CONTROLLING APPLICATION USAGE WITH APP-ID

PROTECTION IS NOT A PRINCIPLE BUT AN EXPEDIENT

- App-ID reduces the attack surface
- App-ID concepts and operation
- Configure App-ID objects
- Unknown and encrypted application traffic
- Migrating to an App-ID-based Security Policy
- Updating App-ID

EDU-210 Version A
PAN-OS® 10.2

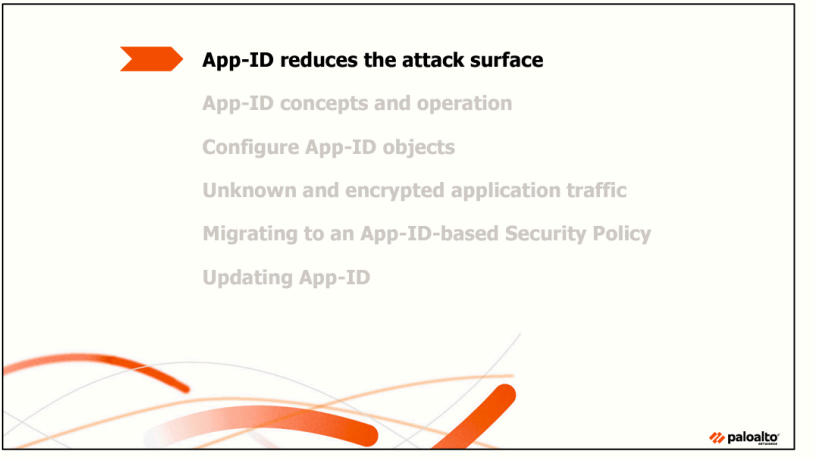
paloalto NETWORKS

Learning Objectives

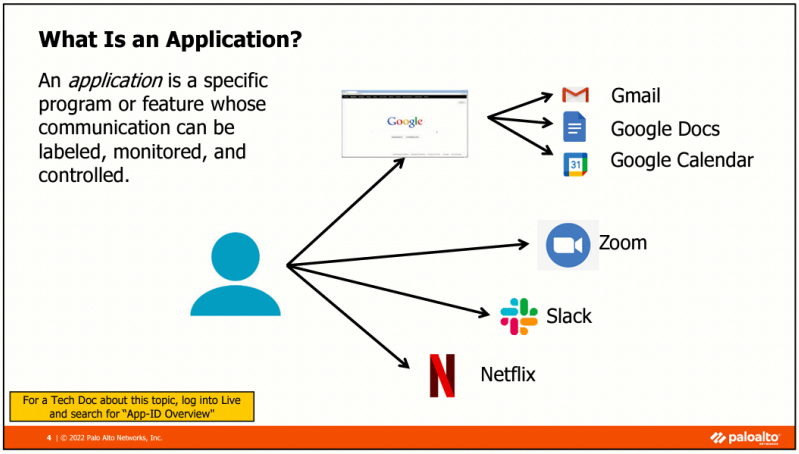
After you complete this module,
you should be able to:

- Identify how App-ID reduces the attack surface
- Describe App-ID concepts and operation
- Configure App-ID-based policy rules
- Update App-ID application database

After you complete this module, you should be able to:
- Identify how App-ID reduces the attack surface
- Describe App-ID concepts and operation
- Configure App-ID-based policy rules
- Update App-ID application database



This section describes how to use App-ID to reduce the attack surface of your firewall.



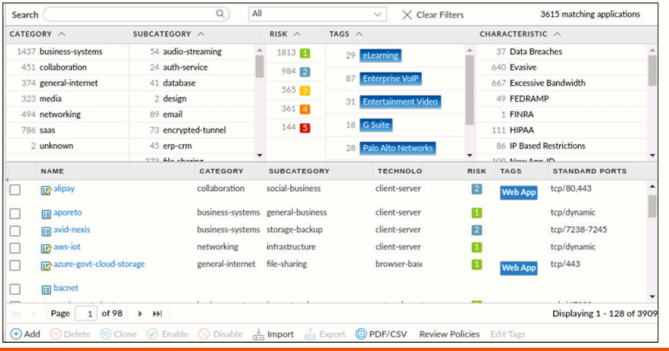
The term *application* does not have an industry-accepted definition in the way that *session* or *packet* does. In Palo Alto Networks terms, an application is a specific program or feature whose communication can be labeled, monitored, and controlled. Applications can be delivered through a web browser,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

What Is App-ID?

For a more information about Applications, use *applipedia.paloaltonetworks.com*

Objects > Applications

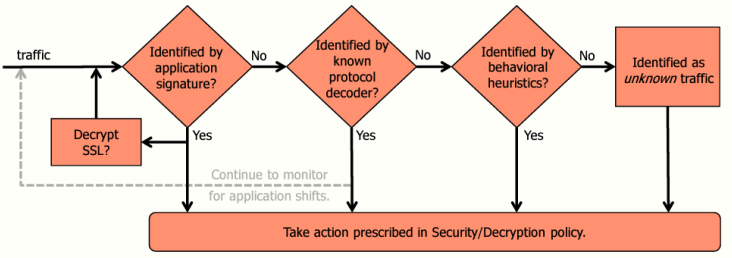


App-ID enables you to see the applications on your network and learn how they work, their behavioral characteristics, and relative risk. Applications and application functions are identified via multiple techniques, including application signatures, decryption (if needed), protocol decoding, and heuristics. When used with User-ID™, you can see exactly who is using the application based on their identity, not just an IP address.

App-ID supports a comprehensive set of applications and application functions, organized by categories, technologies, risk, and so on. This enables you to transition to a positive application enforcement model that allows you to define which applications and application functions are permitted explicitly. If the application is internal or a custom application, you can create a custom App-ID using a set of available protocol and application decoders. Once the custom App-ID is developed, your internal application is classified and inspected the same manner as applications with standard App-IDs.

App-ID Application Identification

App-ID identifies applications in traffic observed by the firewall.



App-ID enables you to see the applications on your network, their behavioral characteristics, and relative risk. App-ID enables more granular network traffic control, such as allowing only sanctioned Office 365 accounts or allowing Slack for instant messaging but blocking file transfer.

App-ID does not rely on any single element, such as a port or protocol, to identify applications. Instead, applications and application functions are identified using multiple techniques. The general flow of traffic through App-ID is as follows:

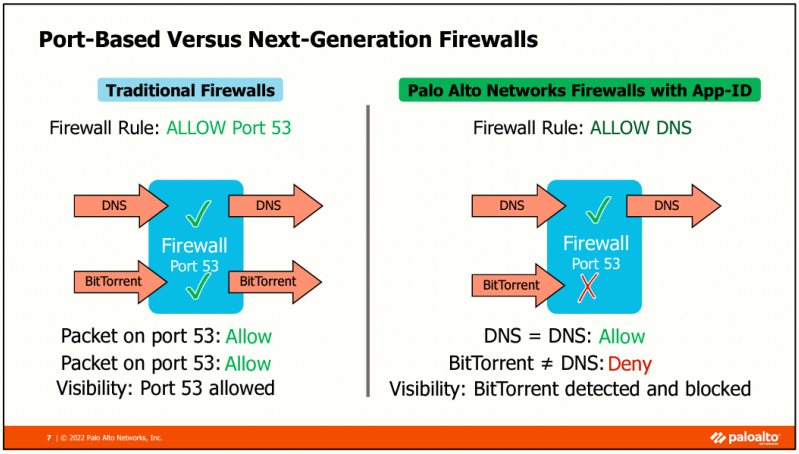
First, App-ID checks the traffic for a *protocol and bit pattern* identified by an application signature. If a signature identifies an application, the firewall checks the Security policy to determine what to do with the traffic.

The firewall also includes protocol decoders that read network traffic and identify *only* a protocol. If a decoder identifies a protocol in the traffic, then the firewall determines what to do with the traffic. For example, if the protocol is identified as SSL (or SSH), the firewall will check its Decryption policy and might decrypt the traffic. App-ID could identify an application in the decrypted traffic and apply the application's security policy.

The firewall might also identify a protocol and then use heuristics to pinpoint behavioral patterns consistent with an application. BitTorrent is an example of an application where the firewall must use heuristics to identify application traffic.

If App-ID cannot identify an application, it labels the traffic as unknown. You can create Security policy rules that tell the firewall what to do with unknown traffic.

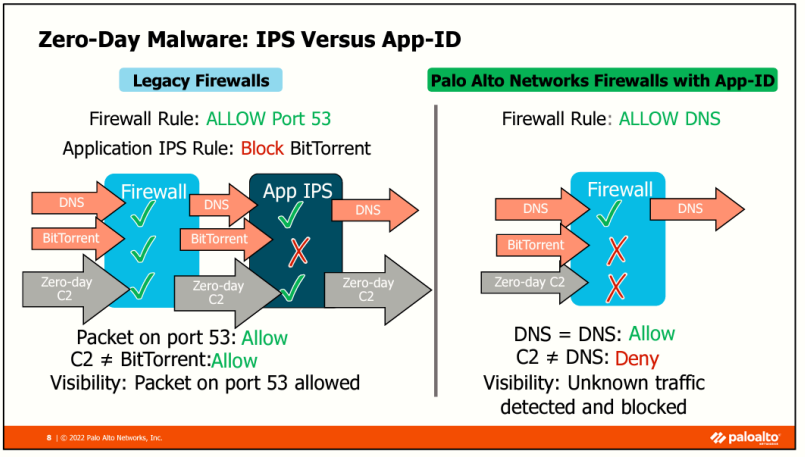
Even after App-ID initially has identified an application, App-ID continues to use the protocol decoders to determine whether the original application has shifted to a new application. Decoders for known protocols use additional context-based signatures to detect other applications that might be tunneling inside of the protocol. For example, Yahoo! Instant Messenger can be carried in the HTTP protocol. If an application shift is detected, the firewall rechecks the Security policy to determine what to do with the traffic.



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. Suppose you configure the firewall Security policy rule to use the application-default port. In that case, 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.

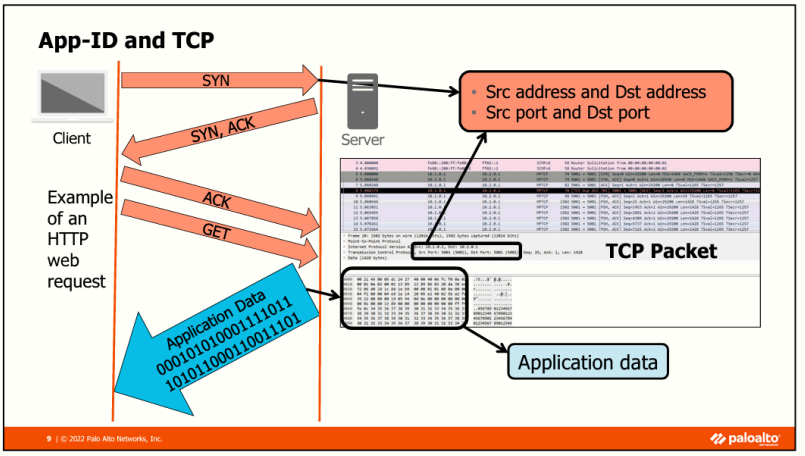
This protection is not available on a network protected by a traditional port-based firewall. On a port-based firewall, DNS would be allowed on port 53, but so would other evasive applications attempting to use port 53, such as BitTorrent in the example here. In such an environment, the network would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



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

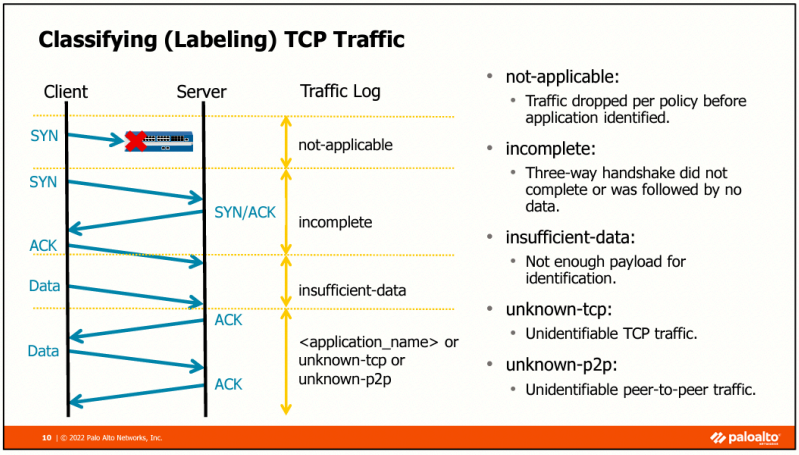
In the application intrusion protection system (IPS) blade server example, the zero-day virus using port 53 is allowed through the firewall because it uses an allowed port and is not BitTorrent. The IPS allows the unknown traffic because the IPS has not explicitly blocklisted it. This problem is inherent with application block policies: The device cannot block what the device does not know. The zero-day malware gets through, and 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.



