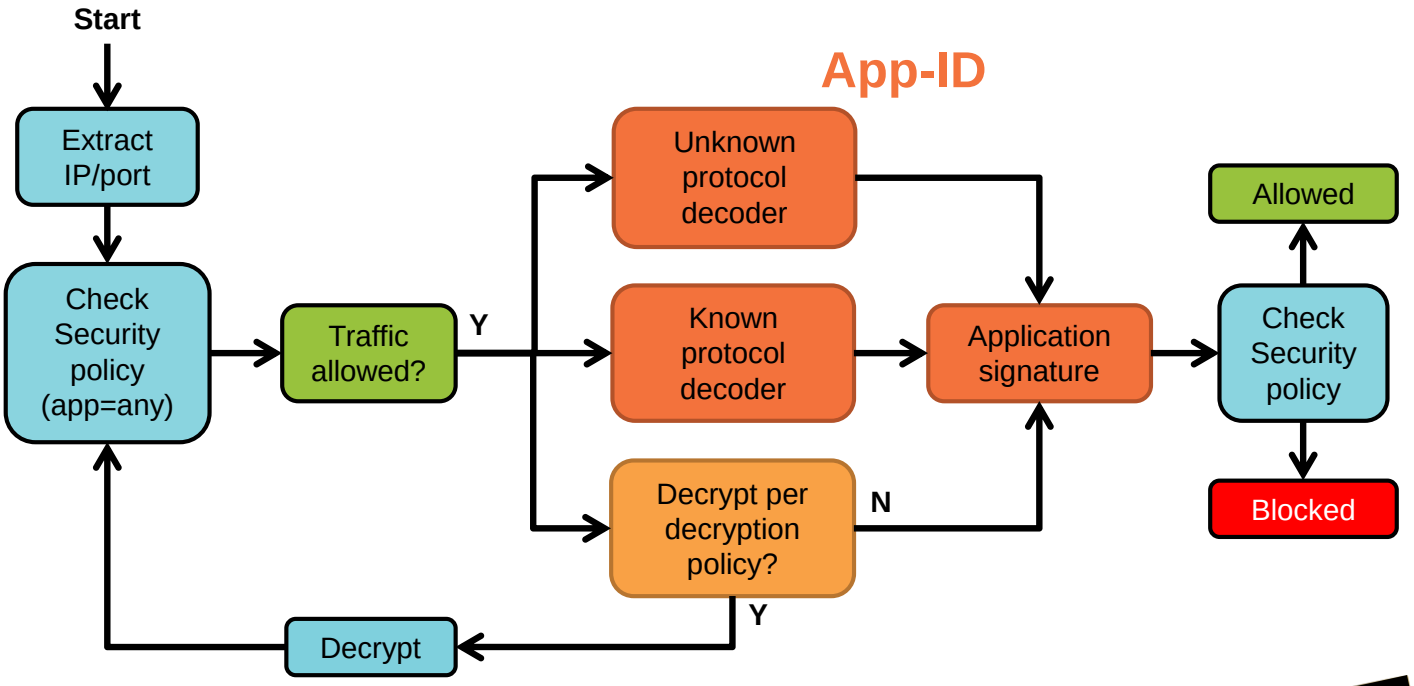
App-ID and TCP



Applications that use TCP usually require multiple packet transfers to identify an application. This example shows an HTTP connection request. The first packet is a TCP SYN packet. Though the first packet does contain the source and destination addresses and ports, it contains no application data. In fact, the next two packets just complete the required TCP three-way handshake and do not contain any application data.

The application data could reside in either the client's HTTP Get request or in the server's reply. For this reason, the firewall might have to examine the fifth packet, for example, before App-ID can detect either the application or the presence of encrypted traffic. If the traffic is encrypted, the firewall must evaluate the administrator-defined Decryption policy to determine what to do next. Depending on the configured policy, the traffic could be allowed or blocked in either encrypted or decrypted form. Decryption is described in the "Decryption" module.

App-ID Operation



Palo Alto Networks App-ID uses four major technologies to help identify applications:

- Application signatures: A database of application signatures updated as part of the firewall content updates
- Unknown protocol decoder: An App-ID heuristics engine used to look at patterns of communication. It attempts to identify the application based on its network behavior. For example, this type of detection is required for applications that use proprietary end-to-end encryption, such as Skype and encrypted BitTorrent.
- Known protocol decoders: A set of application decoders that understand the syntax and commands of common applications
- Protocol decryption: SSL and SSH decryption capabilities

Network traffic is first classified based on its IP address and port. The firewall consults the Security policy to determine if it should allow or block the traffic based on IP address and port. During this initial Security policy check, the application is set to any. If the traffic is allowed, then a session is created and App-ID then looks for an application signature. The firewall uses its known protocol and unknown protocol decoders to identify the application.

If App-ID determines that either SSL or SSH encryption is in use and a Decryption policy is configured, the traffic flow could be decrypted and the unknown and known protocol decoders could be applied to the decrypted traffic to detect an application signature. If the traffic is not decrypted, then the traffic would be identified as the SSH or SSL application. If an application signature cannot be identified, the traffic can be labeled as unknown-tcp or unknown-udp.

After an application has been identified, the firewall checks the Security policy to determine whether to block, allow, or allow and scan for threats.

Application identification (App-ID) overview

Using App-ID in a Security policy

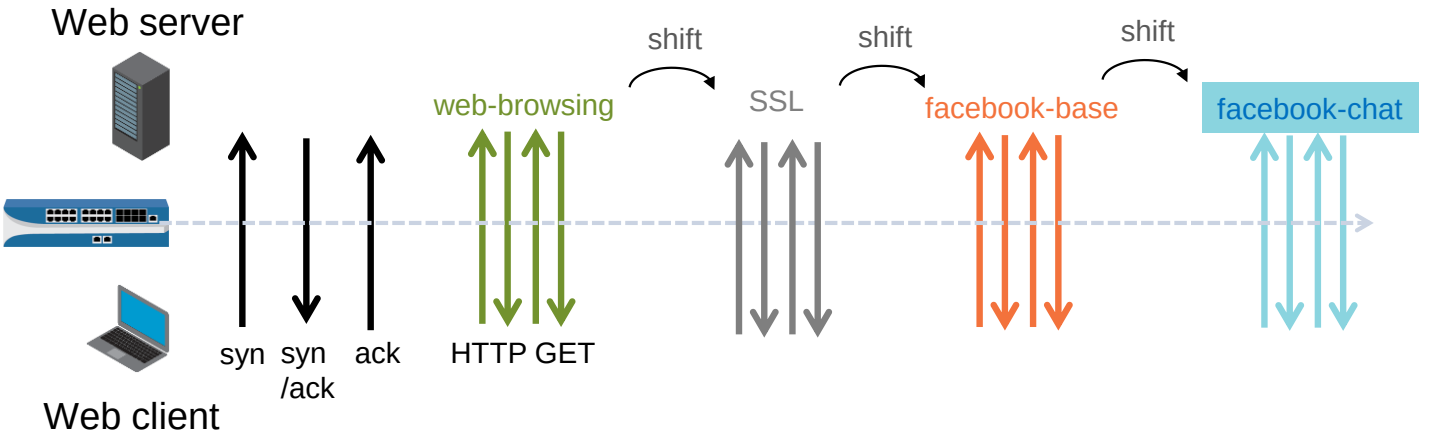
Identifying unknown application traffic

Migrating to an App-ID-based Security policy

Updating App-ID

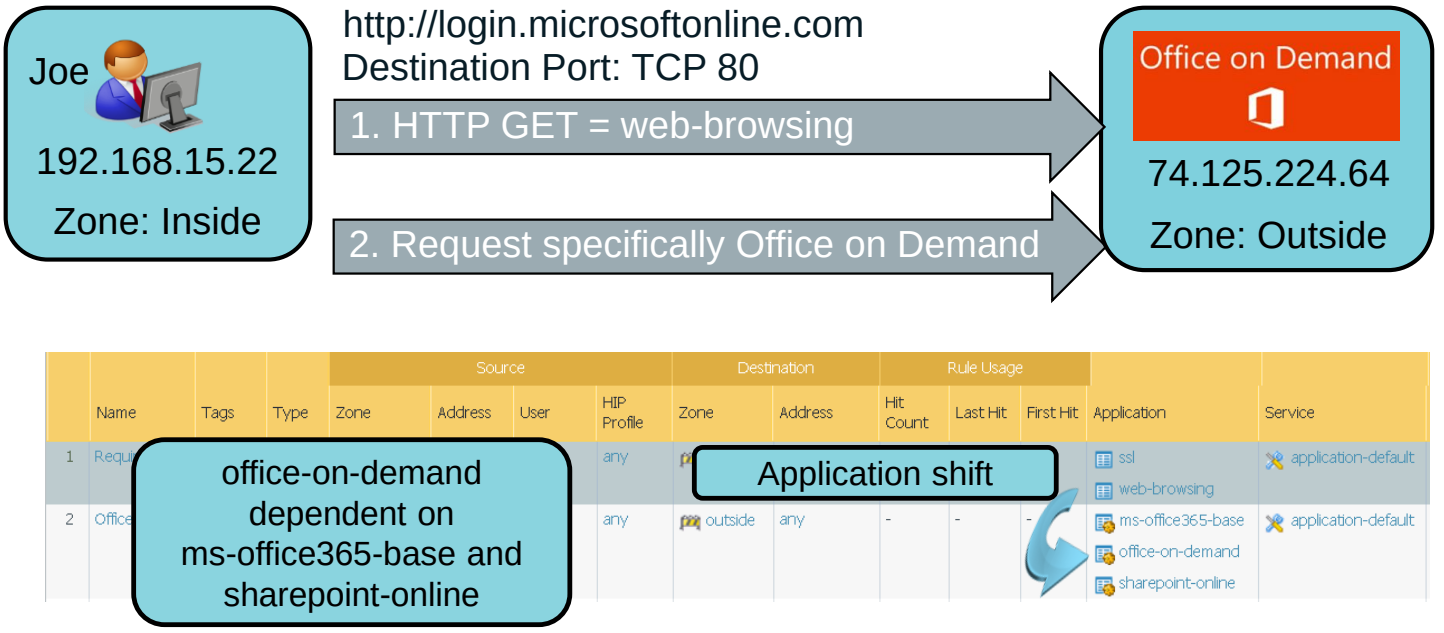
Application Shifts

- Network traffic can shift from one application to another during a session.



Network traffic can shift from one application to another during the lifetime of a session. In the illustration, App-ID cannot identify the traffic from only a TCP syn packet. Even after the TCP three-way handshake has completed, the firewall would report insufficient-data rather than an application name. However, when an HTTP GET is detected, App-ID can report the application as web-browsing. As more packets are received, App-ID might be able to further classify the traffic. In the illustration, the traffic is further identified as facebook-base and then facebook-chat.

Dependent Applications



Some applications can depend on one or more other applications. Network traffic can shift from one dependent application to another during the lifetime of a session. For this reason, when you create a policy to allow dependent applications, you also ensure that the firewall allows the other applications on which the application depends.

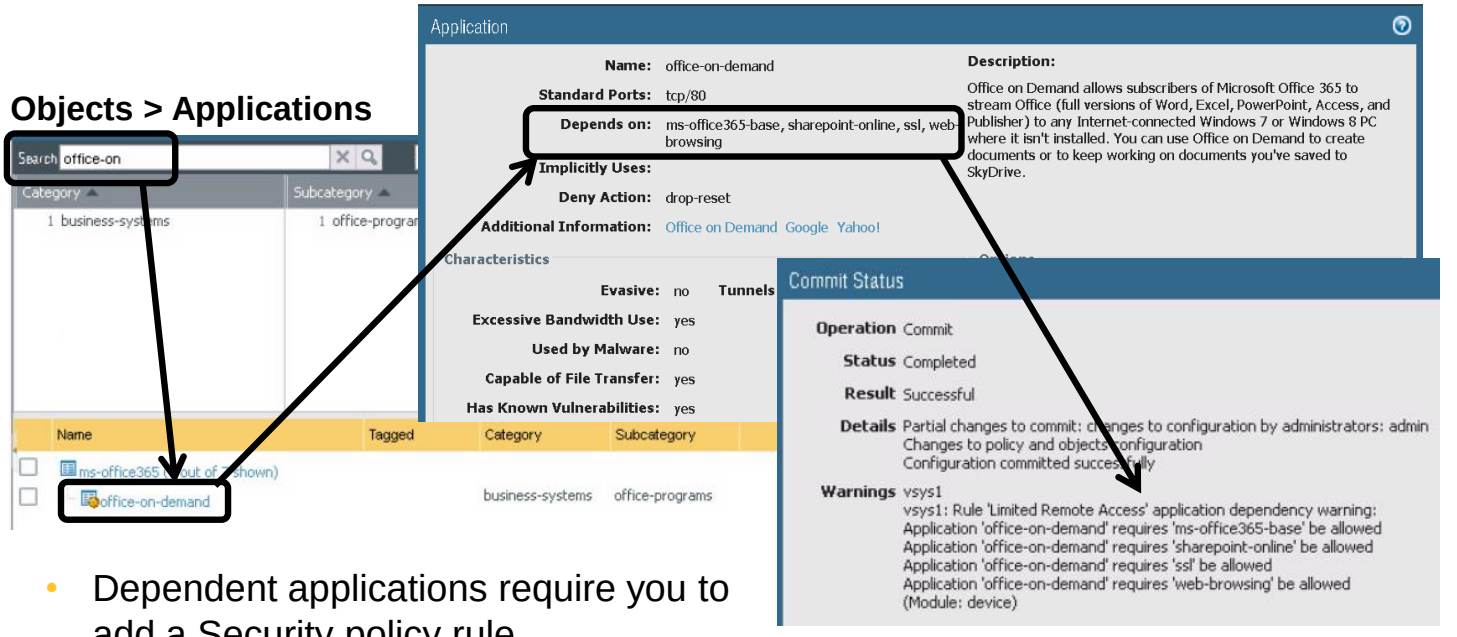
In this example, user Joe in one zone wants to access Office on Demand in another zone. App-ID scans the traffic and finds an HTTP GET, which matches the web-browsing application. The first rule is matched and the HTTP connection is allowed. The Office 365 rule is not checked at this time because a matching rule already has been found.