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. The following two packets 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 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 this course in the Block Threats in Encrypted Traffic module.



Applications that use TCP usually require multiple packet transfers to identify an application. App-ID labels the TCP traffic seen by the firewall. If enough packets are received for App-ID to identify the application, then App-ID assigns an application label such as gmail-base. If App-ID cannot identify the application, it assigns labels such as *not-applicable*, *incomplete*, *insufficient-data*, *unknown-tcp*, or *unknown-p2p*.

App-ID labels traffic as *not-applicable* when the firewall discards the traffic because the Security policy does not allow it. For example, suppose a Security policy allows HTTP traffic on only TCP port 80, but the traffic arrives on a different port. In that case, the firewall blocks the traffic, and App-ID assigns the label not-applicable in logs and reports.

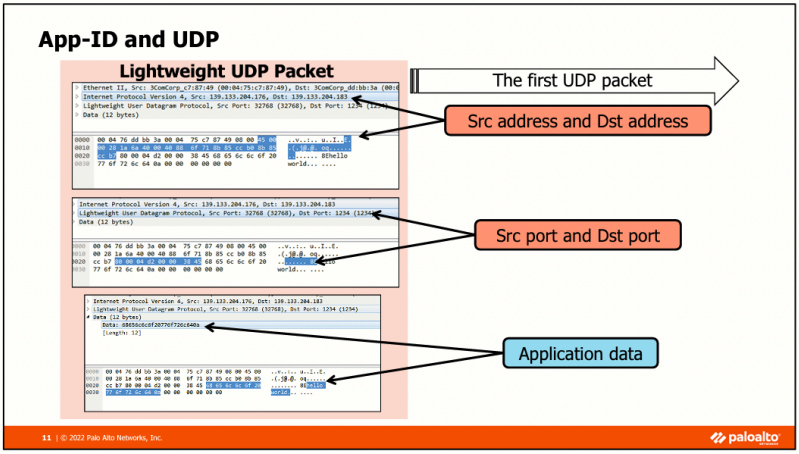
App-ID labels traffic as *incomplete* when the three-way TCP handshake does not complete or when the handshake completes but *no* data follows the handshake. Traffic labeled as incomplete by App-ID is not an application.

App-ID labels the traffic as *insufficient-data* when not enough data is received in the payload to identify the application. In this case, the three-way TCP handshake completes, but not enough data follows the handshake to identify the traffic.

App-ID labels the traffic as *unknown-tcp* when the three-way TCP handshake completes and data flows, but App-ID cannot identify the application.

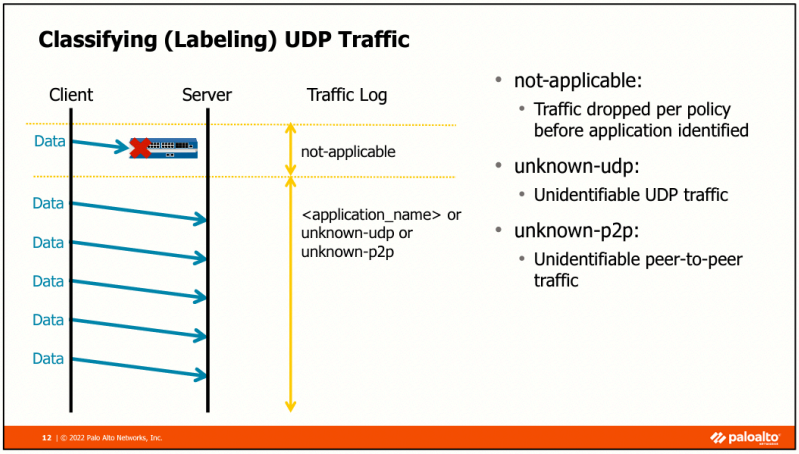
App-ID labels the traffic as *unknown-p2p* when App-ID cannot match the traffic to a specific application, but the traffic exhibits generic peer-to-peer behavior.

An unknown-tcp or unknown-p2p label could result from an internally developed application, commercial application, or malware for which the firewall has no signature.



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 the firewall needs are contained in the first packet. This example shows a single Lightweight UDP packet. The packet includes all source and destination addressing information. It also consists of the application data used to identify the traffic so that the Security policy can process it.

Note: Lightweight User Datagram Protocol (or 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, for example, in VoIP protocols or streaming video. When this feature is not used, UDP-Lite is identical to UDP.



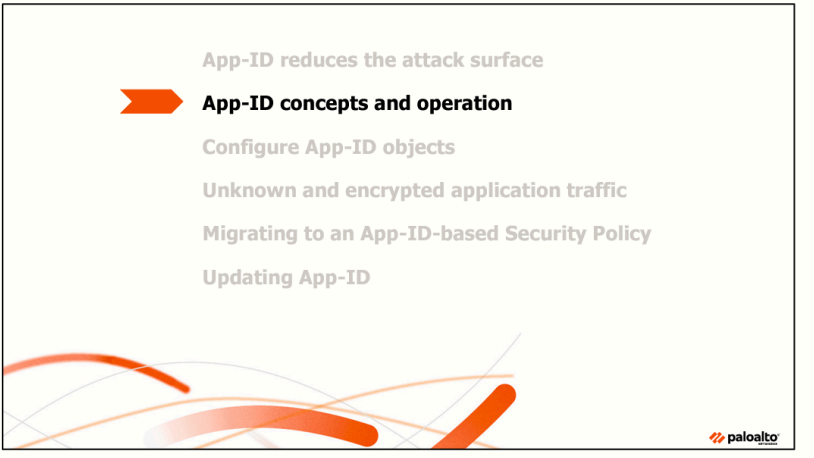
A Palo Alto Networks firewall examining UDP packets often must examine only a single UDP packet to identify the application. In most cases, all the information the firewall needs are contained in the first packet. App-ID labels the UDP traffic seen by the firewall. If App-ID recognizes the application, it assigns an application label such as DNS or call-of-duty. If App-ID cannot identify the application, it assigns an application label such as *unknown-udp* or *unknown-p2p*.

App-ID labels the traffic as *not-applicable* when the firewall discards the traffic because the Security policy does not allow it. For example, suppose a Security policy does not allow NTP, but traffic to port 123 is detected. In that case, the firewall blocks the traffic, and App-ID assigns the label not-applicable in logs and reports.

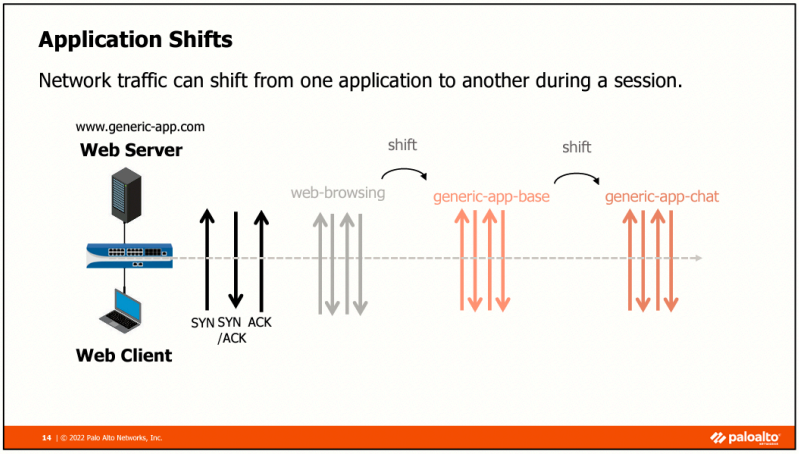
App-ID labels the traffic as *unknown-udp* when App-ID cannot identify the application.

App-ID labels the traffic as *unknown-p2p* when App-ID cannot match the UDP traffic to a specific application, but the traffic exhibits generic peer-to-peer behavior.

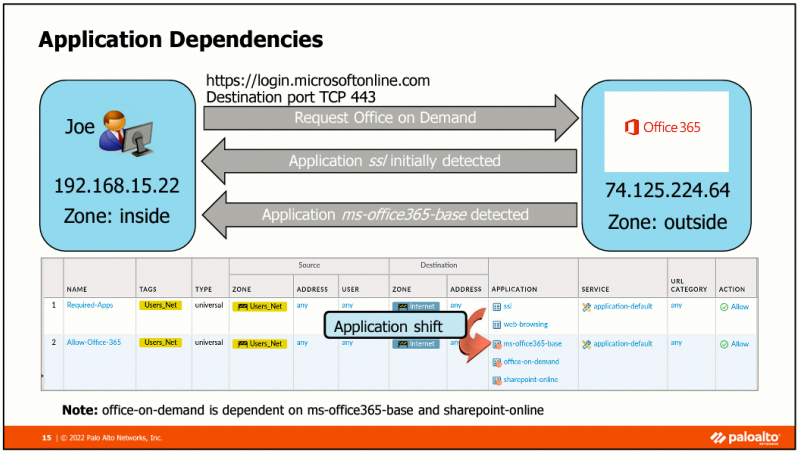
An unknown-udp or unknown-p2p label could result from an internally developed application, commercial application, or malware for which the firewall has no signature.



This section describes the concepts and operation of App-ID.



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



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

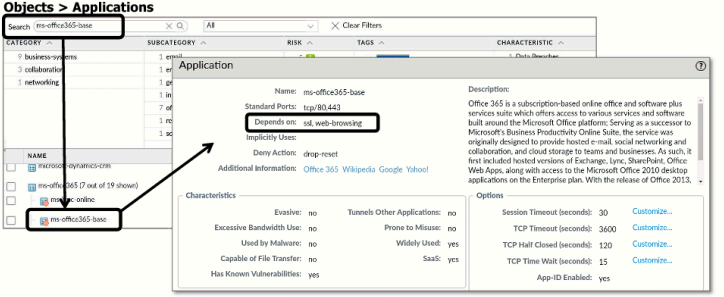
In this example, user Joe in the *Users_Net* zone wants to access Office on Demand in the *Internet* zone. App-ID scans the traffic and finds an HTTPS GET, which matches the *ssl* application. The first rule is matched, and the HTTPS connection is allowed. The Office 365 rule is not checked because a matching rule has already 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 to the following 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 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.