Because Security policy rules are examined for every packet, the firewall can detect application shifts within an established session. When Joe tries to access Office on Demand, an application shift in the current session is initiated. The App-ID engine detects the shift and finds the application signature for office-on-demand.

The Office on Demand application does not match the first rule, so the firewall moves on to the next rule. The second rule matches, so Office on Demand is allowed to run. However, the Office on Demand application depends on the ms-office365-base and sharepoint-online applications, so they are included in the rule.

Does the order of the two rules matter in this example? In this example, the order is not relevant. Traffic that matches one rule cannot match the other rule, so neither rule prevents the other from being evaluated.

Determining Application Dependencies



- Dependent applications require you to add a Security policy rule.

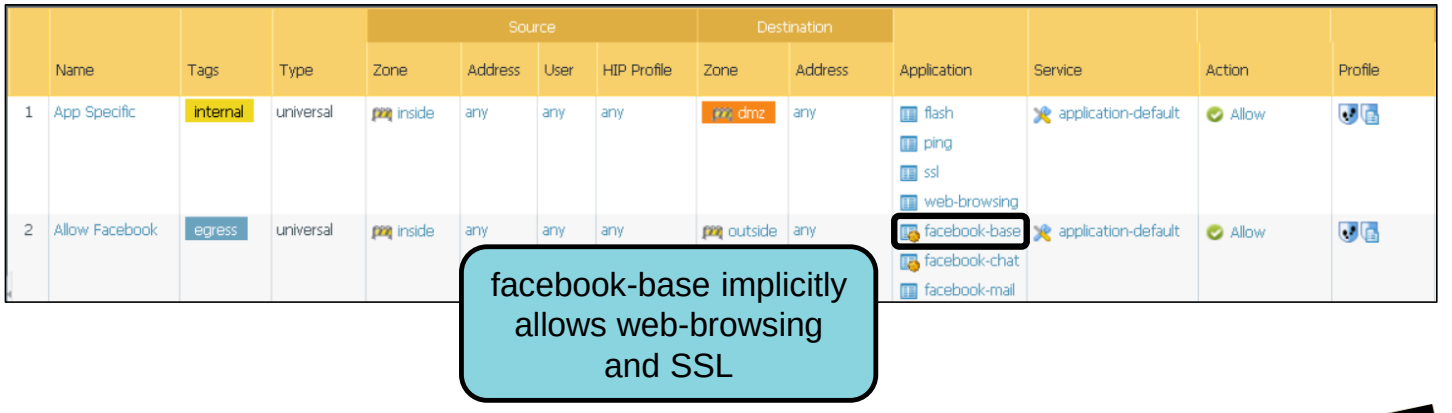
Palo Alto Networks maintains a database of known application signatures for use in the App-ID engine. Each signature covers multiple versions of an application. Application dependencies are among the items listed in the App-ID database.

To display application dependencies in the web interface, select **Objects > Applications**. Application dependency information also is available in Applipedia at http://applipedia.paloaltonetworks.com. In either the web interface or Applipedia, find and select an application and look for the **Depends on** field. For a firewall to be able to pass application traffic, any applications listed in its **Depends on** field also must be allowed by the Security policy.

In the example, notice that the four applications listed in the **Depends on** field must be allowed explicitly on the firewall for use of the application Office on Demand. Therefore, you must create a rule to allow these applications within your Security policy configuration. If the application that another application depends on is not allowed in the Security policy, you will receive warnings when you commit the configuration.

Implicit Applications

- Many common applications implicitly allow parent applications.
- No explicit Security policy rule is required for a parent application.



For many dependent applications, the App-ID database implicitly allows the required parent application without the need for you to explicitly add the parent application to the Security policy. In the example, the facebook-base application implicitly allows the required web-browsing application without the need for you to explicitly add a web-browsing rule to the Security policy. The facebook-chat and facebook-mail depend on facebook-base, so facebook-base explicitly must be added to the rules to enable users to chat or email using Facebook.

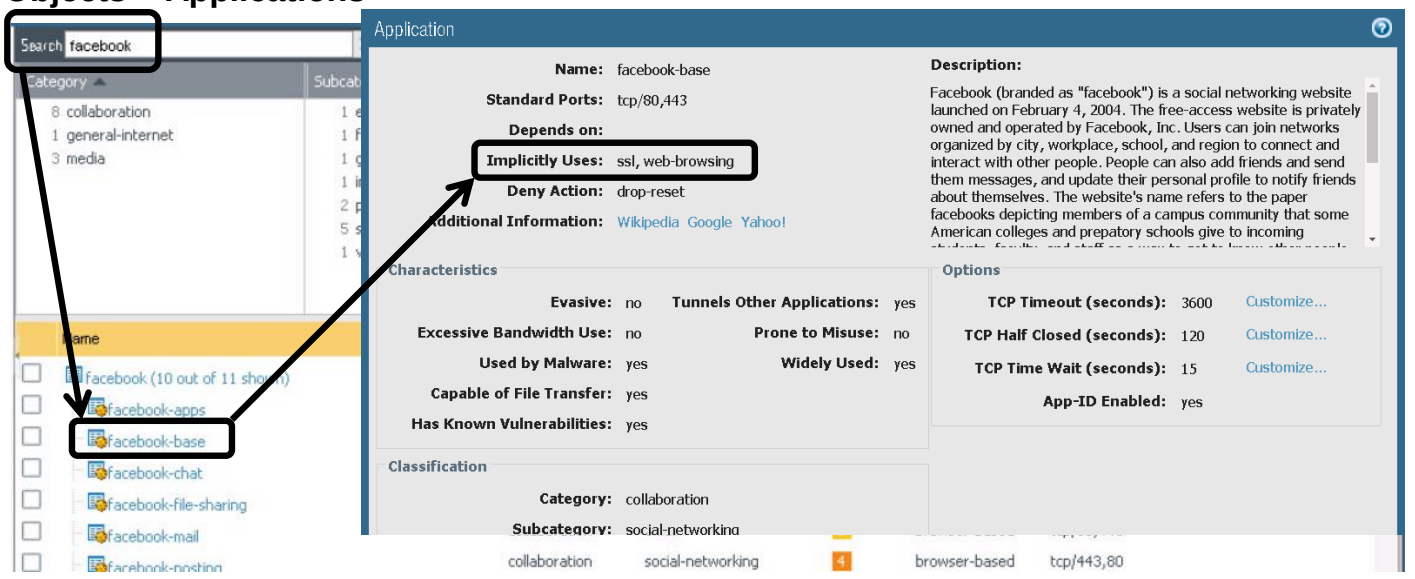
App-ID defines implicit dependencies because the addition of parent applications to a rule in the Security policy could allow more traffic than intended. For example, enablement of web-browsing just to allow facebook-base would allow users to browse other websites. An administrator would have to configure additional Security policy rules to control other website access. Security policy administration is simplified when App-ID implicitly allows parent applications.

Implicit permissions for a parent application are processed only if you have not added an explicit Security policy rule for the parent application.

This implicit support also applies to administrator-defined custom applications that are based on HTTP, SSL, MS-RPC, or RTSP.

Determining Implicitly Used Applications

Objects > Applications

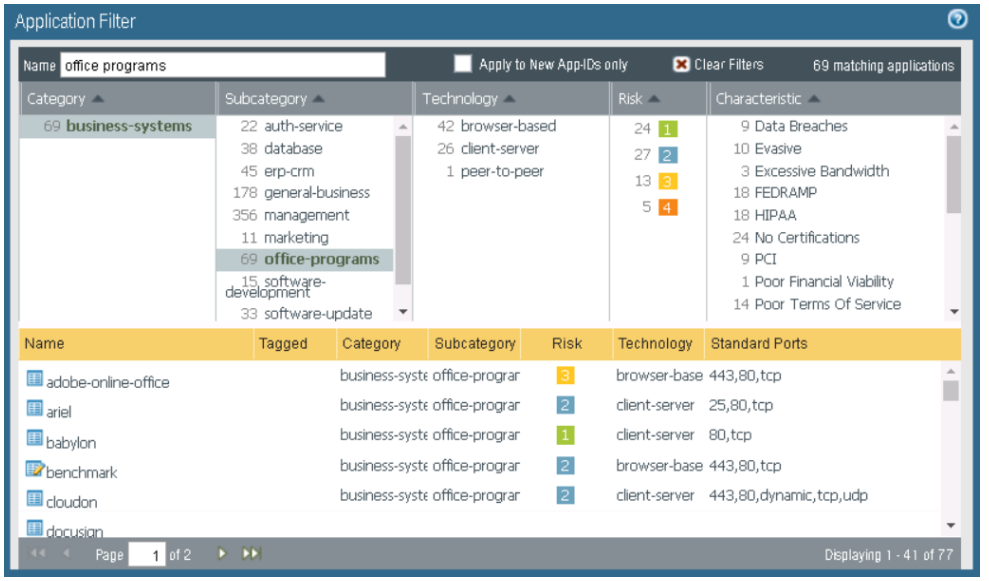


You can determine implicit application dependencies using the firewall web interface or the Applipedia website. In the web interface or Applipedia, find and select an application and look for the **Implicitly Uses** field, which lists any implicitly allowed parent applications.

In this example, facebook-base implicitly allows the parent applications ssl and web-browsing.

Application Filter

Objects > Application Filter > Add



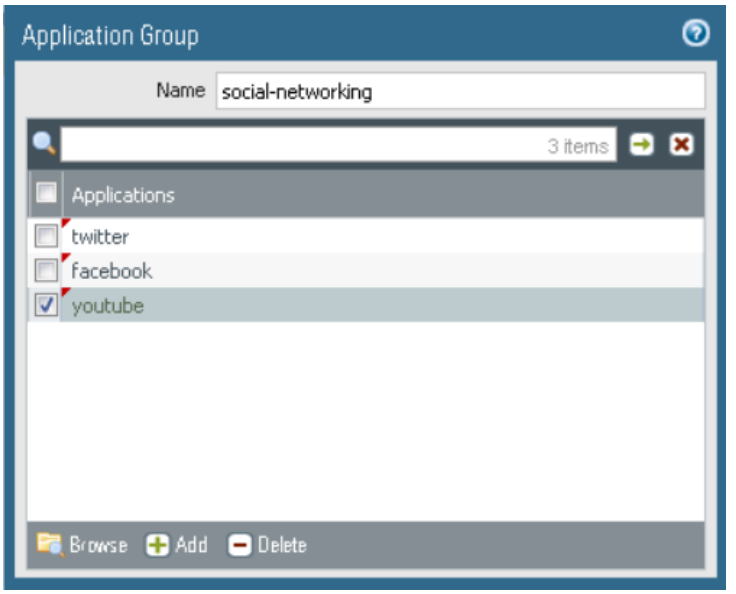
- Dynamic grouping of applications
- Created by selecting filters in the App-ID database
- Used to simplify Security, QoS, and PBF policy rulebases

An application filter is an object that dynamically groups applications based on application attributes that you select from the App-ID database. The selectable attributes are **Category**, **Subcategory**, **Technology**, **Risk**, and **Characteristic**. Application filters are useful when you want to enable access to applications that match filter criteria rather than match specific application names. For example, you might want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To enable these types of applications, create an application filter that matches on the **Category** business-systems and the **Subcategory** office-programs, as shown in this example.

New applications added by Palo Alto Networks to the App-ID database are classified by **Category**, **Subcategory**, **Technology**, **Risk**, and **Characteristic**. Any new applications automatically will match the application filter you define and will be added dynamically to the dynamic application group. The use of dynamic application groups also simplifies firewall administration because changes to a dynamic group do not require a firewall commit.

Application Groups

Objects > Application Groups > Add



- Static, administrator-defined sets of applications
- Used to simplify Security and QoS policy rulebases

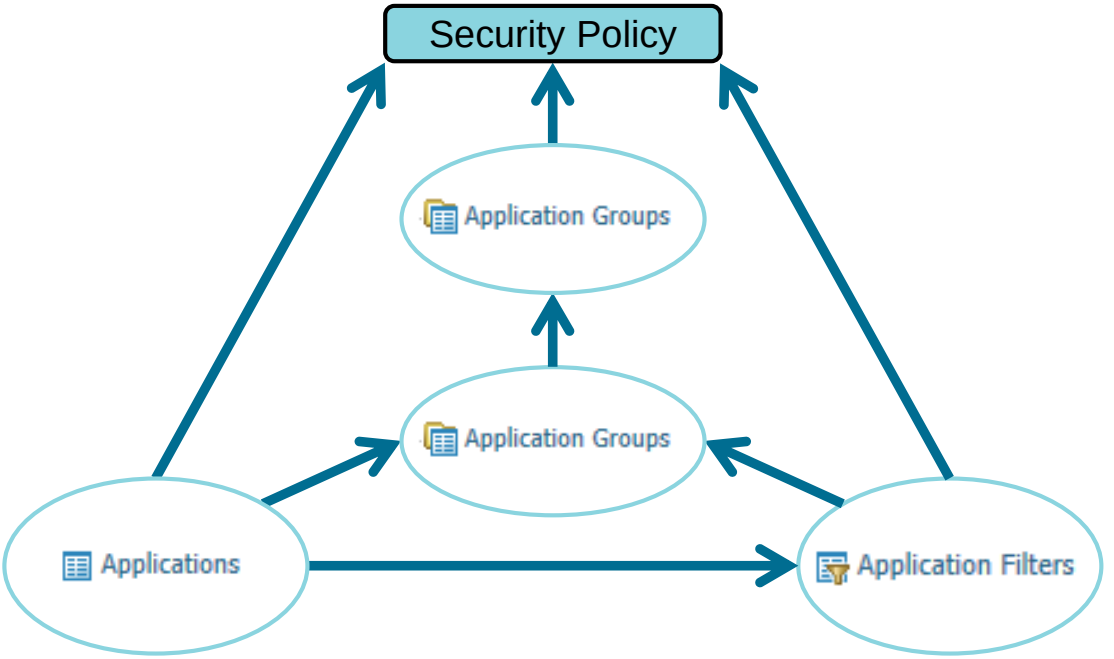
An application group is a static, administrator-defined set of applications. Application groups enable you to create a logical grouping of applications that can be applied to Security and QoS policy rules.

An application group is used when you want to treat a set of applications similarly in a policy. Application groups ultimately simplify administration of your rulebases. Instead of you adding the same list of applications to multiple rules, you can create an application group and add the group to multiple rules. You still must issue a firewall commit after updating an application group.

When you plan for application groups, consider how you want to enforce access to your applications and create separate application groups for each type of access. For example, you might have some applications that you allow only your IT administrators to access, and other applications that you want to make available for any known user in your organization. In this case, you create separate application groups for each of these policy goals.

As another example, although it is best practice to enable only default port access to applications, you might want to group applications that are an exception to this practice and enforce access to those applications in a separate rule.

Nesting Application Groups and Filters

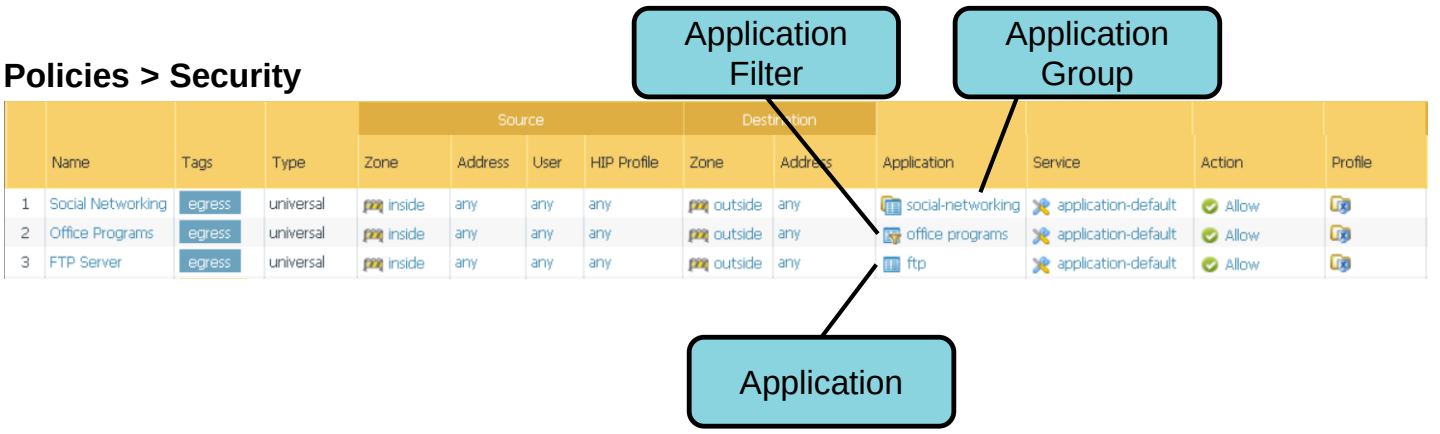


An application group is manually configured to include applications, application filters, and other applications groups. The diagram illustrates the possible ways that application groups and filters can be nested.

You can configure firewall policy rules, including the Security policy rules, to match specific applications, application filters, and application groups.

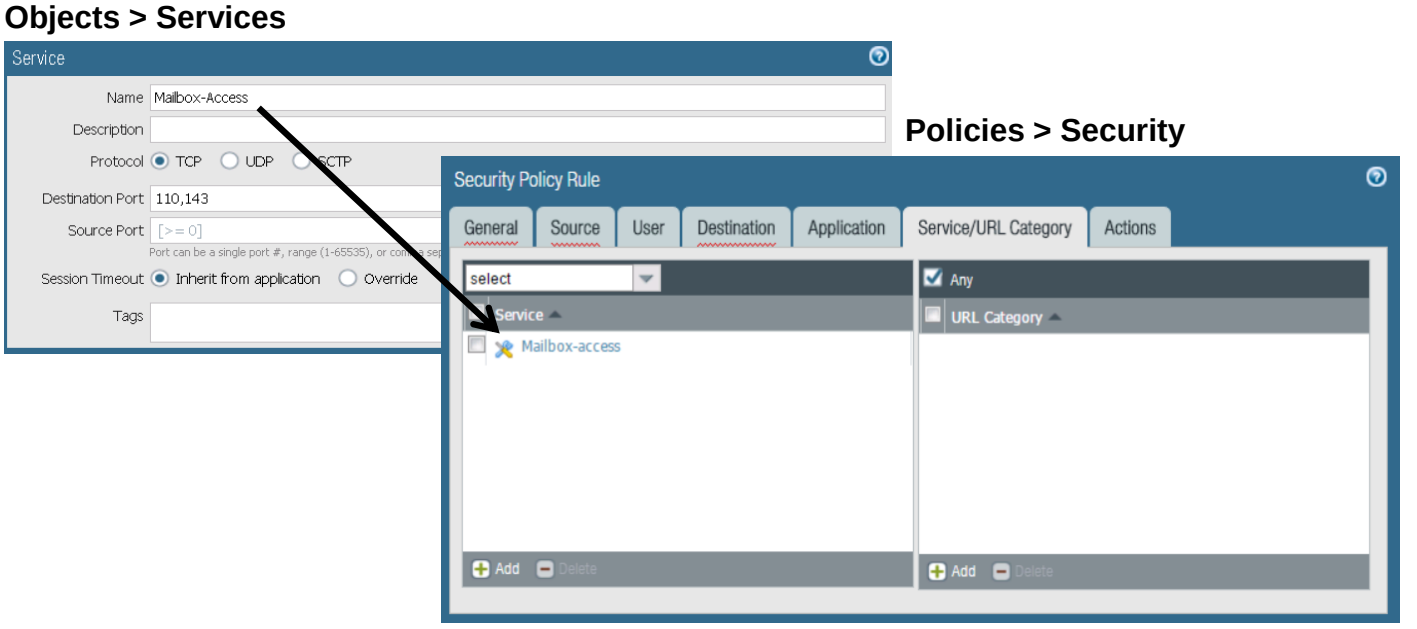
Applications and Security Policy Rules

Policies > Security



Application filters and groups are added to the Security policy rules just as single applications are. They can be used to either allow or deny applications.

Creating and Using Custom Services



Security policy rules on a PAN-OS® firewall match source zone, destination zone, application, and service. The **Application** and **Service/URL Category** tabs specify which applications can be allowed or blocked, and on which port or ports. The services service-http and service-https are the only predefined services. Custom services can be created using **Objects > Services**. In the example, a custom Mailbox-access service is defined and TCP traffic associated with this service is expected only on TCP ports 110 and 143.

The **Service** column in a Security policy rule enables you to select one of these options:

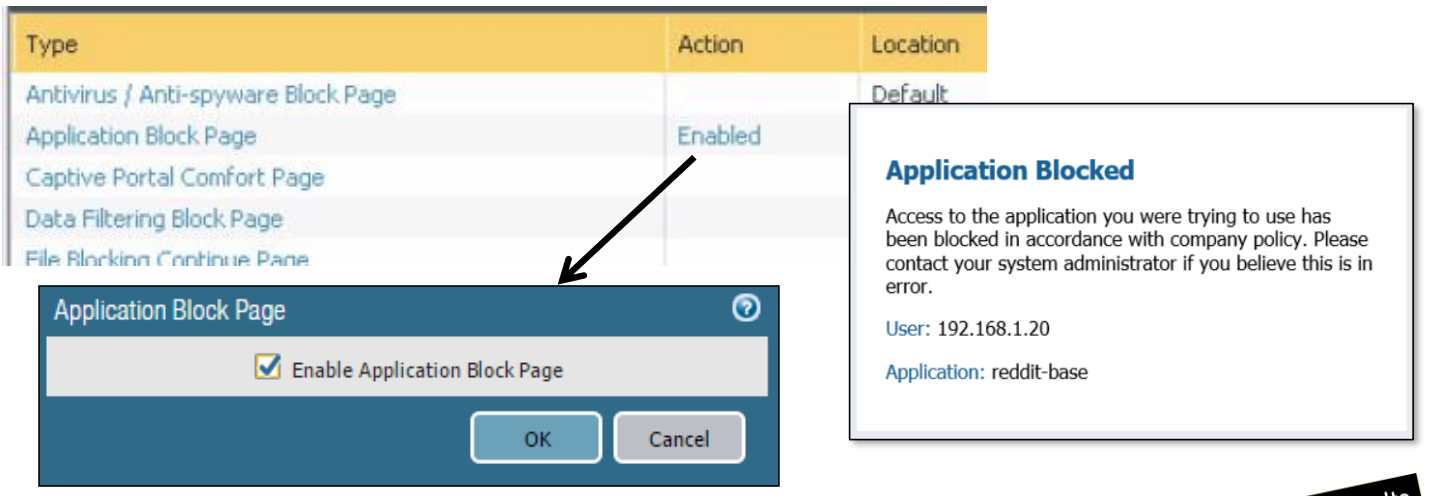
- application-default: This option configures the Security policy to allow an application on only the standard ports defined for the application in the App-ID database.
- service-http or service-https: These predefined services use TCP ports 80 and 8080 for HTTP, and TCP port 443 for HTTPS. Use this Security policy setting if you want to restrict web browsing and HTTP or HTTPS to only these ports.
- any: This option matches any TCP or UDP port. This service typically is used to deny applications.
- select: This option enables an administrator to choose one or more services, even custom services created using **Objects > Services**.

Palo Alto Networks recommends that you use the service application-default when you configure a Security policy rule.

Application Block Page

- For blocked web-based applications, a response page can be displayed in the user's browser.

Device > Response Pages



If the **Application Block Page** is enabled and a Security policy rule denies a web-based application, then a browser-based response page is displayed. The default response page includes the prohibited application name and the user's name if the User-ID feature has been configured. If User-ID has not been configured, then the user's name appears as an IP address. Application block response pages must be enabled using an Interface Management Profile.

The generic response page might result in additional support calls if users do not correctly interpret the message. You can create and upload a custom HTML response page. For more information about creating custom response pages, use the web interface's online help or the *PAN-OS 9.0 Administrator's Guide* at https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html.

Application identification (App-ID) overview

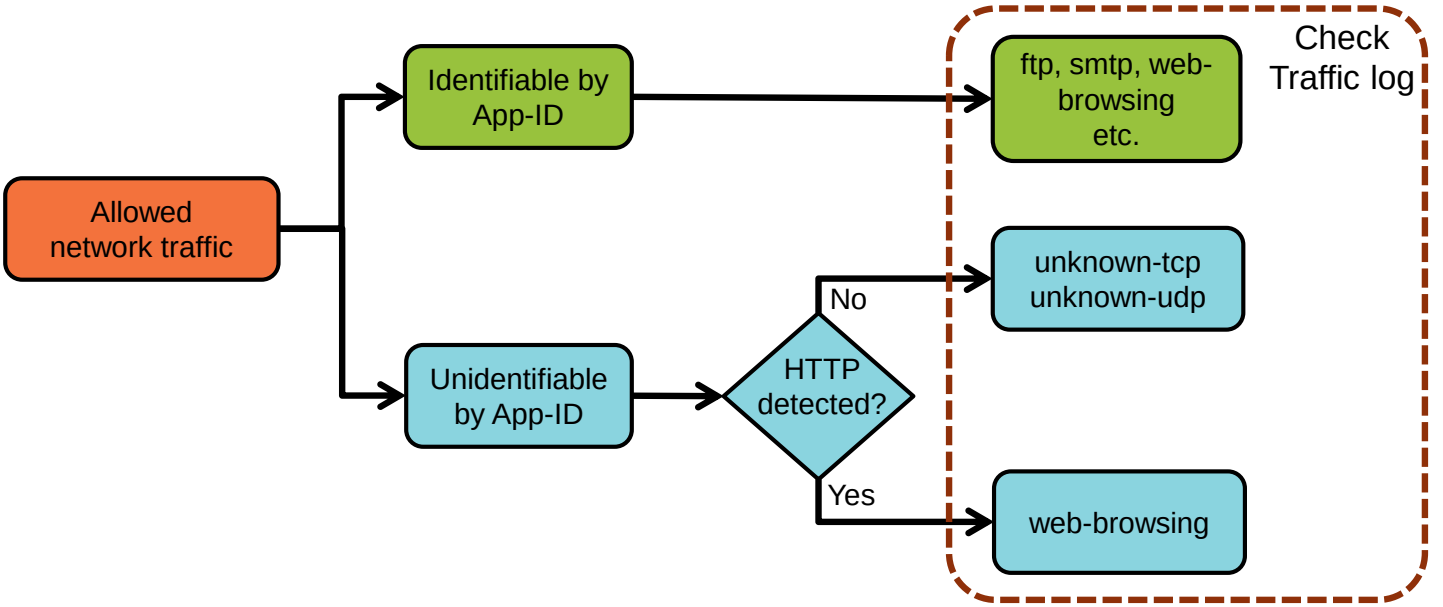
Using App-ID in a Security policy

Identifying unknown application traffic

Migrating to an App-ID-based Security policy

Updating App-ID

Unknown Network Traffic



When you add a Palo Alto Networks firewall to your network, one of the first tasks is to identify your network traffic. Because the Palo Alto Networks firewall is not a port-based firewall, identification of traffic means identification of the applications traversing your firewall. An application can be classified in one of two main categories: applications known to App-ID and applications unknown to App-ID.