View Application Dependencies Before Modifying a Rule

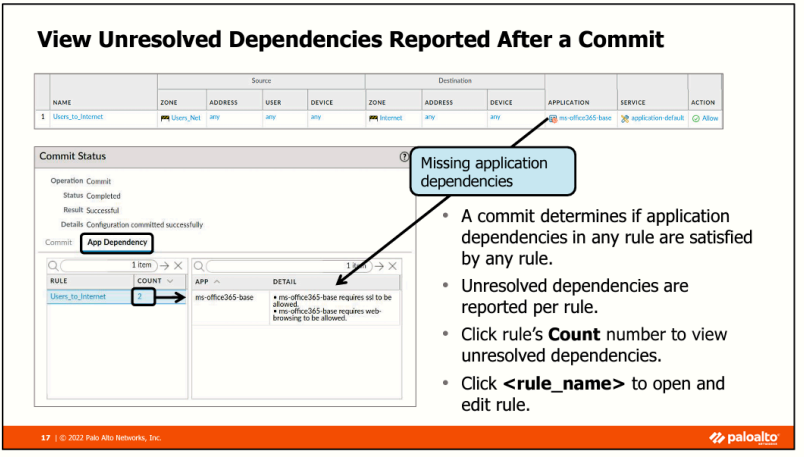


Dependent applications require you to add a Security policy rule.

Palo Alto Networks maintains a database of known application signatures for use by 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 https://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 pass application traffic, any applications listed in its Depends on field must also be allowed by the Security policy.

In the example, notice that the two applications listed in the **Depends on** field must be allowed explicitly on the firewall to use the application ms-office365-base. 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 permitted in the Security policy, you will receive warnings when you commit the configuration.



If you have not resolved application dependencies while creating or editing your policy rules, then what happens? Starting with PAN-OS 9.1, unresolved application dependencies during commit operations are reported on the **App Dependency** sub-tab in the **Commit Status** window.

During a commit operation, the firewall verifies whether the applications listed in the policy have dependent applications and then determines whether any rule in the policy includes these dependent applications. You can add the missing application dependencies to any rule in the policy and commit again. Click the rule's name to add the missing application dependencies to the rule reported in the Status Window. The **Security Policy Rule** window will open to that rule and enable you to edit the application list for the rule.

To see the list of missing application dependencies in the **Commit Status** window, click the **Count** number next to the rule's name. The firewall displays the missing application dependencies in the window for each rule. You must add these applications to some rule in the policy. After adding the missing applications, perform another commit and verify no more reported application dependency warnings.

Implicit Applications

- Many common applications implicitly allow parent applications.
- *No need* to explicitly define these applications in a Security policy rule:
  - The are automatically allowed.

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION
1	Allow-Facebook	Users_Net	universal	Users_Net	any	any	Internet	any	facebook-apps facebook-base facebook-chat	application-default	any	Allow

facebook-base implicitly allows web-browsing and ssl, so no need to add a rule for them.

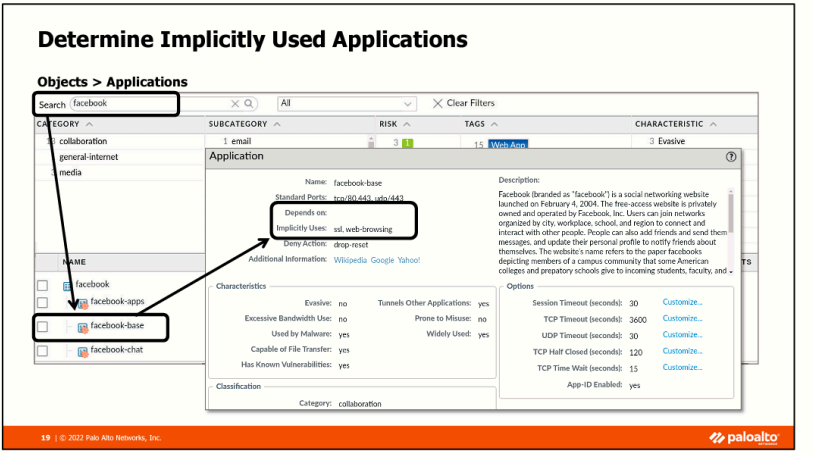
For a Tech Doc about this topic, log into Live and search for "Applications with Implicit Support"

For many applications, the App-ID database implicitly allows the required parent application without the need for you to add the parent application to the Security policy explicitly. In the example, the facebook-base application implicitly allows the required web-browsing application without the need for you to add a web-browsing rule to the Security policy explicitly. The facebook-chat and facebook-apps applications 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 adding parent applications to a rule in the Security policy could allow more traffic than intended. For example, the enablement of web-browsing to allow facebook-base would enable 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.

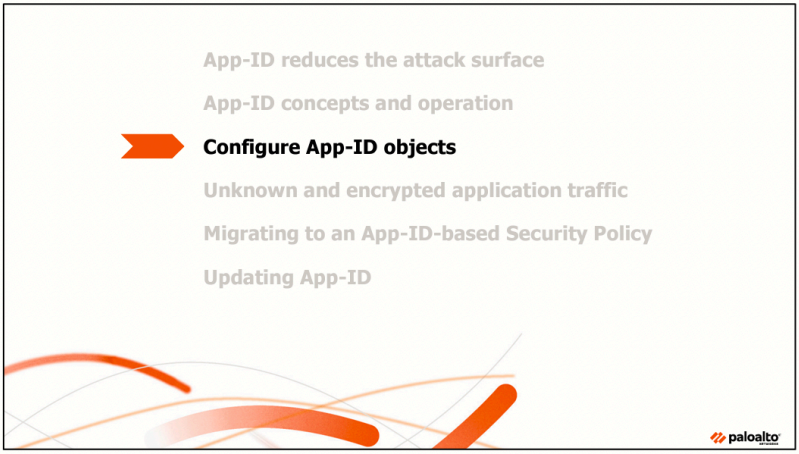
Implicit permissions for a parent application are processed only if you have not added an explicit Security policy rule for the parent application.

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



You can determine implicitly allowed applications using the firewall web interface or the Applipedia website at https://applipedia.paloaltonetworks.com. 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.

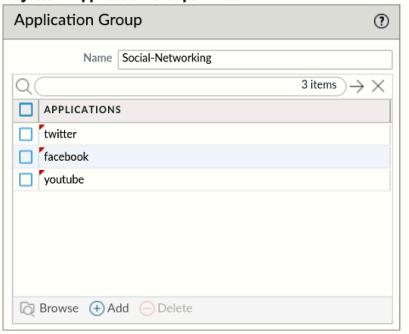
In this example, facebook-base implicitly allows the parent applications ssl and web-browsing.



This section describes the concepts and operation of App-ID.

Application Groups

Objects > Application Groups > Add



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

Unlike the dynamic list of applications in an application filter, an application group is a static, administrator-defined set of applications. Application groups enable you to create a logical grouping of applications applied to Security and QoS policy rules.

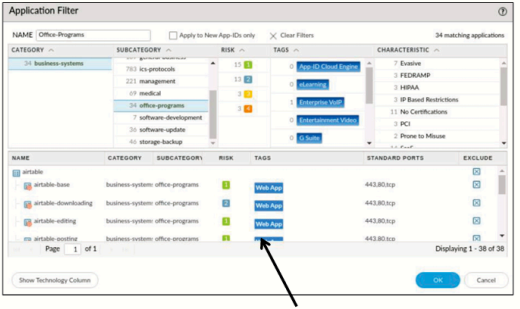
An application group is used to treat a set of applications similarly in a policy. Application groups ultimately simplify the administration of your rule bases. Instead of adding the same list of applications to multiple rules, you can create an application group and add the group to multiple rules. 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 you want to make available for any known user in your organization. In this case, you create separate application groups for each policy goal.

As another example, although best practice enables 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.

Application Filters

Objects > Application Filter > Add



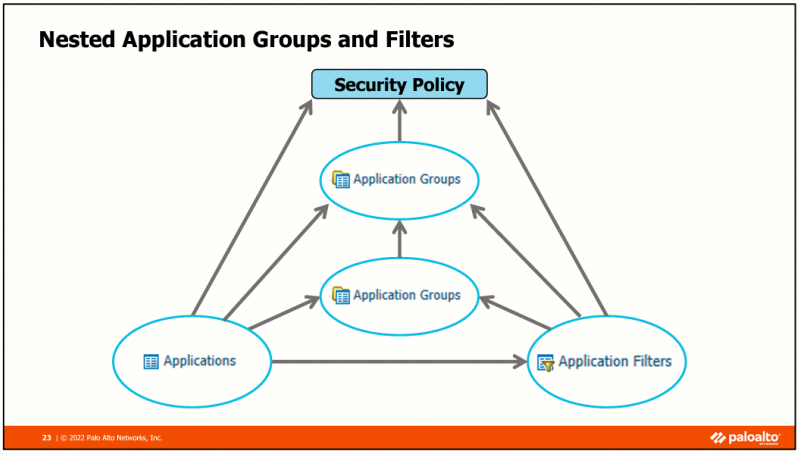
Application tags can be used as application filters.

- Dynamic group 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**, **Risk**, **Tags**, and **Characteristic**.

Application filters are useful when you enable access to applications that match filter criteria rather than match specific application names. For example, you might want to allow employees to choose their office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. As shown in this example, to enable these types of applications, create an application filter that matches the Category business-systems and the Subcategory office-programs.

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

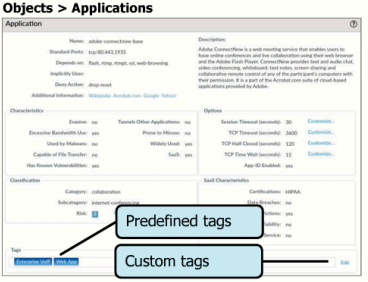


An application group is manually configured to include applications, application filters, and other applications groups. The diagram illustrates the possible ways that application groups and filters can be nested.

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

Predefined and Custom Application Tags

Objects > Applications



- Palo Alto Networks assigns one or more tags to applications in App-ID:
  - Starting with PAN-OS 9.1
- Tags are updated as part of normal *Applications and Threats* content updates
- To use tags in Security policy:
  1. Use tags in application filters.
  2. Use application filters in Security policy.

Application filter filtering on Enterprise VoIP tag

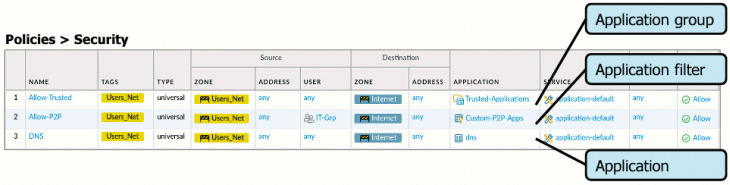
			Source		Destination				
	NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION
1	Permit-VOIP	Users_Net	Users_Net	any	Internet	any	Allow-VOIP	application-default	Allow

Palo Alto Networks assigns one or more predefined tags to applications in the App-ID database. Palo Alto Networks maintains these tags over time as part of the weekly *Applications and Threats* content updates. You can indirectly use these tags in Security policy rules to control application traffic. Rules-based on Palo Alto Networks-defined application tags will automatically update to handle a new list of applications any time Palo Alto Networks updates its application tags and distributes the update via weekly content update. These weekly updates to the application tags could simplify ongoing policy maintenance. You can create custom application tags using the **Edit** link in an App-ID application's **Application** window.

To use predefined or custom application tags in Security policy rules, use the tags to build an application filter. Then use the application filter in the **Application** column of a Security policy rule.

In the example shown here, the *adobe-connectnow-base* application has the Palo Alto Networks pre-assigned tags *Enterprise VoIP* and *Web App*. Then an *Allow-VOIP* application filter was created that filters the App-ID database for all applications assigned the *Enterprise VoIP* tag. Finally, the Allow-VOIP application filter was added to the *Permit-VOIP* Security policy rule. The result is that any user in the Users_Net zone can access any application in the *Internet* zone if the application has been assigned the *Enterprise VoIP* tag.