Applications known to App-ID are named in the Traffic log, viewable at **Monitor > Logs > Traffic**. For example, an application could be identified as ftp or smtp. An application that uses HTTP initially might be classified as web-browsing, but as more packet data becomes available the application could be more specifically identified, for example, as google-docs-base.

When App-ID cannot identify an application, the traffic can be identified as unknown-tcp or unknown-udp. One exception to this identification is when the traffic contains HTTP. Such traffic is identified generically as web-browsing.

Identify Unknown Application Traffic

Iterative process:

- Create rules to allow or block applications known to be traversing the firewall
- Create a *temporary* rule to detect unidentified applications traversing the firewall
- As applications are identified, create specific rules to allow or block them

Policies > Security

	Name	Tags	Type	Source				Destination		Application	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address			
1	Known Good	egress	universal	any	any	any	any	any	any	known good	application-default	Allow
2	Known Bad	egress	universal	any	any	any	any	any	any	known bad apps	application-default	Deny
3	Unclassified Apps	egress	universal	any	any	any	any	any	any	any	any	Allow

Monitor > Logs > Traffic to see application identification

Identification of network traffic is an iterative process. First create Security policy rules to allow or block those applications that are known to be traversing your firewall. Then create a temporary Security policy rule to detect unidentified applications traversing your firewall. For example, Known Good allows necessary and expected applications through the firewall. Known Bad blocks identified applications that are not permitted on your network.

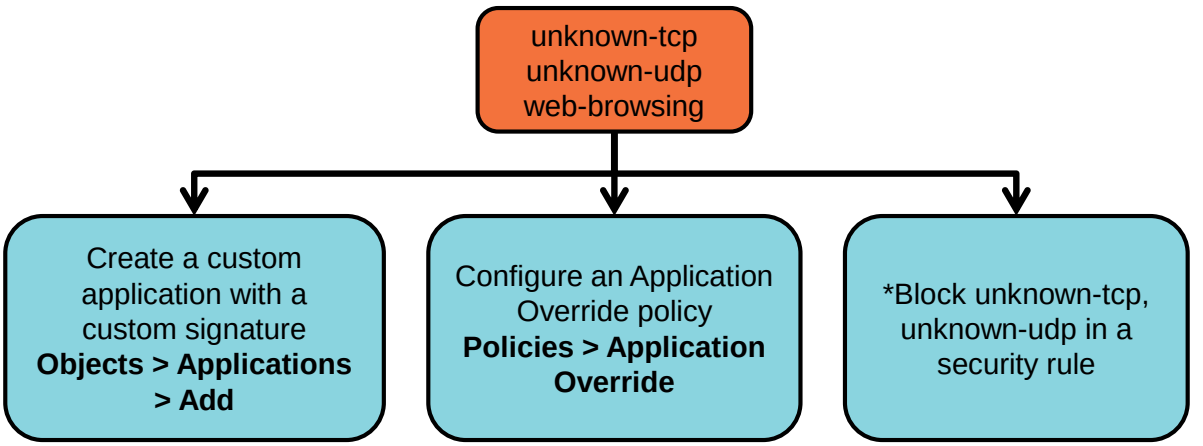
However, most organizations acknowledge that they do not yet know all of the applications in use on their network. These unidentified applications must be identified so that specific Security policy rules can be added to allow or block them. In the example, **Unclassified Apps** enables you to determine which other applications are encountered by the firewall. Traffic that does not match the first two rules is matched by Unclassified Apps. With the rule's action set to "Allow," the firewall receives enough packet information—even if the protocol is TCP—to be able to identify the application. The application could be specifically identified, or identified as unknown-tcp or unknown-udp.

The newly identified application is listed in the Traffic log. Use this information to create a new rule to allow or block the application.

Note: If this last rule was set with the action of "Deny," in the event of an incoming TCP connection attempt the firewall would classify the application as *unknown*, which results in a Traffic log entry with an application label of *not-applicable*.

You should be actively reviewing your logs to identify and classify unidentified traffic. You could expose your network to danger if you continue to allow unidentified applications. As an alternative to creating a specific rule to capture unidentified traffic, you can enable logging on the default Interzone-default rule. By default, logging on this rule is disabled.

Controlling Unknown Applications



*Could block more traffic than intended

At least three methods are available to the firewall for processing traffic identified only as unknown-tcp, unknown-udp, or web-browsing.

The first method is to create administrator-defined, custom applications. First use a network packet capture to identify unique bit patterns in the application. Next, create a custom application signature to match that bit pattern. Lastly, use the custom application in a Security, QoS, or PBF policy rule just like applications identified in the Palo Alto Networks App-ID database.

Your second choice is to configure an Application Override policy rule. An Application Override policy rule can be used to identify custom application traffic based on its source zone and IP address, its destination zone and IP address, and its port and protocol. Creation of an Application Override policy prevents the firewall from using App-ID to process the Layer 7 data in an attempt to identify an application. Application override also disables Security Profiles. You still must create a Security policy rule to allow the application to traverse between firewall zones.

For more information about creating custom applications or configuring an Application Override policy, use the web interface's online help or the *PAN-OS 9.0 Administrator's Guide* at https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html.

The third method to control unknown applications is to block unknown-tcp or unknown-udp traffic, which could block more traffic than you intended. The unknown-tcp or unknown-udp traffic seen inside an organization usually is benign. For example, it could be an in-house-developed backup utility or a scripted maintenance task. However, you should be concerned about unknown-tcp or unknown-udp that appears in sessions going out to or coming in from the internet. Before you block unknown-tcp or unknown-udp, try to identify the traffic by using the Traffic log and packet captures, and instead create a custom application or configure an Application Override policy.

Application identification (App-ID) overview

Using App-ID in a Security policy

Identifying unknown application traffic

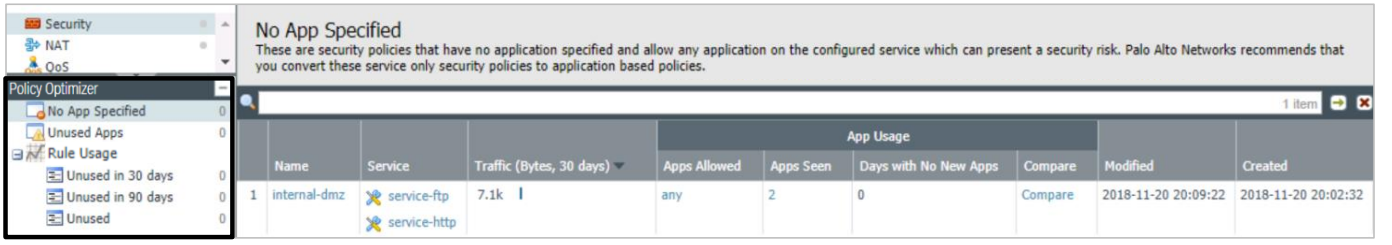
Migrating to an App-ID-based Security policy

Updating App-ID

Policy Optimizer

- Migrate port-based rules to App-ID-based rules
- Help reduce attack surface and provide information about application usage
- Prevent evasive applications from running on non-standard ports
- Identify over-provisioned application-based rules

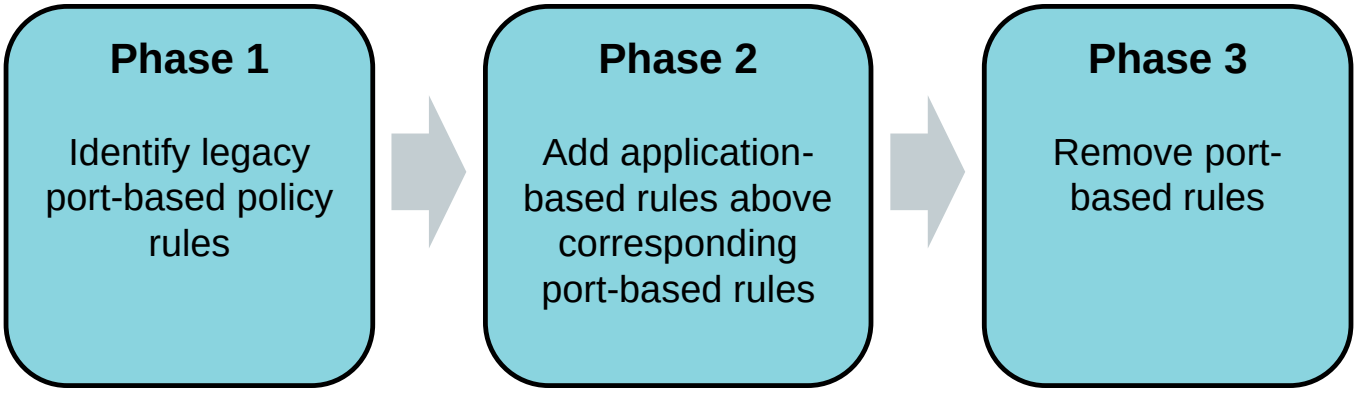
Policies > Security > Policy Optimizer > No App Specified



The Policy Optimizer provides a simple workflow to migrate your legacy or port-based Security policy rulebase to an App-ID based rulebase, which improves security by reducing the attack surface and providing information about applications being used. The Policy Optimizer enables you to clone an existing port-based rule and then add the appropriate applications to your cloned rule. When you convert port-based rules to application-based rules, you improve your security posture because you select the applications you want to allow or whitelist and deny all other applications. This conversion to application-based rules also can prevent evasive applications from running on non-standard ports when it is combined with restricting application traffic to its default ports. When you allow the appropriate applications over the appropriate ports, you can eliminate unwanted and potentially malicious traffic from your network.

The Policy Optimizer can help identify over-provisioned application-based rules that allow applications that you do not use on your network. The use of rules that are too broad in scope increases your attack surface and puts your network at risk of inadvertently allowing malicious traffic.

Moving to Application-Based Policies



The graphic illustrates one way to implement the *migration* method to migrate an existing port-based policy to an application-based policy.

In Phase 1 you identify existing legacy port-based Security policy rules and determine which policy rules to convert and in which order. A gradual conversion is safer than migration of a large rulebase at one time and allows you to more easily ensure that new application-based rules control the necessary applications. The Policy Optimizer provides sorting options to help you prioritize which rules to convert or clean up.

In Phase 2 you use the Security policy's Policy Optimizer tool to add application-based rules to the Security policy. Add each new application-based rule above its corresponding port-based rule. The goal is to ensure that traffic matches the application-based rule before it can match the legacy port-based rule. Matching of traffic to a specific application reduces your organization's attack surface.

Phase 3 is the final cleanup of the Security policy. You review the Traffic logs and Security policies to determine if traffic is continuing to match any legacy port-based rule. If no legitimate traffic has matched a legacy rule, then that legacy rule can be safely removed. If traffic has matched a legacy rule, the corresponding application-based rule is updated to match the traffic. At the end of Phase 3, you will have removed all or most of the legacy rules, and the attack surface will be minimized.

Phase 1: Viewing Data of Port-Based Rules

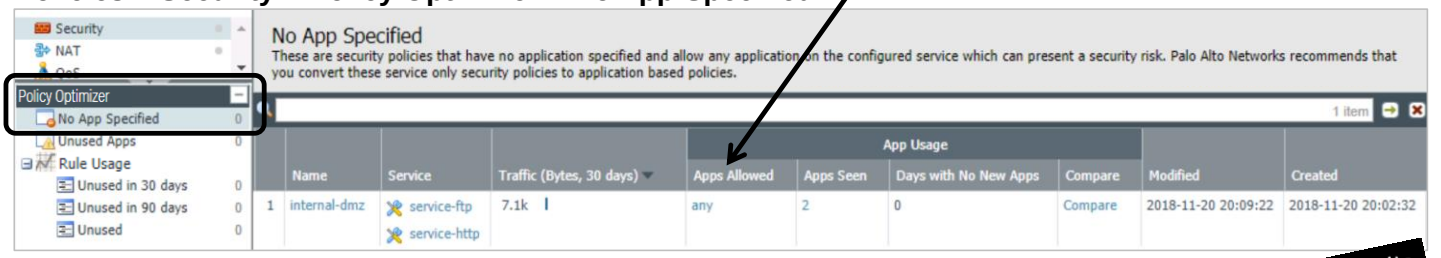
Use **No App Specified** to discover port-based rules.

Policies > Security

	Name	Source			Destination		Application	Service
		Zone	Address	User	Zone	Address		
1	internal-dmz	inside	any	any	dmz	any	any	service-ftp service-http

Application “any” triggers **No App Specified** match

Policies > Security > Policy Optimizer > No App Specified



During the first 30 days of the migration process, the firewall should log enough traffic and application data to allow you to move through Phase 1 of the migration process. In Phase 1 you begin to identify port-based rules in the Security policies and prioritize which rules should be migrated to App-ID based rules. Browse to **Policies** > **Security** > **Policy Optimizer** and click **No App Specified** to begin the process.

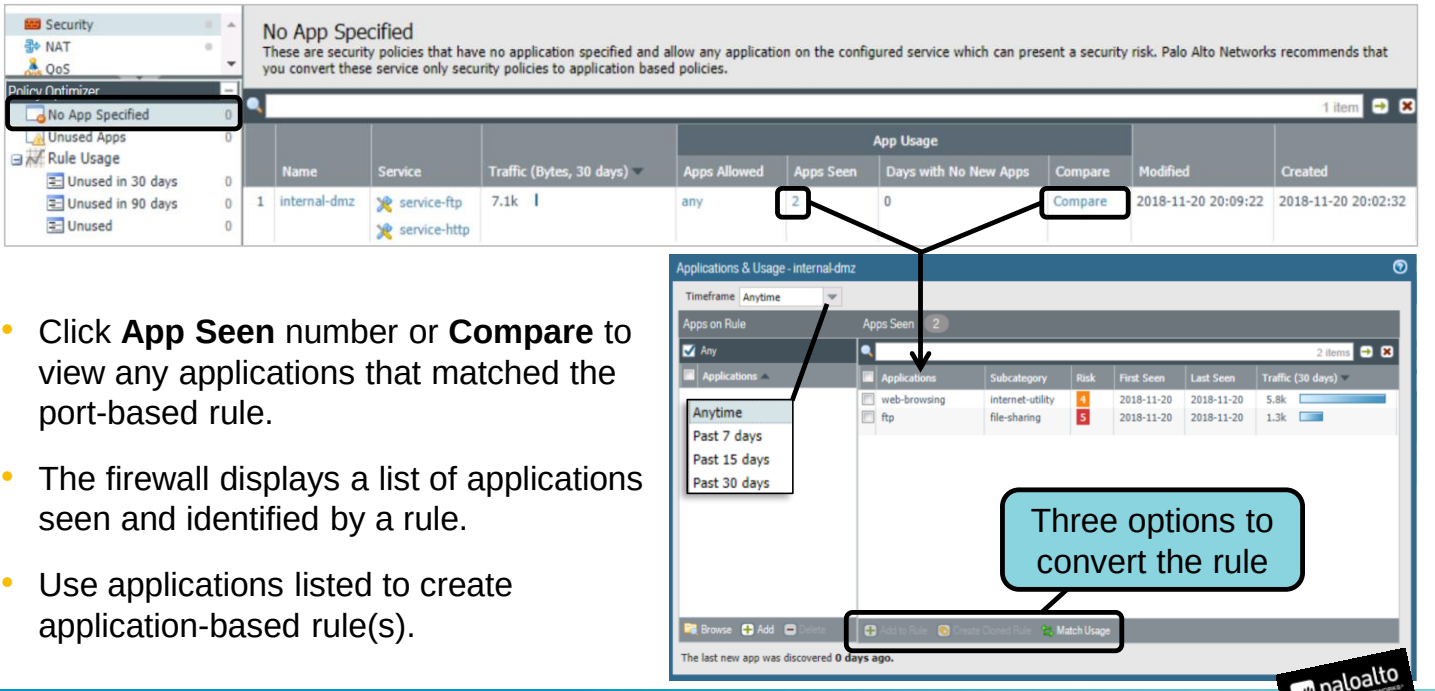
No App Specified displays all port-based Security policy rules. The firewall considers any rule port-based if its **Application** field is configured as “any.” In the example, the “internal-dmz” rule in the Security policy has its **Application** field configured as “any.” This rule allows any application traffic from the inside zone to the dmz zone if it is on either TCP port 21 or 80.

Supplemental Notes

The firewall processes the Security policy at the beginning of each hour and checks for rules with the Application configured as “any.” The firewall adds information about these rules to the **No App Specified** window.

Discovering Applications Matching a Port-Based Rule

Policies > Security > Policy Optimizer > No App Specified



- Click **App Seen** number or **Compare** to view any applications that matched the port-based rule.
- The firewall displays a list of applications seen and identified by a rule.
- Use applications listed to create application-based rule(s).

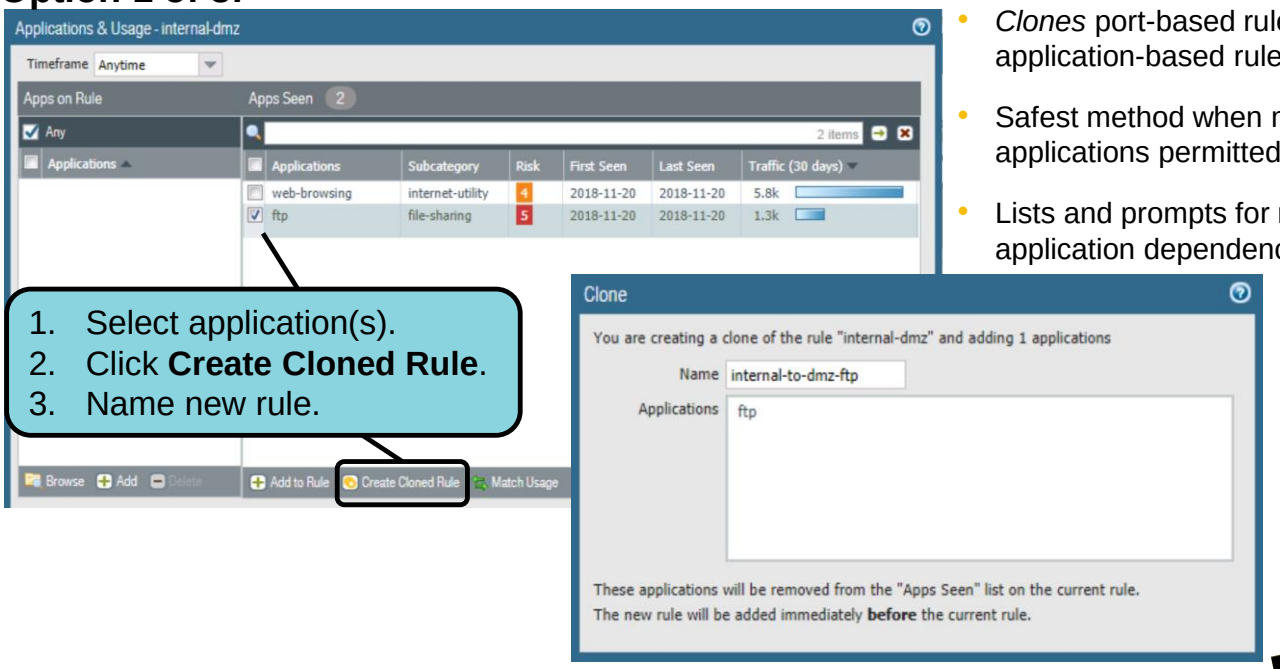
You must do more than identify your port-based rules. You also must convert your port-based rules so that they control the specific applications that are used in your organization. In the **No Apps Specified** tool, pick a Security policy rule and click either the number in the **Apps Seen** column or the word **Compare** in the **Compare** column. The **Applications & Usage** window will open.

The **Applications & Usage** window includes an **Apps Seen** column that displays a list of all applications that have been seen and identified by the Security policy rule. The **Applications & Usage** window also provides three options to convert a port-based rule into an application-based rule. The **Add to Rule** and **Match Usage** options *replace* a port-based rule with an application-based rule. The **Create Cloned Rule** option creates a new application-based rule based on the port-based rule. The new rule is placed directly above the original rule in the Security policy.

Some applications appear on the network at intervals, for example, for quarterly or yearly events. These applications might not display in the **Applications & Usage** window if you do not collect or view network activity over a sufficiently long time period. To display the longest and most accurate list of applications beneath **Apps Seen**, choose the longest **Timeframe** possible. In the example, **Anytime** was selected.

Phase 2: Cloning a Port-Based Rule Using “Create Cloned Rule”

Option 1 of 3:



- *Clones* port-based rule to new application-based rule
- Safest method when many applications permitted by a rule
- Lists and prompts for required application dependencies

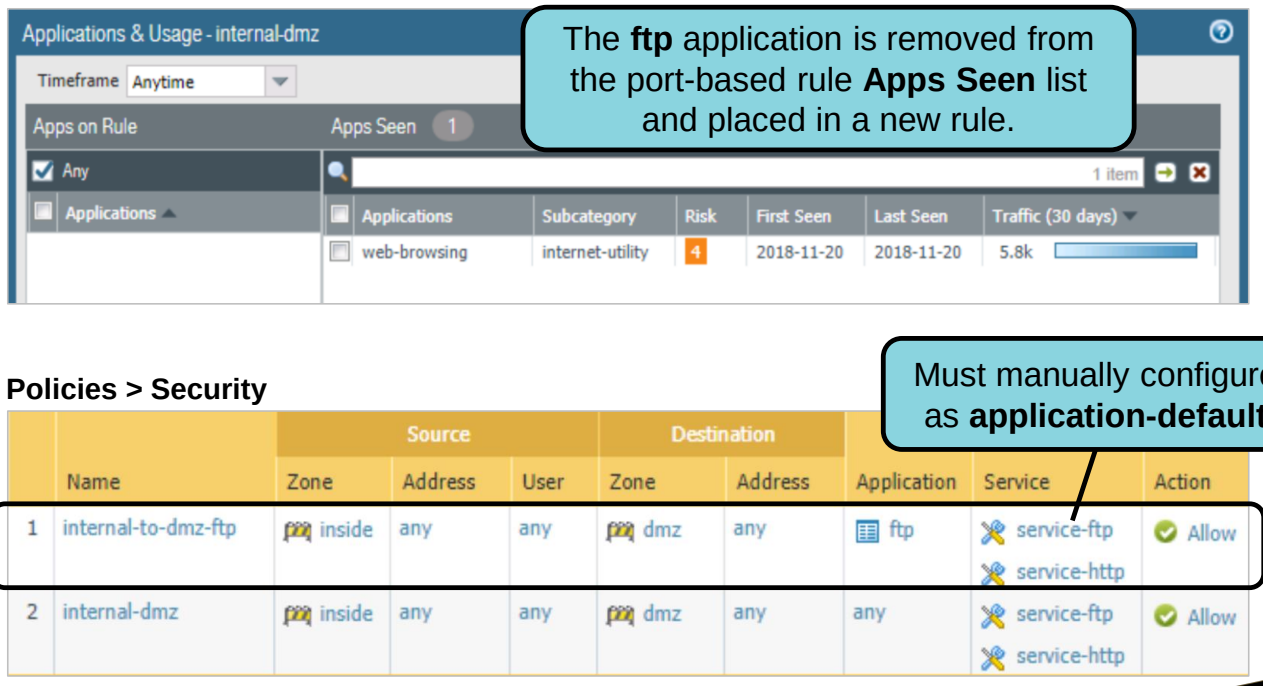
The **Create Cloned Rule** option creates a new application-based rule and places it in the Security policy directly above the original port-based rule. You still must perform a commit operation after the Security policy update.

Start by selecting only those applications from the **Apps Seen** column that you want to allow in the new, cloned rule. Then click **Create Cloned Rule**, which opens a new **Clone** window where you are prompted to enter a name for the new cloned rule. The **Clone** window also lists any applications that are required by the applications in the cloned rule. These applications are known as application dependencies. **Create Cloned Rule** enables to you select and add these applications to a rule. Click **OK** to add the new, cloned application-based rule. Any applications added to the cloned rule are removed from the port-based rule **Apps Seen** list.

You can repeat this process multiple times, selecting a different set of applications each time, to create multiple application-based rules from a single port-based rule.

The **Create Cloned Rule** method is the safest way to migrate rules, especially when **Applications & Usage** shows more than a few well-known applications that match the rule. Any traffic that does not match the new application-based rule hits the original port-based rule, so there is no risk of losing application availability. If traffic from legitimate applications has not hit the port-based rule for a reasonable period of time, you can remove it to complete the migration of that rule.