App-ID in Policy Rules Reduces the Attack Surface



- Implement App-ID using a positive enforcement model:
  - Specify what to allow rather than what to block.
- Implement policy by application rather than by port:
  - Specify applications, application groups, application filters.

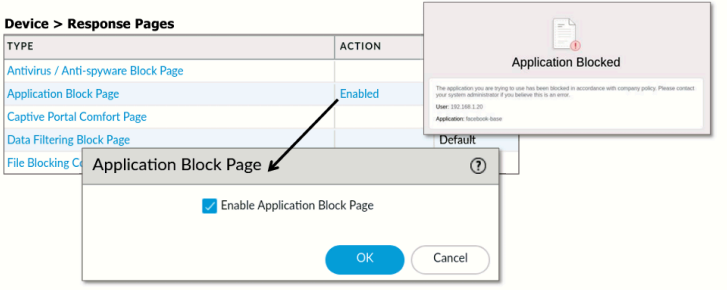
App-ID reduces the attack surface because only permitted applications can traverse the network. There are fewer avenues of attack when you limit the number of services and applications permitted on the network.

App-ID enables your organization to transition to a positive enforcement model where you configure the types of network traffic to allow rather than which types to block. You can enable sanctioned applications and application functions while blocking or controlling any remaining applications and unknown traffic. In an *application-based* policy, the identity of an application becomes the basis for a firewall policy and a port number. If you also enable User-ID, you can specify which users and groups can use the sanctioned applications. Use App-ID and User-ID together to reduce the cyberattack across your organization significantly.

You can use specific application names in the firewall policy rules. However, you can also create application groups or apply application filters and specify them in policy rules for added flexibility.

Application Block Page

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



If the **Application Block Page** is enabled and a Security policy rule denies a web-based application, a browser-based response page is displayed. The default response page includes the prohibited application name and the user's name if configured in the User-ID feature. 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 *PAN-OS 10.2 Administrator's Guide* https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin.html.

View Applications used in the Traffic Log

- App-ID labels traffic in logs and reports.
- The goal is to reduce the number of illegitimate or unknown applications allowed by the firewall.

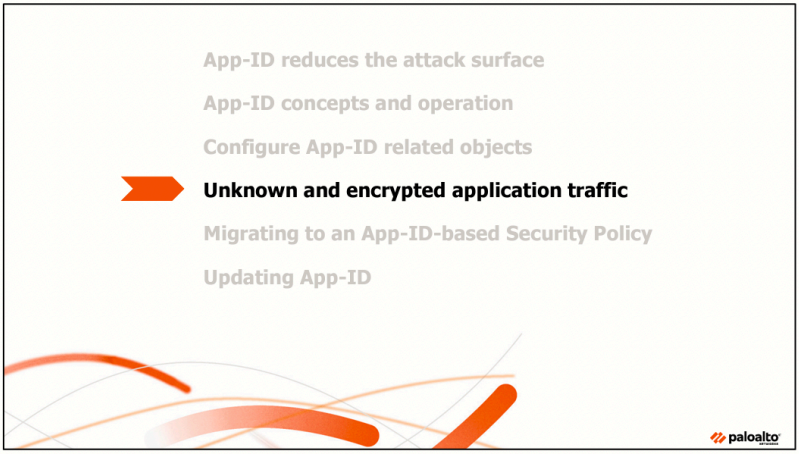
Monitor > Logs > Traffic

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES
	07/20 22:54:12	end	Users_Net	Internet	192.168.1.20	69.171.250.63	443	instagram-base	allow	Allow-Trusted	tcp-fin	17.0k
	07/20 22:54:12	end	Users_Net	Internet	192.168.1.20	69.171.250.174	443	instagram-base	allow	Allow-Trusted	tcp-fin	1.2M
	07/20 22:54:03	end	Users_Net	Internet	192.168.1.20	69.171.250.174	443	instagram-base	allow	Allow-Trusted	tcp-fin	8.2k
	07/20 22:53:49	end	Users_Net	Internet	192.168.1.20	184.31.10.237	443	twitter-base	allow	Allow-Trusted	tcp-fin	54.6k
	07/20 22:53:42	end	Users_Net	Internet	192.168.1.20	172.217.14.174	80	google-base	allow	Allow-Trusted	tcp-fin	912
	07/20 22:53:37	end	Users_Net	Internet	192.168.1.20	184.31.10.237	443	twitter-base	allow	Allow-Trusted	tcp-fin	7.1k
	07/20 22:53:27	end	Users_Net	Internet	192.168.1.20	184.31.10.237	443	twitter-base	allow	Allow-Trusted	tcp-fin	2.6k
	07/20 22:53:25	end	Users_Net	Internet	192.168.1.20	3.225.55.231	443	instagram-base	allow	Allow-Trusted	tcp-fin	12.9k
	07/20 22:53:18	end	Users_Net	Internet	192.168.1.20	192.229.210.163	443	twitter-base	allow	Allow-Trusted	tcp-fin	8.8k
	07/20 22:53:07	end	Users_Net	Internet	192.168.1.20	72.21.91.70	443	twitter-base	allow	Allow-Trusted	tcp-rst-from-client	3.4k

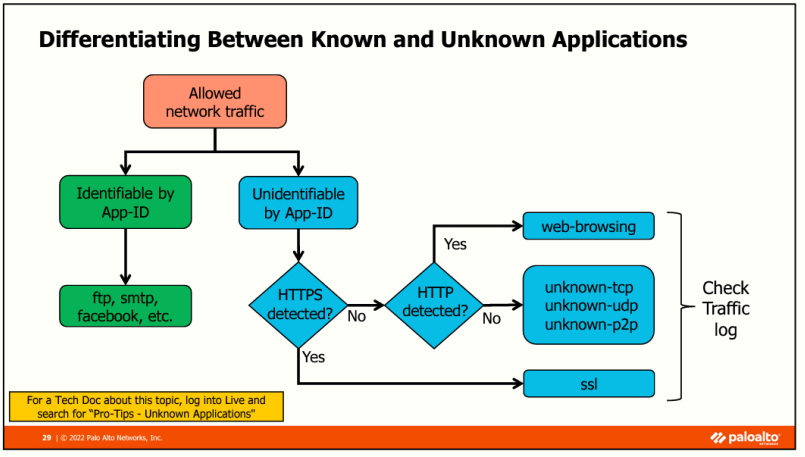
App-ID labels traffic observed by the firewall. The label is displayed in various logs and reports as an application name. Shown here is the Traffic log with the **Application** column highlighted. Notice that App-ID has labeled specific applications such as Instagram-base, twitter-base, and google-base. App-ID may also apply generic labels such as incomplete, unknown-udp, and insufficient-data to other traffic.

The goal of reading the log is to use the information to reduce the number of illegitimate or unknown applications that are allowed by the firewall. You can reduce or eliminate any unknown applications that traverse the data center perimeter by monitoring the log.

Use custom application labels to label unknown internal or commercial applications, and then modify Security policy rules to control this traffic. Also, remove or modify any Security policy rules that allow illegitimate traffic.



This section describes how to configure App-ID-related objects.



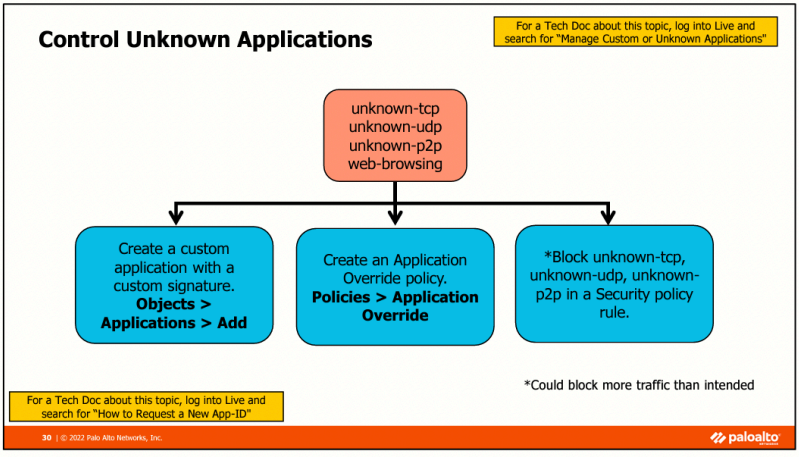
Applications can be divided into two main categories: applications known to App-ID and applications unknown to App-ID.

Applications known to App-ID are labeled in the Traffic log and reports. For example, an application could be identified as *ftp* or *facebook*.

Initially, applications unknown to App-ID might be identified as generic SSL if HTTPS is detected. If you have configured the firewall to decrypt the traffic, then App-ID might further identify the decrypted traffic as a specific application.

If HTTP is detected rather than HTTPS, then applications unknown to App-ID initially might be identified as generic *web-browsing*. As more packet data becomes available, then App-ID might further identify the generic *web-browsing* application as something more specific. For example, *web-browsing* might be further identified as *google-docs-base*.

When App-ID cannot identify an application or label the traffic as generic *web-browsing*, then App-ID labels the traffic as *unknown-tcp*, *unknown-udp*, or *unknown-p2p*.



The firewall has at least three methods available for processing traffic identified only as unknown-tcp, unknown-udp, unknown-p2p, or web-browsing.

One method to control unknown applications is to block unknown-tcp, unknown-udp, or unknown-p2p traffic in the Security policy. This method could block more traffic than you intend. The unknown-tcp, unknown-udp, or unknown-p2p traffic seen inside an organization could be a benign, internally developed application. However, you should be particularly concerned about unknown-tcp, unknown-udp, or unknown-p2p traffic that appears in sessions traversing the data center perimeter.

Another method is to create a custom application rather than block unknown traffic. First, use a network packet capture to identify unique bit patterns in the application. Next, create a custom application signature to match that pattern and name the new custom application. Last, use the custom application in a Security, QoS, or PBF policy rule like you use the Palo Alto Networks predefined applications. Creating custom applications based on custom signatures is described in another course module.

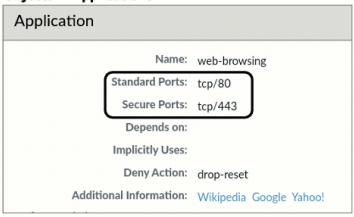
Yet another method for controlling unknown traffic is configuring an Application Override policy rule. For example, suppose you need to manage a custom application. In that case, an Application Override policy rule can be used to identify traffic for that application based on its source zone and IP address, its destination zone and IP address, and its port and protocol. You must create a Security policy rule to prevent the application from traversing between firewall security zones. The creation of an Application Override policy is described in another course module.

Control Applications on SSL-Secure Ports

- *Application-default* matches:
  - Cleartext applications on their **Standard Ports**
  - SSL-encrypted applications on their **Secure Ports**
- Supported applications are:
  - web-browsing
  - SMTP
  - FTP
  - LDAP
  - POP3
  - IMAP

For more information about this topic, see the module in this course on "Using decryption to Block Threats in Encrypted Traffic"

Objects > Applications



Before the PAN-OS 9.0 release, selecting the *application-default* service setting in a policy rule enabled you to allow applications only on their App-ID-defined standard ports. However, an SSL encrypted application might use a different default port than the standard port it uses when in cleartext.

Starting with the PAN-OS 9.0 release, the *application-default* service setting has been extended to allow specific SSL-encrypted applications on their default SSL *secure ports*, in addition to the application's standard ports. For a cleartext session, the *application-default* matches against the **Standard Ports** for the application. For an encrypted session, the *application-default* matches the **Secure Ports** for the application.

For example, a Security policy designed to allow web-browsing on only the *application-default* ports now will allow cleartext web-browsing traffic on the standard TCP port 80 *and* SSL-encrypted web-browsing traffic on the secure TCP port 443.