Result of Using “Create Cloned Rule”



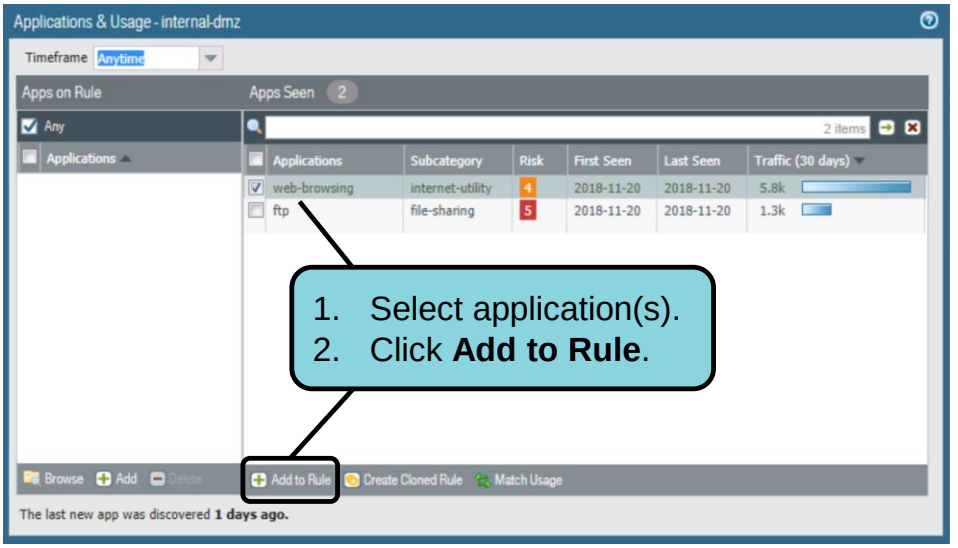
The screenshots illustrate the result of cloning a port-based rule to add a new application-based rule. The firewall removes the **ftp** application from the port-based rule **Apps Seen** list because the application now will be controlled by the new cloned rule.

In the Security policy, the new application-based rule is placed directly above the port-based rule, which ensures that, after you perform a commit, the application-based rule will match FTP traffic before the port-based rule. If the policy works as planned, then you eventually can disable and remove the port-based rule.

To finish cloning a rule, you must manually edit the Security policy rule and modify the **Service** to **application-default** and then perform a commit to activate the new configuration.

Replacing a Port-Based Rule Using “Add to Rule”

Option 2 of 3:



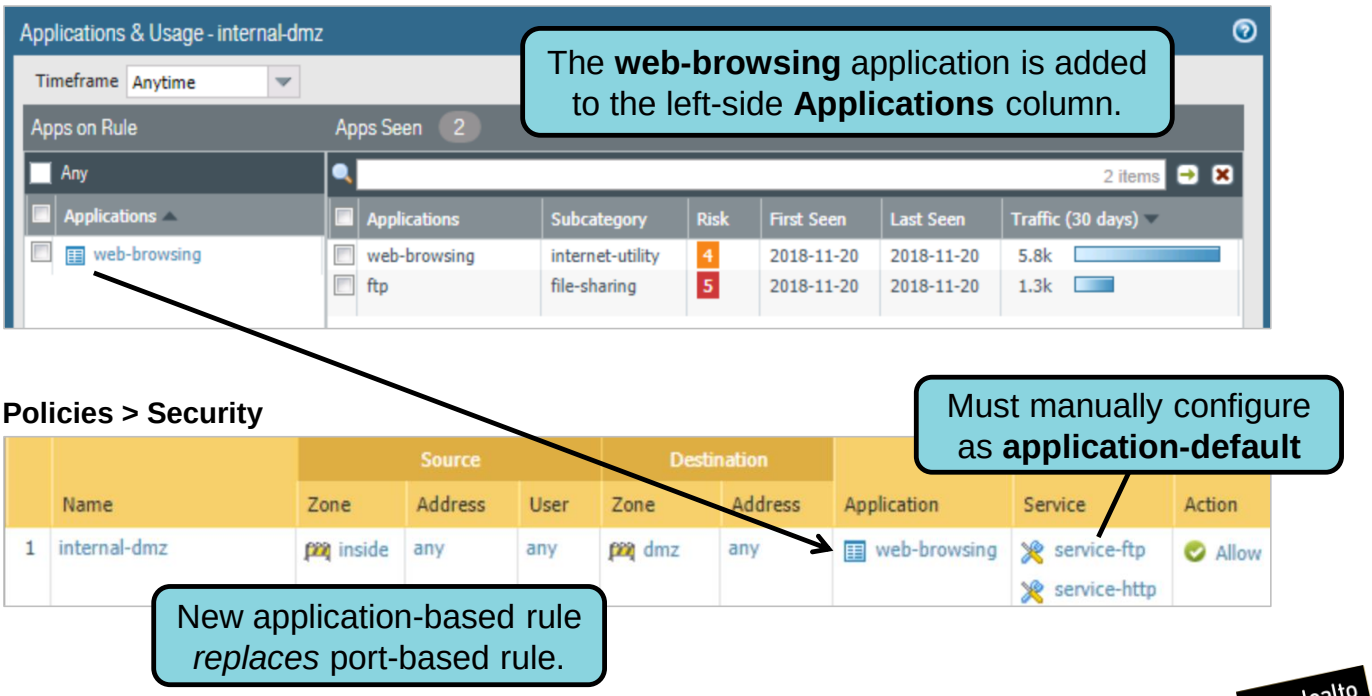
- Firewall *replaces* port-based rule with application-based rule.
- Moves *selected* applications to a new rule
- Lists and prompts for required application dependencies
- Riskier method because some required applications could be inadvertently missed.

Add to Rule is the second option to convert port-based policy rules to application-based policy rules. Start by selecting only those applications from the **Apps Seen** column that you want to allow in the new replacement rule. Then click **Add to Rule**. After you click **Add to Rule**, the selected applications are copied to the **Apps on Rule** column and the tool uses them to build a new application-based rule. Click **OK** to continue the rule conversion process.

If any applications on the **Apps on Rule** list depend on other applications, then the firewall opens a new **Application Dependencies** window that lists these applications. Click **Yes** to have these applications added to the new application-based rule. The firewall replaces the old port-based rule with a new application-based rule. The Security policy has changed, so you must commit the configuration.

This method can be riskier because you might inadvertently miss applications that should be on the rule, but the original port-based rule is removed and cannot catch any accidental omissions. However, this method is quick and easy to use to convert a port-based rule that has only a few well-known applications. For example, for a port-based rule that allows traffic only to TCP port 22, the only legitimate application is SSH, so addition of the *ssh* application to the rule would be safe.

Result of Using “Add to Rule”



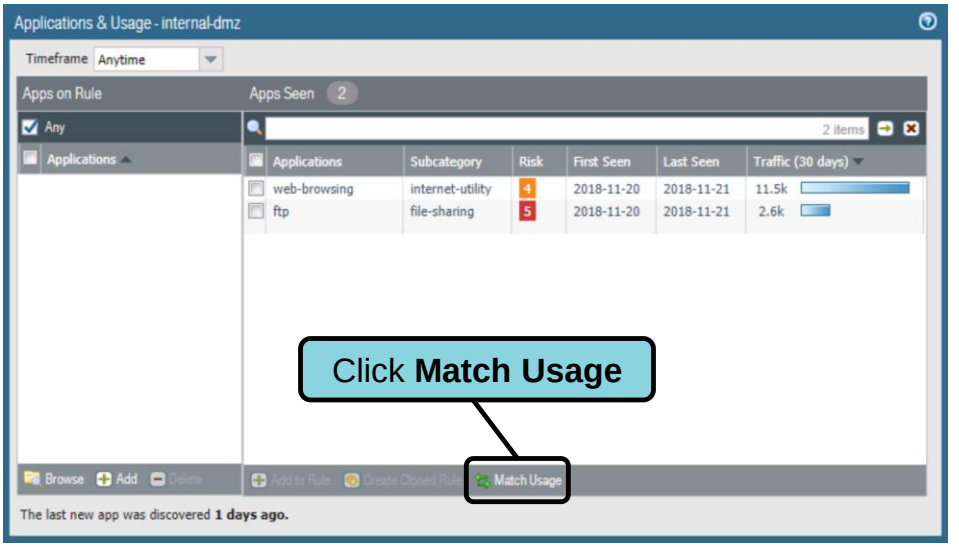
The screenshots illustrate the result of replacing a port-based rule with a new application-based rule. The firewall removes the **web-browsing** application from the port-based rule **Apps Seen** list and moves it to the **Apps on Rule** column because the web browsing traffic now will be controlled by the new cloned rule.

In the Security policy, the new application-based rule is placed where the original port-based rule formerly existed. This placement ensures that, after you perform a commit, the application-based rule will match web browsing traffic. To finish adding the rule, you must manually edit the Security policy rule and modify the **Service** to **application-default** and then perform a commit to activate the new configuration.

Notice in this example that the new rule does not allow FTP traffic and the old rule that did allow FTP traffic has been removed. In the new configuration, FTP traffic from the inside zone to the dmz zone will not be allowed.

Replacing a Port-Based Rule Using “Match Usage”

Option 3 of 3:



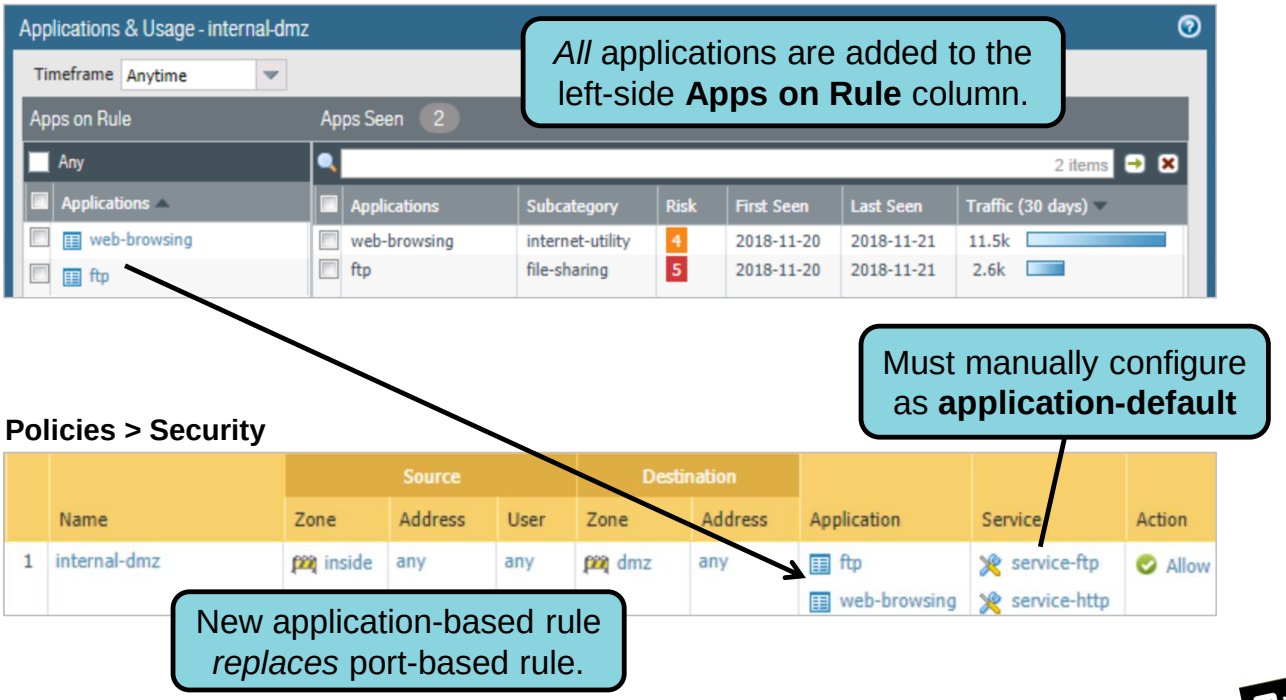
- Use only when the rule matches a small number of legitimate applications.
- Copies *all* applications under **Apps Seen** to **Apps on Rule**
- Firewall *replaces* port-based rule with application-based rule.

Match Usage is the third option to convert port-based policy rules to application-based policy rules, and it replaces a port-based rule in the Security policy with an equivalent application-based rule. You should use **Match Usage** to convert a rule only when the rule has seen a small number of well-known applications with legitimate business purposes.

After you click **Match Usage**, the entire list of applications beneath **Apps Seen** is copied to the **Apps on Rule** column and the tool uses these applications to build a new application-based rule. Be aware that the original port-based rule allowed any application if it was on the allowed port, so **Apps Seen** could include unneeded or unsafe applications. Click **OK** to continue the rule conversion process. If any applications on the **Apps on Rule** list depend on other applications, then the firewall opens a new **Application Dependencies** window that lists these applications. Click **Yes** to have these applications also added to the new application-based rule.

The firewall replaces the old port-based rule with a new application-based rule. The Security policy has changed, so you must commit the configuration.

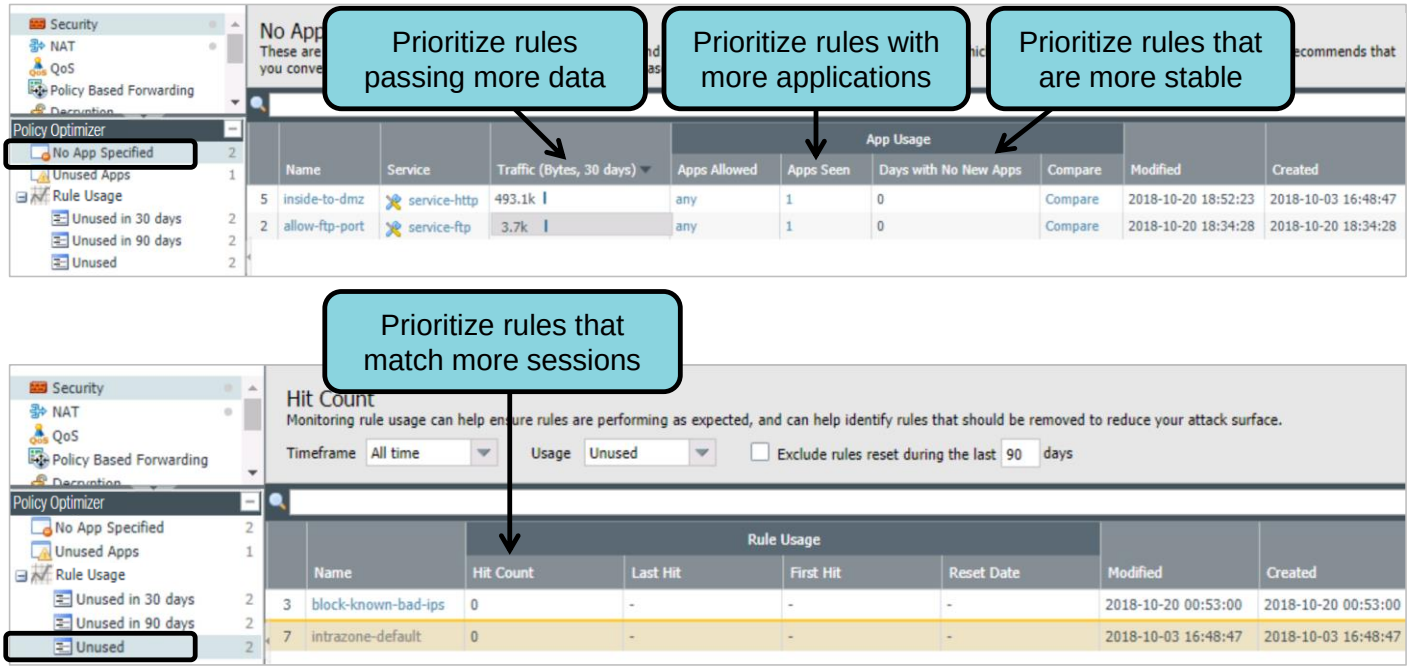
Result of Using “Match Usage”



The screenshots illustrate the result of replacing a port-based rule with an application-based rule.

Use of **Match Rule** copies *all* the applications from **Apps-Seen** to **Apps on Rule**. After you click **OK**, the firewall modifies the original rule to become an application-based rule. Then you must manually edit the Security policy rule and modify the **Service** to **application-default** and then click **Commit**.

Prioritizing Port-Based Rules to Convert



Palo Alto Networks recommends that you convert a few port-based rules at a time to application-based rules, in a prioritized manner. A gradual conversion is safer than migration of a large rulebase at one time, and you can more easily ensure that new application-based rules control the necessary applications.

No App Specified helps you prioritize rules for conversion based on your business goals and risk tolerance. Use the information in the following columns to prioritize port-based rules for conversion:

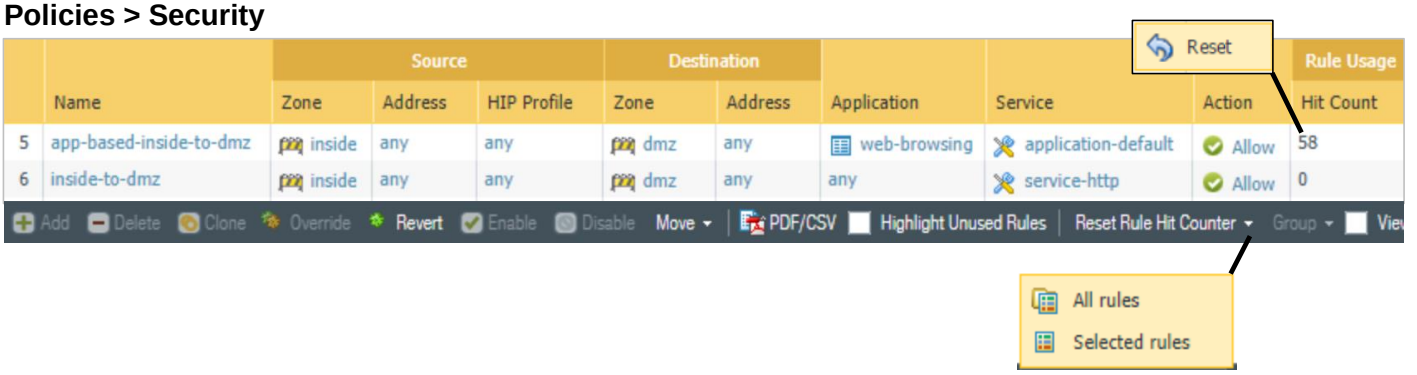
- **Traffic (Bytes, 30 days)**: The 30-day window places rules that *currently* pass the most data at the top of the list. A longer time span would put more emphasis on older rules that would remain at the top of the list because they have large cumulative totals, even though they no longer might see much data transferred.
- **Apps Seen**: A large number of legitimate applications matching a port-based rule might indicate you should replace the rule with multiple application-based rules that more tightly define the applications, users, and sources and destinations.
- **Days with No New Apps**: After the applications shown on a port-based rule stabilize, you can be more confident the rule is mature and that conversion will not accidentally exclude legitimate applications, and no more new applications will match the rule.
- **Created** and **Modified** dates help you evaluate the stability of a rule because older rules that have not been modified recently also might be more stable.

Hit Count also helps you to prioritize port-based rules for conversion. **Hit Count** displays rules that matched the greatest number of sessions over a selected time period. You can exclude rules for which you reset the hit counter and specify the exclusion time period in days. Exclusion of rules with recently reset hit counters prevents misconceptions about rules that show fewer hits than you expect because you did not know the counter was reset.

Phase 3: Reviewing Port-Based Rules

- After 60 days, review the **Policy Optimizer** columns in the Security policy.
- Look for port-based rules with zero hits.

Policies > Security

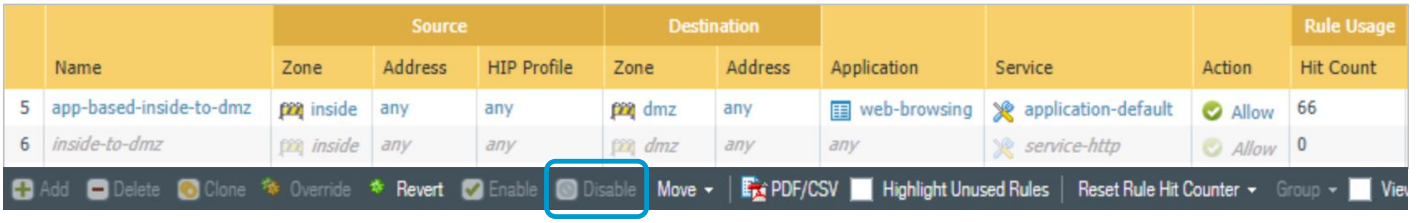


After 60 days, review the port-based rules to verify that no new traffic is being matched to them. View the **Policy Optimizer Hit Count** column in the Security policy. A value of zero in the **Hit Count** column indicates that a rule has not been used. You also can use the **Last Hit** column to determine the amount of time elapsed since a rule was used.

Hit Count is not reset after a reboot, a software upgrade, or a content upgrade. You have two choices for resetting rule counters. To reset the **Hit Count** value of a single rule to zero, hover your mouse pointer over the current value until a drop-down arrow appears and then select **Reset** from the drop-down menu. To reset a single rule or multiple rules, select the rules and click **Reset Rule Hit Counter** and select **Selected rules**. To reset all rules, click **Reset Rule Hit Counter** and select **All rules**.

Disabling Port-Based Rules

Policies > Security



- Disable port-based rules that have not matched to any new traffic.
- Disabled rules are rendered in gray italic font.
- Tag rules that must be removed later (optional).

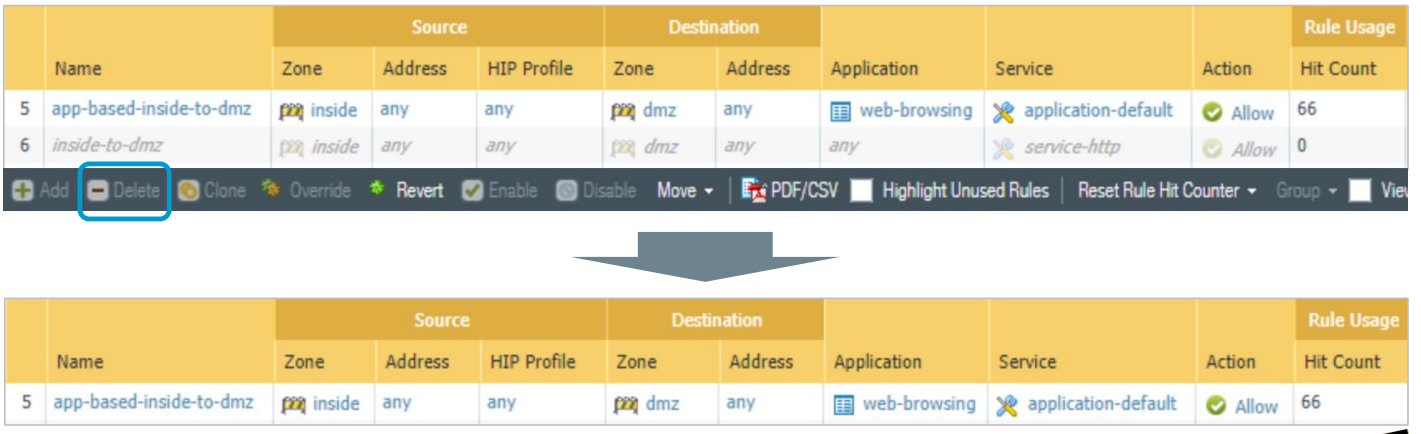
After your review of Security policy rule matches, disable those rules that have not been used. Disabled rules still are configured and can be re-enabled quickly, if necessary.

Port-based rules for applications that are used infrequently, such as accounting applications that are used only quarterly or annually, might take longer to replace and remove. You can use tags to mark these port-based rules for future removal, but keep them until their applications have been run once and their traffic has been recorded in the Traffic log and is viewable in the **Applications & Usage** window.

Removing Port-Based Rules

- After 90 days, delete port-based rules that have not matched to any new traffic.
- The goals:
  - At least 80% application-based rules
  - No inbound or outbound *unknown* applications (internal is acceptable)

Policies > Security



After 90 days, if no end-user issues have been reported with the application-based Security policy, then you can remove the disabled port-based rules. Removal of the legacy rules in Phase 3 is critical for improving the security posture. The migration should not be considered complete until Phase 3 tasks are performed.

Your goal is to convert at least 80 percent of the port-based rules to application-based rules. The actual percentage will vary based on the environment. In general, the higher the percentage is, the narrower the attack surface and the more secure the policy. You should create custom signatures and policy rules to eliminate all data center perimeter traffic labeled by App-ID as unknown.

After you have completed Phase 3, any future Security policy rules should be added as application-based rules.

Supplemental Notes

Deny rules that are port-based generally are safe because they do not expand the attack surface.