The *application-default* setting for both standard and secure ports is supported for the applications web-browsing, SMTP, FTP, LDAP, POP3, and IMAP. You can view the Standard Ports and Secure Ports that Palo Alto Networks has defined for the application by navigating to Objects > Applications for any of these applications.

Any pre-existing Security policy rules designed to allow applications—especially web-browsing—on port 443 using the predefined service *service-https* should be updated to use the service application-default instead.

Control Applications on Non-Standard Ports

Policies > Security

	NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
1	Block-SSH-Evasion	universal	Users_Net	any	any	any	Internet	any	any	ssh ssh-tunnel	any	any	Deny
2	Allow-RDP	universal	Users_Net	any	any	any	Extranet	any	any	ms-rdp	application-default	any	Allow
3	Allow-MySQL	universal	Users_Net	any	any	any	Extranet	any	any	mysql	Service-MySQL-45451	any	Allow

- Malicious traffic often uses non-standard application ports.
- Rule 1 blocks SSH tunnels on the standard *or* non-standard ports.
- Rule 2 allows RDP traffic on *only* standard ports.
- Rule 3 allows mysql traffic only on a non-standard port.

Objects > Applications

Application

Name: mysql
Standard Ports: tcp/3306
Depends on:
Implicitly Uses:
Deny Action: drop-reset
Additional Information: Wikipedia Google Yahoo!

Malicious traffic often uses non-standard application ports to evade network security features. Select the value application-default in the Service column in your Security policy to block applications not running on standard ports. This option is recommended for allow rules because it prevents applications from running on unusual ports and protocols, which can be a sign of undesired application behavior if it is not intentional.

Rule 1 blocks SSH tunnel traffic on any port (standard or non-standard) because of the **any** in the **Service** column. Rule 2 allows RDP traffic on only standard ports because of the **application-default** in the **Service** column. Rule 3 allows MySQL traffic on only non-standard port 45451 because of the custom **service-mysql45451** in the **Service** column.

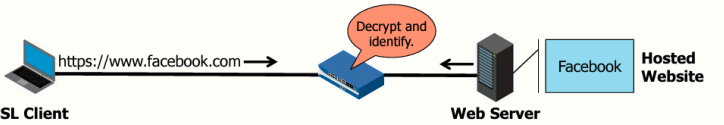
Note: When you use **application-default** in the **Service** column, the firewall still identifies all applications on all ports. However, the Security policy will match only traffic for applications using their default ports and protocol.

Supplemental Notes

Three options are available for the **Service** column:

- **application-default**: This choice specifies that the matched application is allowed or denied only on its standard ports defined by Palo Alto Networks.
- **any**: This choice matches all TCP or UDP ports from 1 to 65535. The specified application is allowed or denied on any protocol or port.
- **select**: This choice requires that you specify which TCP or UDP port the application can use to match the policy rule. Choose an existing service or create a custom service by browsing to **Objects > Services** and clicking **Add**.

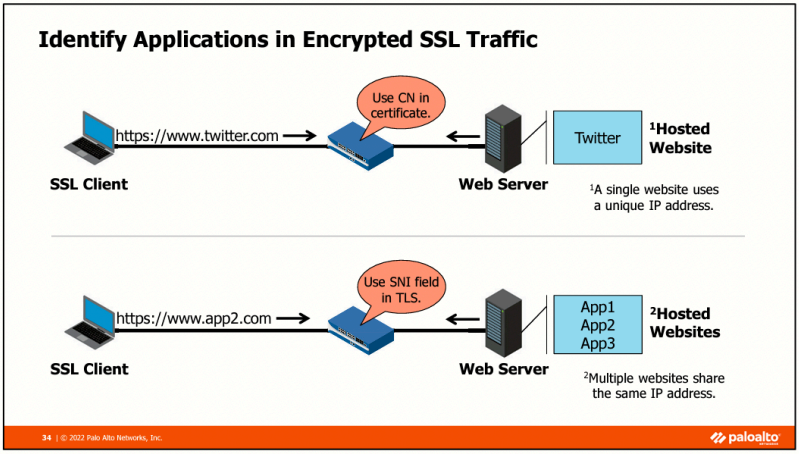
Identify Applications in Decrypted SSL Traffic



- SSL encrypts application-layer data.
- The firewall can identify and decrypt SSL traffic.
- App-ID identifies applications in decrypted SSL traffic:
  - Uses signatures, decoders, behavioral heuristics

The application layer data is encrypted when an SSL/TLS client connects to a secure web server. However, App-ID can identify SSL/TLS traffic. If you configure the firewall to decrypt the SSL/TLS traffic, App-ID can use signatures, decoders, and behavioral heuristics to identify the application.

In the example, a user on the SSL client connects to the webserver that hosts the Facebook website. The firewall is configured to decrypt and inspect the traffic to identify the application-layer data.



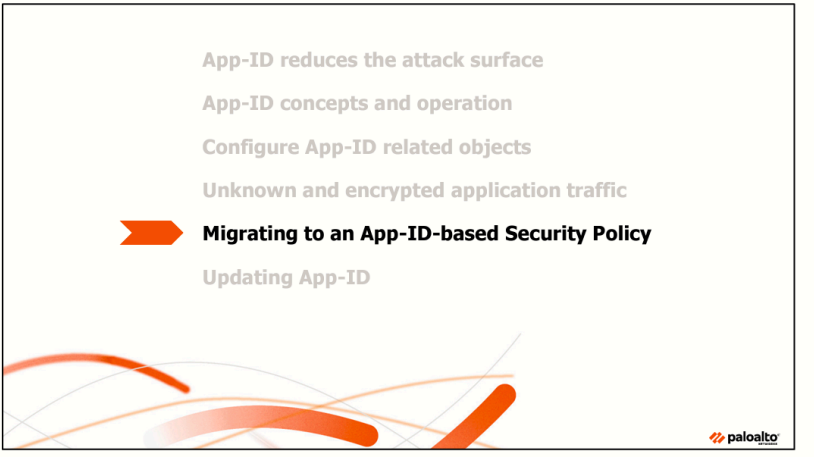
App-ID cannot use signatures and decoders to identify applications in encrypted traffic. However, the firewall attempts to identify the encrypted application using two other methods. The first method relies on the Common Name field in a certificate, which typically contains either the FQDN of the server or its IP address. The second method relies on a TLS protocol extension named Server Name Indication (or SNI), enabling multiple hostnames to be served over HTTPS from the same IP address.

If a web server hosts only a single website, then the Common Name (or CN) identifies the application. The SSL client initiates an SSL/TLS connection to the webserver and requests access to the website. The web server responds with its certificate. The firewall uses the FQDN in the CN field to identify the application. In the example, the SSL client initiates a connection to www.twitter.com. The web server certificate, which includes the Common Name www.twitter.com, identifies the application as Twitter.

The requirement that every website have its own unique FQDN and IP address is not practical, so many web servers host multiple websites. The CN field of a certificate cannot be used to identify the application because multiple web-based applications share a common FQDN and IP address. Instead, the firewall can use SNI to attempt to identify the application.

During the TLS handshake, browsers and applications use SNI to send the webserver to the FQDN they want to connect to. The firewall reads the SNI field and attempts to use the FQDN in the SNI to identify the application. The web server reads the SNI field to determine which certificate to send back to the client to verify the website's identity. In the example, the SSL client initiates a connection to www.app2.com and includes www.app2.com in the SNI field. The firewall uses the SNI information to identify the application.

Suppose the firewall cannot identify the traffic using the CN field in the certificate or the SNI field in the TLS handshake. In that case, the traffic is identified generically as SSL.



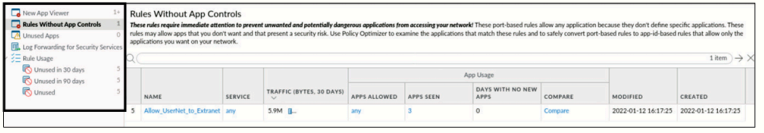
This section describes how to configure App-ID-related objects.

Policy Optimizer

For a Tech Doc about this topic, log into Live and search for "Security Policy Rule Optimization"

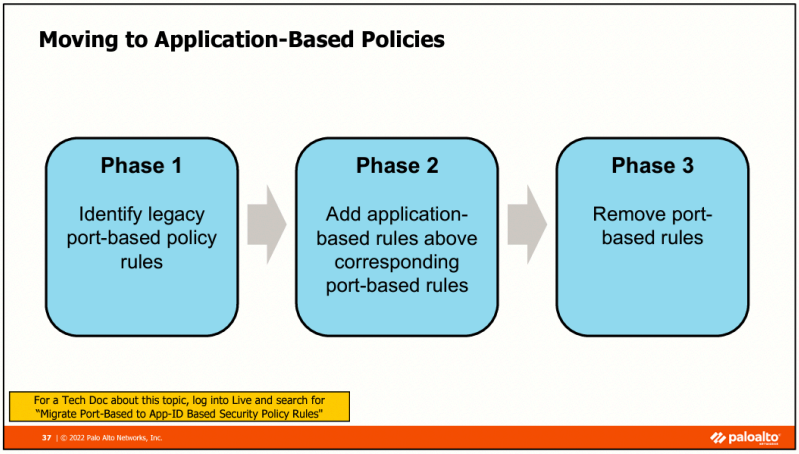
- Migrate port-based rules to App-ID-based rules
- Help reduce attack surface and provide information about application usage
- Prevent evasive applications from running on non-standard ports
- Identify over-provisioned application-based rules

Policies > Security > Policy Optimizer > Rules Without App Controls



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 add the appropriate applications to your cloned rule. You improve your security posture when converting port-based rules to application-based rules because you select the applications you want to allow or allowlist and deny all other applications. This conversion to application-based rules can also prevent evasive applications from running on non-standard ports when combined with restricting application traffic to its default ports. When you allow the appropriate applications over the correct 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 you do not use on your network. The use of too broad rules in scope increases your attack surface and puts your network at risk of inadvertently allowing malicious traffic.

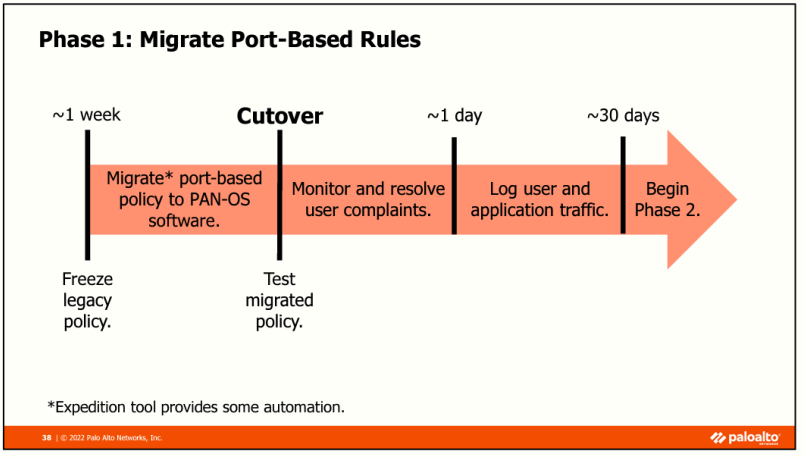


The graphic illustrates one way to implement the *migration* method to migrate an existing port-based policy to an application-based policy.

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 the migration of a large rulebase at one time. It allows you to ensure that new application-based rules control the necessary applications more efficiently. 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 checking the legacy port-based rule. Matching 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 policy rules to determine whether traffic is continuing to match any legacy port-based rule. If no legitimate traffic matches a legacy rule, that legacy rule can be safely removed. The corresponding application-based rule is updated to match the traffic if traffic has matched a legacy rule. At the end of Phase 3, you will have removed all or most legacy rules, and the attack surface will be minimized.