Application identification (App-ID) overview

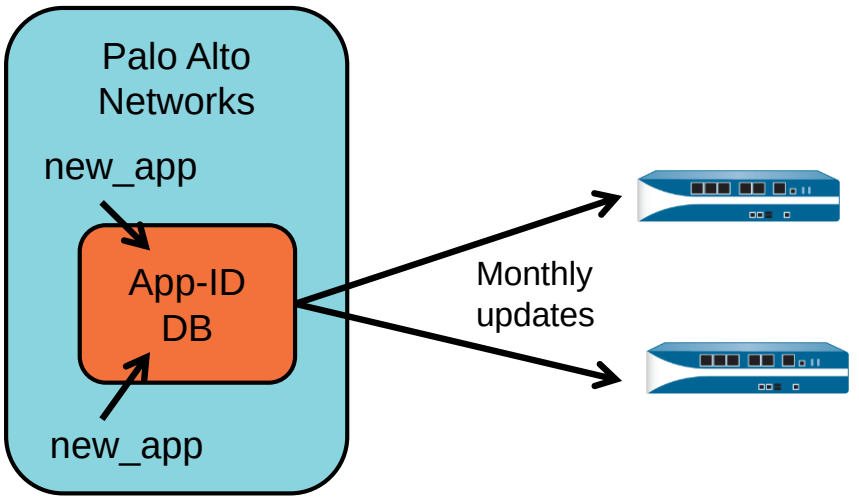
Using App-ID in a Security policy

Identifying unknown application traffic

Migrating to an App-ID-based Security policy

Updating App-ID

Dynamic Content Updates: App-ID



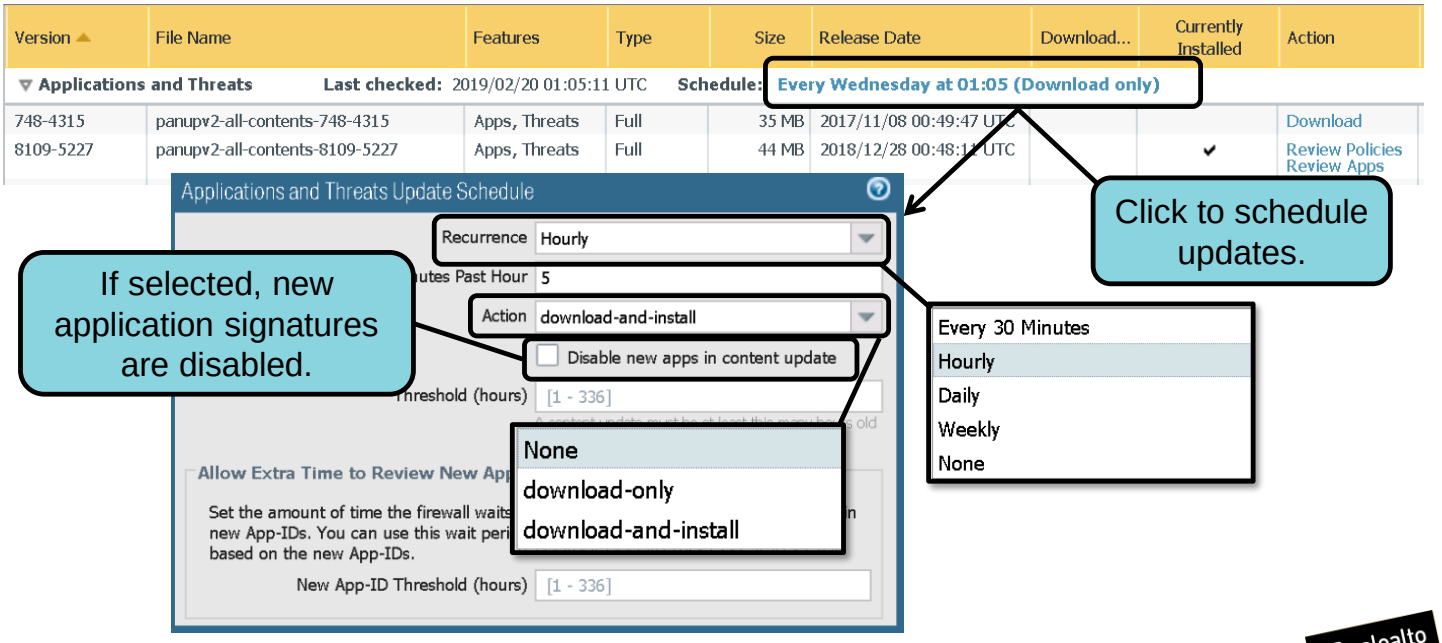
Choices:

- Scheduled download only
- Scheduled download and install
- Manual download and install

Palo Alto Networks adds new applications to the App-ID database nearly every week. You can schedule an automatic download or automatic download and installation of the updated App-ID database. Updated content also can be manually downloaded and installed. The App-ID database is downloaded as part of the application and threat content update.

Scheduled App-ID Updates

Device > Dynamic Updates



You can schedule App-ID updates to be automatically downloaded and installed. However, sometimes the identification of a new application might interact adversely with your current policy rules. For example, an application that formerly was identified as web-browsing and allowed by a policy rule might be blocked after an App-ID update because it becomes a uniquely identified application with no matching Security policy rule. However, you can pre-analyze the effect of new application signatures on your policy rules before you enable the new application signatures in App-ID. This pre-analysis capability is included in PAN-OS 7.0 and later.

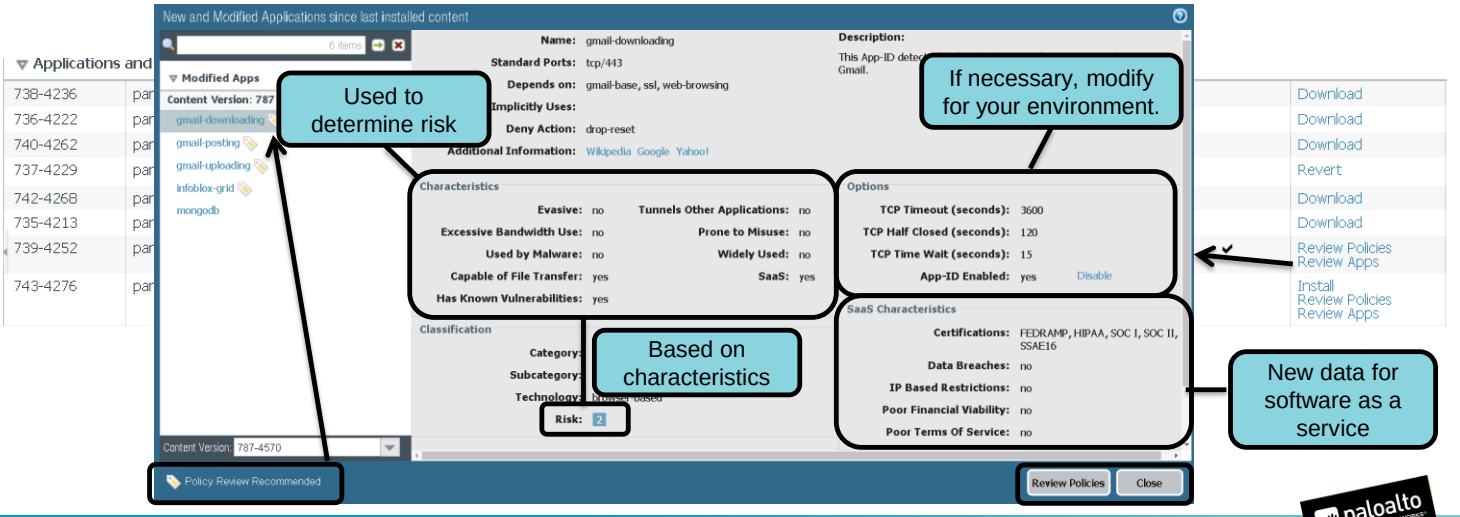
To enable the capability to pre-analyze the effect of new application signatures on your policy rules, check the **Disable new apps in content update** check box. New App-ID content updates are downloaded and installed, but any new application signatures are disabled until you individually enable them.

PAN-OS 8.0 adds an option for you to schedule a firewall to check for new updates every 30 minutes (existing options were hourly, daily, weekly, or not at all). Starting with PAN-OS 8.1, Palo Alto Networks made Applications updates available on the third Tuesday of each month; Threats updates are available once a week. Your firewall can check for updates more frequently because urgent updates can be released at any time.

Content Update Absorption

- **Review Apps** for list of modified applications and details for each application
- **Review Policies** to see policy rules that may enforce traffic differently

Device > Dynamic Updates



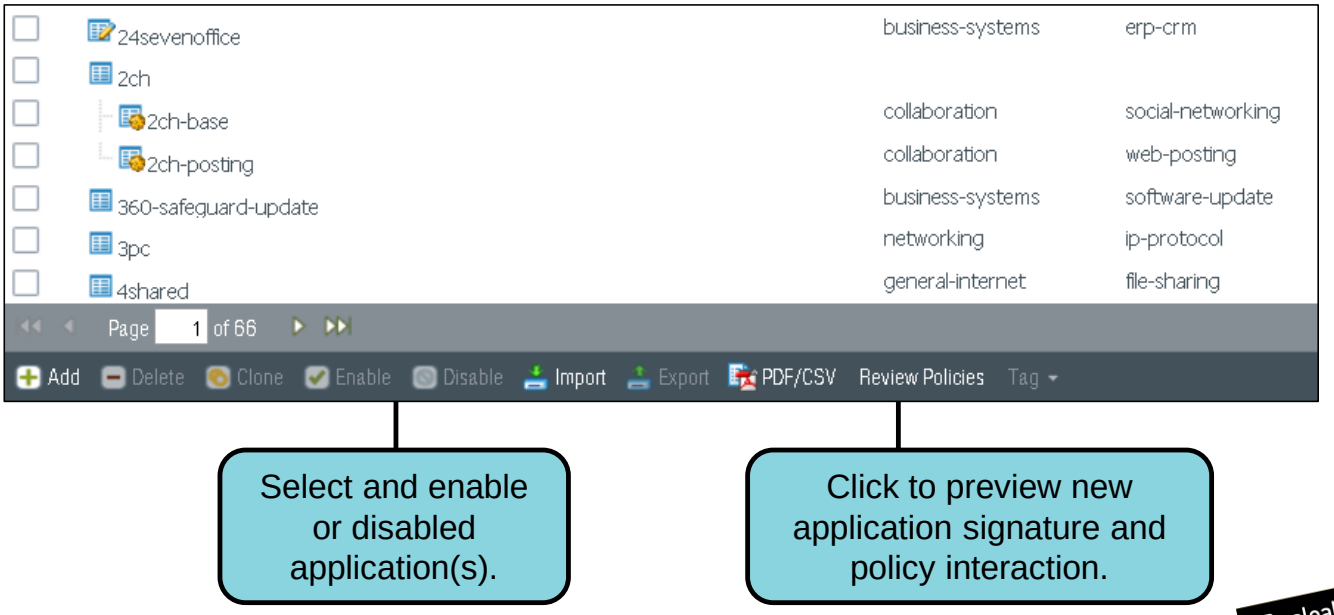
Application content updates increase your visibility into and control of application traffic by providing the firewall with new and modified applications. As the firewall installs the latest application content updates, it begins to classify traffic based on the newly identified applications without any additional configuration. Because of the impact to policy enforcement, you now can see a list of applications that were modified in a content release and assess how those changes will impact your Security Profiles.

Click **Review Apps** in the **Action** column to display a list of all the applications that were modified in a content release, and to see the details for each application. The list contains modified applications and updates to applications with network-wide impact such as LDAP or IKE flagged with a Policy Review Recommendation. Inclusion of the Policy Review Recommended flag means that you now have a visible sign of which policies to evaluate for potential changes in rule enforcement based on the modifications made to the application.

Click **Review Policies** to display the Security policy rules that might enforce traffic differently after the application is modified.

Pre-Analyze New Application and Policy Interaction

Objects > Applications



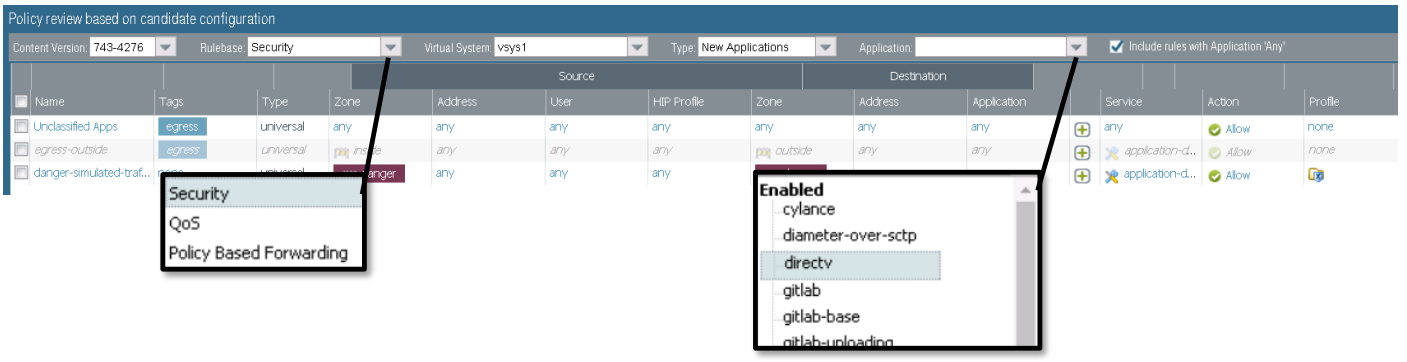
To pre-analyze the interaction of new application signatures with your current policy rules, click **Review Policies**. To enable new application signatures in App-ID, check the application's check box and click **Enable**.

Only application signatures released in new content updates with version prefix 484- and later can be disabled.

Review Policies

- View which policy rules will match new applications

Objects > Applications > Review Policies



The policy review window enables you to investigate and view which policy rules will match new application signatures.

Module Summary

Now that you have completed this module, you should be able to:

- Define application identification
- Describe the four major technologies to help identify applications
- Configure application filters and application groups
- Detect unidentified applications traversing the firewall
- Migrate a port-based rule to an App-ID based rule
- Configure scheduling of updates to App-ID

Now that you have completed the module, you should be able to:
- Define application identification
- Describe the four major technologies to help identify applications
- Configure application filters and application groups
- Detect unidentified applications traversing the firewall
- Migrate a port-based rule to an App-ID based rule
- Configure scheduling of updates to App-ID

Questions?

Review Questions

1. Which item is the name of an object that dynamically groups applications based on application attributes that you define: Category, Subcategory, Technology, Risk, and Characteristic?
   a. application
   b. application filter
   c. application group
   d. Application Profile
2. True or false? In Palo Alto Networks terms, an application is a specific program or feature that can be detected, monitored, and blocked if necessary.
   a. true
   b. false
3. Before App-ID would identify traffic as facebook-base, it would first identify the traffic as which application?
   a. unknown-tcp
   b. unknown-udp
   c. web-browsing
4. Which three statements are true regarding App-ID? (Choose three.)
   a. It addresses the traffic classification limitations of traditional firewalls.
   b. It is the Palo Alto Networks traffic classification mechanism.
   c. It uses multiple identification mechanisms to determine the exact identity of applications traversing the network.
   d. It still is in the developmental stage and is not yet released.
5. True or false? Application groups can contain applications, filters, or other application groups.
   a. true
   b. false

App-ID Lab (Pages 65-89 in the Lab Guide)

- Load a firewall lab configuration
- Create an application-based firewall rule
- Enable the Application Block Page
- View the Traffic log for application information

PROTECTION. DELIVERED.

Answers to Review Questions

1. b
2. a (true)
3. c
4. a, b, c
5. a (true)