Several days before the migration begins, stop changes to your legacy firewall policy and start the like-for-like migration of the legacy, port-based policy to PAN-OS software. Palo Alto Networks offers the Expedition migration tool that can help to automate some of this process. Information about how to use Expedition is outside the scope of this course.

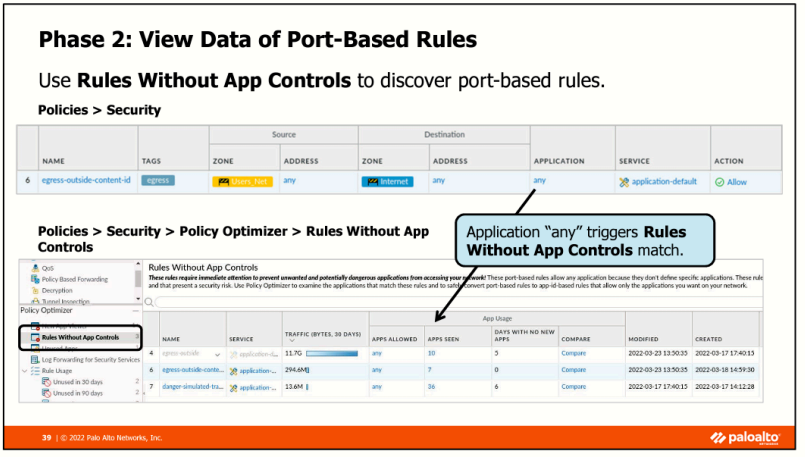
Perform the cutover from the legacy firewall to the Palo Alto Networks firewall during a maintenance window. Following the cutover, test the configuration to verify that the Security policy of the new firewall is working as expected. Monitor the firewall on the first business day after the cutover to ensure that any user-reported complaints are addressed and that the firewall is performing as expected.

From this point, the Palo Alto Networks firewall will be operating as a port-based firewall on the production network. Run the firewall in this mode for up to 30 days to collect application traffic information in the Traffic log. As the firewall logs application traffic, use the log information to convert your port-based rules to application-based rules. After running the firewall for 30 days, most of your applications should have been logged by the firewall. You should move to application-based rules as soon as possible because these rules reduce your attack surface.

Supplemental Notes

Use the Security policy's Policy Optimizer tool or the Traffic log to determine which applications matched which rules. The firewall (or Panorama) must maintain at least 30 days of logs. View the earliest traffic log entry in the web interface to determine if it was recorded at least 30 days earlier.

For additional information about the Expedition migration tool, log into Live and search for "Expedition documentation" or see https://live.paloaltonetworks.com/t5/Expedition-Articles/Expedition-Documentation/ta-p/215619. This URL provides *Expedition Administrator's Guide*, *Expedition Hardening Guide*, and *Expedition User's Guide*.



After 30 days, the firewall should have logged enough traffic and application data to allow you to move to Phase 2 of the migration process. In Phase 2, you add application-based rules to the Security policy. Browse to **Policies > Security > Policy Optimizer** and click **Rules Without App Controls** to start the process.

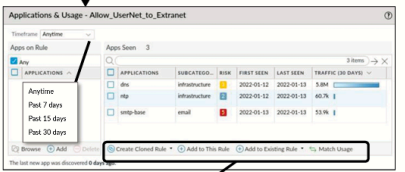
Rules Without App Controls displays all port-based Security policy rules. The firewall considers any rule port-based if its **Application** field is configured as "any." In the example, the egress-outside-content-id rule in the Security policy has its **Application** field configured as "any." This rule allows any application traffic from the Users_Net zone to the Internet zone on the defined default ports for an application.

Supplemental Notes

The firewall is scheduled to process 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 **Rules Without App Controls** window. You cannot customize the scheduled time.

Phase 2: Discover Applications Matching a Port-Based Rule

Policies > Security > Policy Optimizer > Rules Without App Controls



- 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).

Four options to convert the policy

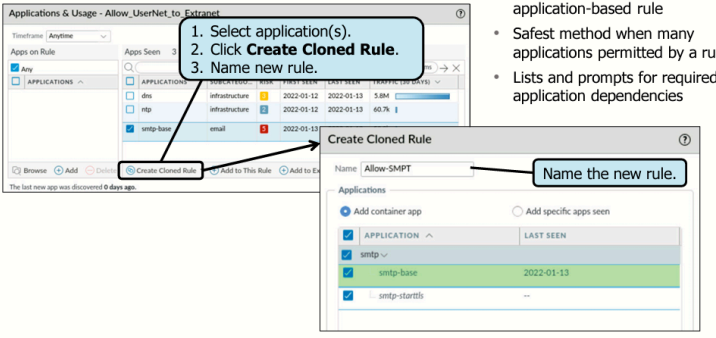
You must do more than locate your port-based rules. You also must convert them so that they control the specific applications that are used in your organization. In the **Rules Without App Controls** tool, pick a Security policy rule and click the number in the **Apps Seen** column or the word **Compare** in the **Compare** column. The **Applications & Usage** window for the rule 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 four options to convert a port-based rule into 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. The **Add to This Rule** and **Match Usage** options *replace* the port-based rule with an application-based rule. The **Add to Existing Rule** option adds the application to another Security policy rule of your choice.

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

Phase 2: Clone a Port-Based Rule Using "Create Cloned Rule"

Option 1 of 4:



- *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

41 | © 2022 Palo Alto Networks, Inc.

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

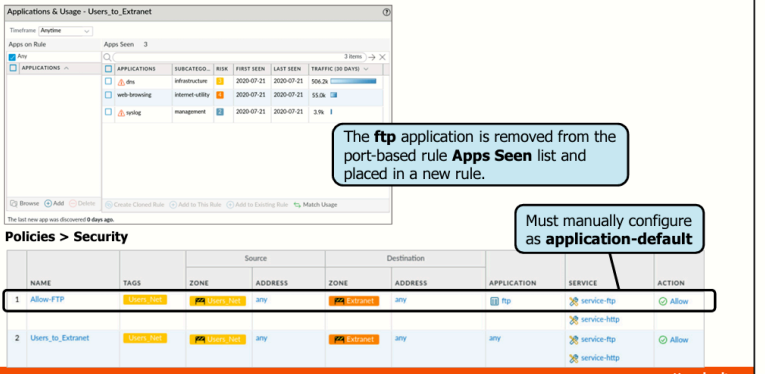
Start by selecting only those applications from the **Apps Seen** column you want to allow in the new, cloned rule. Then click **Create Cloned Rule**, which opens a new **Clone** window, where you are prompted to enter a name for the new cloned rule. The **Create Cloned Rule** window also lists any applications required by the applications in the cloned rule. These applications are known as application dependencies. You can select and add these applications to a rule in the Create Cloned Rule window. The window also prompts you to add either the specific application or the container app to which the application belongs. For example, gmail-base and gmail-posting are part of the container app named gmail.

Finish by clicking **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 various 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, you can remove it to complete the migration of that rule.

Result of "Create Cloned Rule"



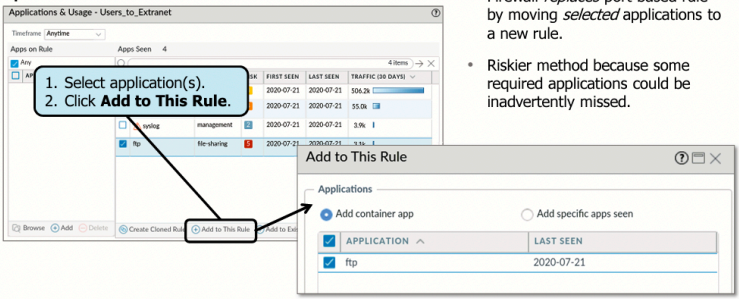
The screenshots illustrate the result of cloning a port-based rule to add a new application-based rule. The firewall removes the **ftp** application from the port-based rule **Apps Seen** list because the new cloned rule will now control the application.

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, you can eventually disable and remove the port-based rule.

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

Phase 2: Replace a Port-Based Rule Using "Add to This Rule"

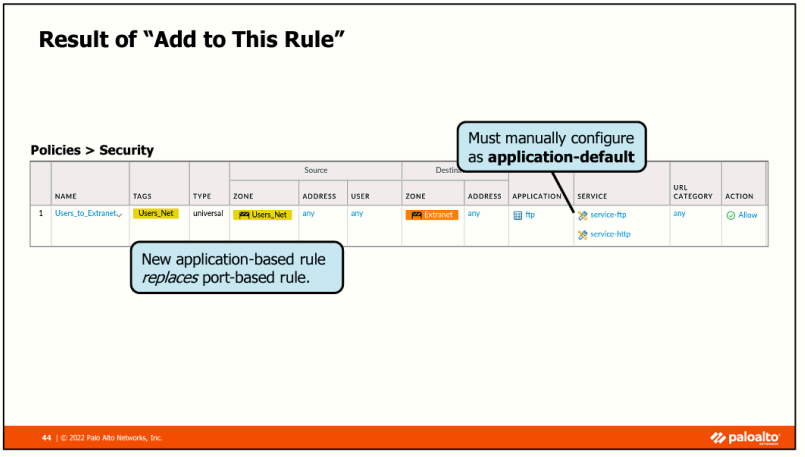
Option 2 of 4:



- Firewall *replaces* port-based rule by moving *selected* applications to a new rule.
- Riskier method because some required applications could be inadvertently missed.

Add to This 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 you want to allow in the new replacement rule. Then click **Add to This Rule**. A window opens that prompts you to add either the specific application or the container app to which the application belongs. For example, gmail-base and gmail-posting are part of the container app named gmail.

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.

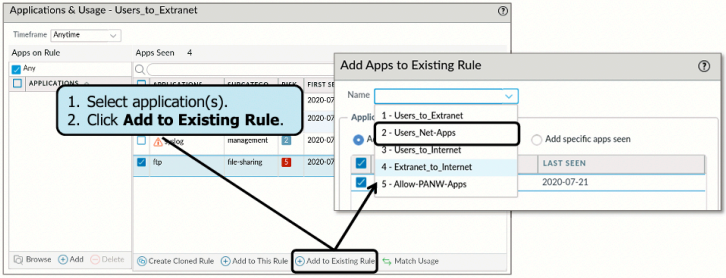


The screenshot illustrates replacing a port-based rule with a new application-based rule. Only the selected application or applications were placed into the new application-based rule. Even though web-browsing matched the original port-based rule, it is not included in the new rule because it was not selected. This rule conversion method can be riskier because you might inadvertently miss applications that should be on the rule. Still, the original port-based rule is removed and cannot catch any accidental omissions. However, this method is quick and easy to convert a port-based rule with only a few well-known applications.

The new application-based rule is placed where the original port-based rule formerly existed in the security policy. After you perform a commit, this placement ensures that the application-based rule will match FTP traffic. To finish modifying the rule, you must manually edit the rule, modify the **Service** to **application-default**, and then perform a commit to activate the new configuration.

Phase 2: Replace a Port-Based Rule Using "Add to Existing Rule"

Option 3 of 4:

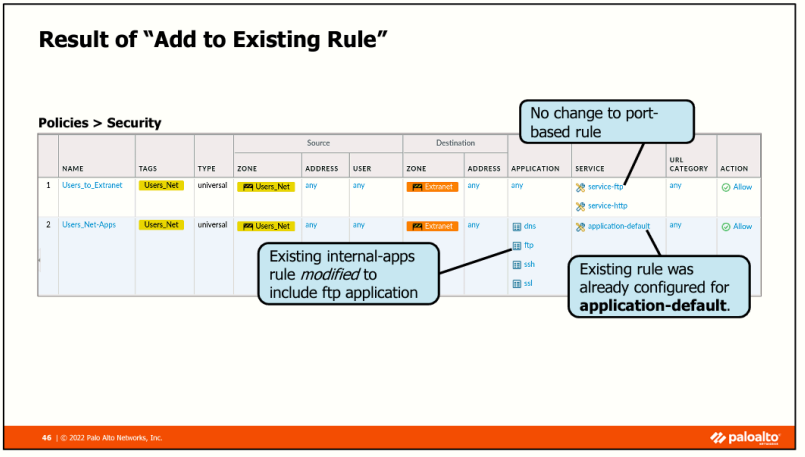


45 | © 2022 Palo Alto Networks, Inc.

Add to Existing Rule is the third 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 add to an existing rule. Then click **Add to Existing Rule**. A window opens that prompts you to add either the specific application or the container app to which the application belongs. For example, gmail-base and gmail-posting are part of the container app named gmail.

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.

Then click **OK** in the **Add Apps to Existing Rule** window to change the security policy.

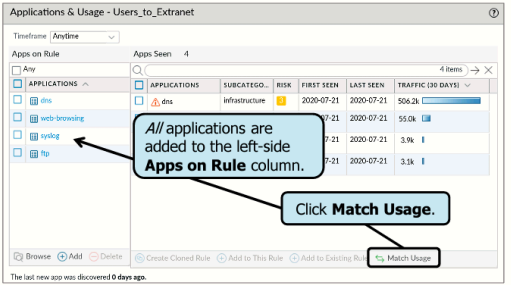


The screenshot illustrates the result of adding an application to an existing rule. Only the selected application or applications were placed into the new application-based rule. In this example, the ftp application was added to the internal-apps rule. Even though web-browsing matched the original port-based rule, it is not included in the new rule because it was not selected. The original port-based rule remains. You must decide what to do with the original port-based rule.

To finish modifying the rule, you might have to manually edit the rule, modify the Service to **application-default**, and then perform a commit to activate the new configuration. In the example here, the internal-apps rule was already configured with a **Service** of **application-default**.

Phase 2: Replace a Port-Based Rule Using "Match Usage"

Option 4 of 4:



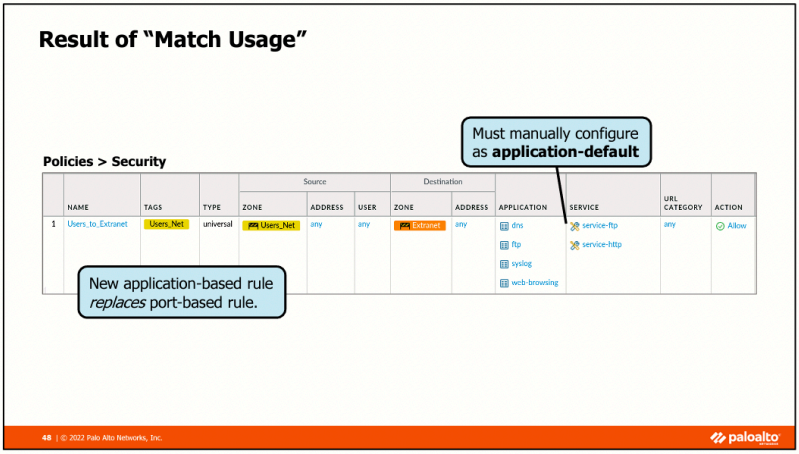
- Use only when the rule matches a small number of legitimate applications.
- Copies *all* applications under **Apps Seen** to **Apps on Rule**.
- Firewall *replaces* port-based rule with application-based rule.

47 | © 2022 Palo Alto Networks, Inc.

Match Usage is the fourth option to convert port-based policy rules to application-based policy rules. 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.

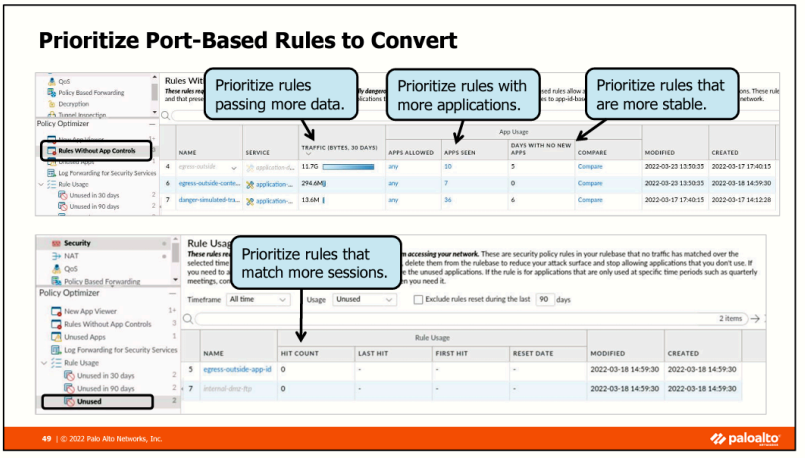
After you click **Match Usage**, the entire list of applications beneath **Apps Seen** is copied to the **Apps on Rule** column, and the tool uses these applications to build a new application-based rule. Be aware that the original port-based rule allowed any application on the allowed port so that **Apps 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 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.



The screenshot illustrates replacing a port-based rule with an application-based rule.

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



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 a migration of a large rulebase at one time, and you can more easily ensure that new application-based rules control the necessary applications.

Rules Without App Controls 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:

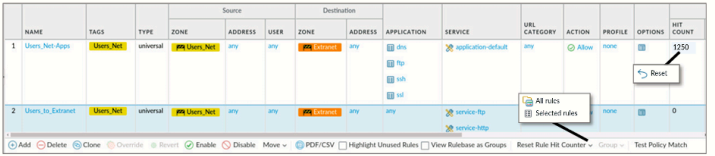
- **Traffic (Bytes, 30 days)**: The 30-day window places rules that *currently* pass the most data at the top of the list. A time span longer than 30 days might put more emphasis on older rules that would remain at the top of the list because they have large cumulative totals, even though they no longer might see much data transferred.
- **Apps Seen**: A large number of legitimate applications matching a port-based rule might indicate that you should replace the rule with multiple application-based rules that more tightly define the applications, the users, and the sources and destinations.
- **Days with No New Apps**: After the applications are shown on a port-based rule stabilize, you can be more confident the rule is mature, 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 most significant number of sessions over a selected 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 expected because you did not know the counter was reset.

Phase 3: Review Port-Based Rules

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

Policies > Security

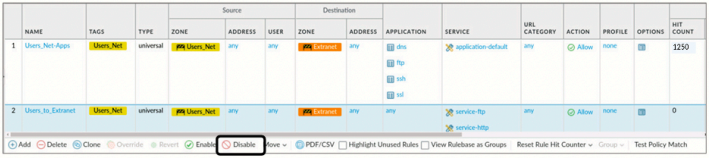


After 60 days, review the port-based rules to verify that no new traffic matches them. View the **Hit Count** column in the Security policy. A zero value in the **Hit Count** column indicates that a rule has not been used. You can also use the Last Hit column to determine the time elapsed since a rule 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, point to the current value until a drop-down arrow appears and select **Reset** from the drop-down menu. To reset a single rule or multiple rules, choose the rules, click **Reset Rule Hit Counter**, and select **Selected rules**. To reset all rules, click **Reset Rule Hit Counter** and select **All rules**.

Phase 3: Disable Port-Based Rules

Policies > Security



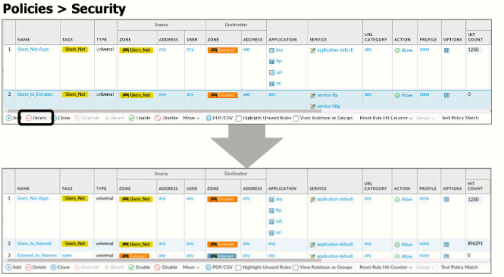
- Disable port-based rules that have not matched to any new traffic.
- Disabled rules are rendered in gray italic font.
- Tag rules that must be removed later (optional).

After reviewing 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 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.

Phase 3: Remove 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)



For a Tech Doc about this topic, log into Live and search for "Best Practices for Migrating to Application-Based Policy"

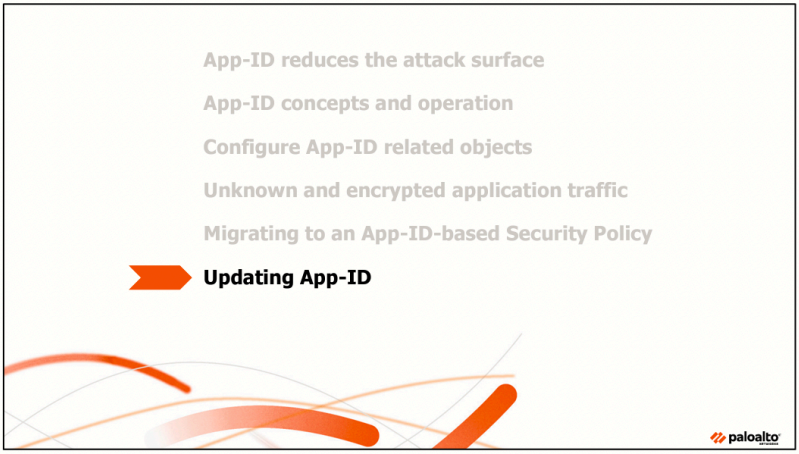
After 90 days, if no end-user issues have been reported with the application-based Security policy, then you can remove the disabled port-based rules. Removing the legacy rules in Phase 3 is critical for improving the security posture. The migration should not be considered complete until Phase 3 tasks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

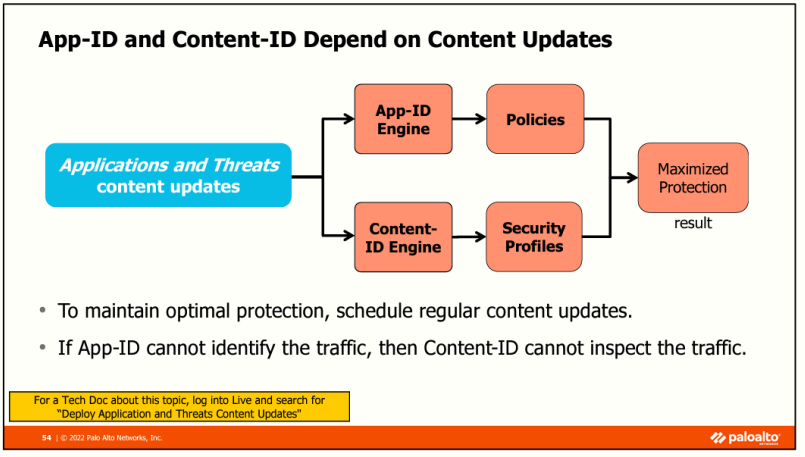
After you have completed Phase 3, any future Security policy rules should be added as application-based rules.

Supplemental Notes

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



This section describes how to configure App-ID-related objects.

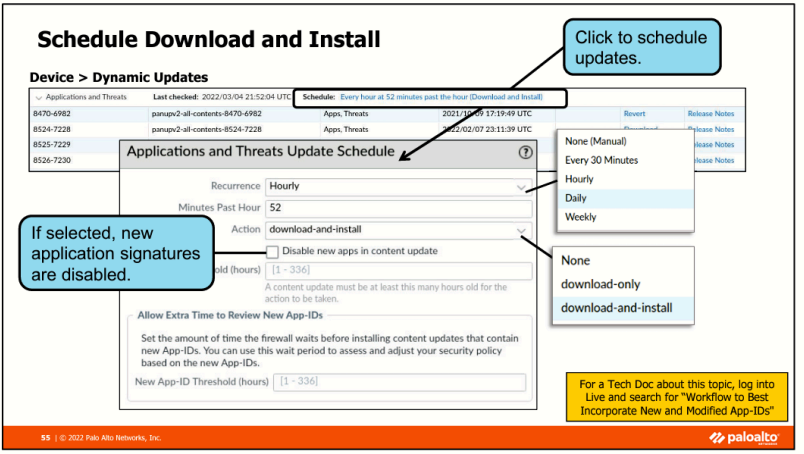


Application identification and content inspection depend on the *Applications and Threats* content updates. To maintain the most current protection level possible, you should schedule regular downloads and installation of new content updates.

If the App-ID engine cannot identify the traffic using signatures, decoders, contexts, or heuristics, the traffic is labeled as an *unknown,* and content inspection cannot be performed. Content-ID cannot inspect the traffic because, like the App-ID engine, does not know or have the decoders and contexts necessary to read and interpret the traffic. The three traffic types that App-ID labels as *unknown* are malware, internally developed applications, or commercially available applications. Palo Alto Networks has not yet added an application signature.

Supplemental Notes

The firewall does not always perform Content-ID inspection. For example, the firewall skips Content-ID inspection for traffic matched to a Security policy rule with no attached Security Profiles. Also, if your traffic matches an Application Override policy rule but has no predefined application signature, then no Content-ID inspection is performed. Configuration of an Application Override policy is described later in this course.



To schedule *Applications and Threats* content updates, browse Device > Dynamic Updates and click the current schedule. The **Applications and Threats Update Schedule** window opens. Set the Recurrence to **Every 30 Minutes** to ensure that your firewall sees new content updates within 30 minutes of their release. Also, choose a time to check for new updates. The firewalls in the example would check for new updates at 15 and 45 minutes after the hour.

From the **Action** drop-down menu, select **download-and-install**. A download transfers updated content to the firewall, including any new or updated application and threat signatures. New or updated *application* signatures are marked as *pending* and rendered in a gray, italicized font in the web interface. Neither *application* nor *threat* signatures are used for traffic inspection following a download operation.

The install operation removes the pending status from new *application* signatures. *Application* signatures are available to App-ID for policy evaluation, but policy rules cannot use updated application signatures until you perform a commit operation. The install operation makes any new or updated threat signatures immediately available to the Content-ID engine for traffic inspection. You do not need to perform a commit operation to use new or updated *threat* signatures.

The optional **Disable new apps in content update** check box disable any new application signatures and make them pending application signatures. You can use pending application signatures for policy checking but not policy enforcement. Palo Alto Networks recommends that you *not* disable new applications because individually re-enabling each disabled application could be time-consuming and cause errors.

In rare cases, a newly released content update could have an error that might take a few hours to detect, fix, and re-release. You can use the **Threshold** value to delay download and installation for a specified number of hours. A value of 24 to 48 hours is recommended for an application-uptime firewall and a value of 6 to 12 hours for a security-first firewall.

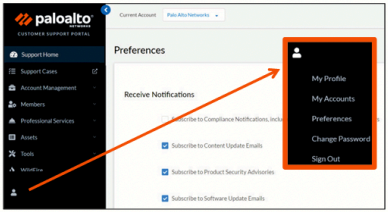
Use the **New App-ID Threshold (hours)** value to delay only content updates that include new application signatures. These content updates still are downloaded so that you can use the pending application signatures to review and update policy rules. A value of 24 to 48 hours is recommended for an application-uptime firewall and a null value for a security-first firewall. The delay for an application-uptime firewall provides you with time to review and update your policy rules.

Review Content Update Release Notes

Device > Dynamic Updates

VERSION	FILE NAME	FEATURES	RELEASE DATE	CURRENTLY INSTALLED	ACTION	DOCUMENTATION
Applications and Threats	**Last checked:** 2022/03/04 21:52:04 UTC	**Schedule:** Every hour at 52 minutes past the hour (Download and Install)				
8537-7273	panupv2-all-contents-8537-7273	Apps, Threats	2022/03/03 21:02:04 UTC		Install Review Policies Review Apps	Release Notes

https://support.paloaltonetworks.com



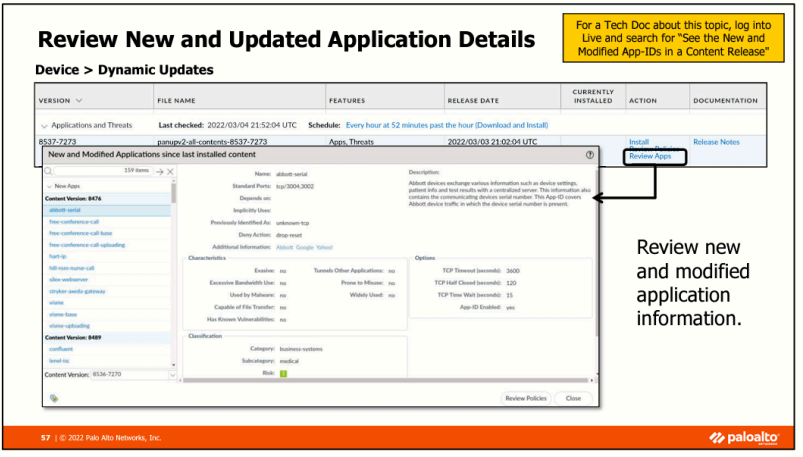
- Content Release Notes describe Security policy impacts.
- Get Content Release Notes from:
  - Firewall
  - Customer Support email

For a Tech Doc about this topic, log into Live and search for "Best Practices for Applications and Threat Content Updates"

Always review Content Release Notes for the list of newly identified and modified application and threat signatures that the content release introduces. Content Release Notes also describe how the update might impact existing Security policy enforcement and provide recommendations about how you can modify your Security policy to best leverage what is new.

You can review Content Release Notes for applications and threats directly on the firewall. Browse to **Device > Dynamic Updates** and click **Release Notes** for a specific content release version.

To subscribe to content update emails, visit the Customer Support Portal, edit your **Preferences**, and select **Subscribe to Content Update Emails**.



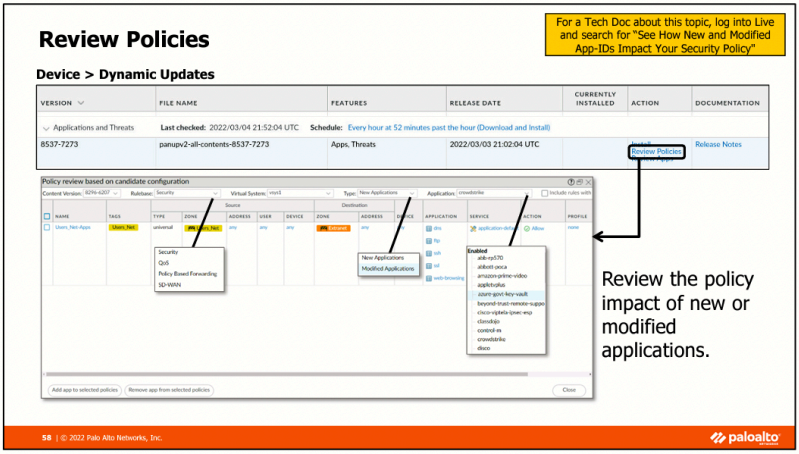
After you download a content update, the web interface displays a Review Apps link. Click **Review Apps** to open the **New and Modified Applications since the last installed content** window, which lists all new or updated application signatures included in the content update.

To assess possible impact to policy enforcement by new application signatures, look for the following fields:

- **Depends on**: Lists the application signatures that this App-ID relies on to uniquely identify the application. If one of the application signatures listed in the **Depends on** field is disabled, the dependent App-ID is also disabled.
- **Previously Identified As:** Lists the App-IDs that matched the application before the new App-ID was installed to identify the application uniquely.
- **App-ID Enabled**: All App-IDs display as enabled when a content release is downloaded unless you choose to disable the App-ID signature before installing the content update manually.

To assess possible impact to policy enforcement by modified application signatures, look for the following fields:

- **Expanded Coverage**, **Removed False Positive**: These fields indicate how the application's coverage has changed to be either more comprehensive or narrower.
- A clock icon that indicates a metadata change where specific application details have been updated.



Installation of new application signatures included in a content update sometimes can cause a change in policy enforcement for the application that is now identified differently.

After downloading and installing a new content release with new and updated application signatures, click **Review Policies** to review their policy impact. During a policy review, application signatures are compared against policy rules in the candidate configuration.

Select the application to compare against your policies by using the **Application** field. You can explore the policy impact of **New Applications** and **Modified Applications**. Use the **Content Version** field to compare other content updates to the candidate policies. Supported policies are the **Security**, **QoS**, **Policy Based Forwarding**, and **SD-WAN** policies. If you have a firewall capable of multiple virtual systems, you can modify the Virtual System field to modify which virtual system you view policy impacts.

Module Summary

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

- Identify how App-ID reduces the attack surface
- Describe App-ID concepts and operation
- Configure App-ID-based policy rules
- Update App-ID application database

Now that you have completed the module, you should be able to perform the tasks listed.

Additional Resources

For a digital review of this module, log into Beacon and search for:

"App-ID"

Review Questions

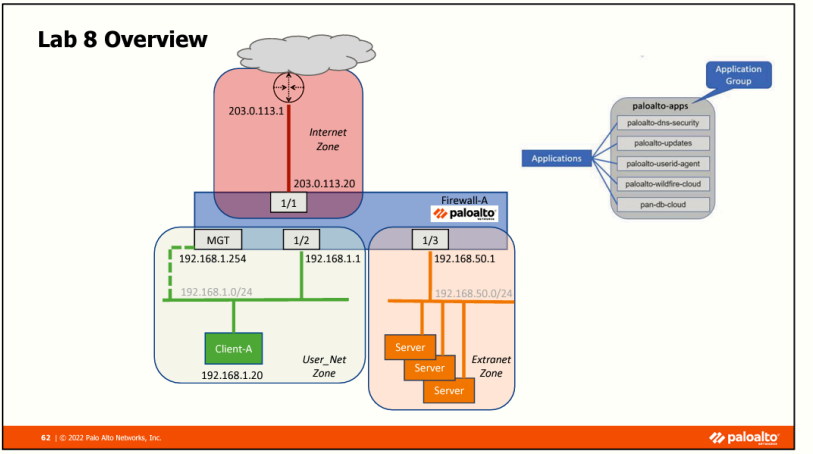
1. Which three methods does App-ID use to identify network traffic? (Choose three.)
   a. signatures
   b. protocol decoders
   c. heuristics
   d. URL category
   e. application filter match

2. How would App-ID label TCP traffic when the three-way handshake completes but not enough data is sent to identify an application?
   a. not-applicable
   b. incomplete
   c. insufficient-data
   d. unknown-tcp

3. True or false? When migration is done from another vendor's firewall to a Palo Alto Networks firewall, a best practice is always to migrate the existing Security policy.
   a. true
   b. false

4. True or false? If App-ID cannot identify the traffic, Content-ID cannot inspect the traffic for malware.
   a. true
   b. false

5. When an *Applications and Threats* content update is performed, which is the earliest point you can review the impact of new application signatures on existing policies?
   a. after clicking **Check Now**
   b. after download
   c. after install
   d. after commit



Your instructor can provide an overview of the lab environment and the details needed for this lab. See the following page for a list of tasks that you will carry out in this lab.

Lab 8: Controlling Application Usage with App-ID

- Load a baseline configuration
- Generate application traffic
- Configure an application group
- Configure a Security policy to allow update traffic
- Test the Allow-PANW-Apps Security policy rule
- Examine the tasks list to see shadowed message
- Modify the Security policy to function properly
- Test the modified Security policy rule

Answers to Review Questions

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