



TECHDOCS

Internet Gateway Best Practice Security Policy

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2023-2024 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

January 18, 2024

Table of Contents

Best Practice Internet Gateway Security Policy.....	5
What Is a Best Practice Internet Gateway Security Policy?.....	6
Why Do I Need a Best Practice Internet Gateway Security Policy?.....	9
How Do I Deploy a Best Practice Internet Gateway Security Policy?.....	10
Identify Your Application Allow List.....	12
Map Applications to Business Goals for a Simplified Rulebase.....	12
Use Temporary Rules to Tune the Allow List.....	13
Application Allow List Example.....	14
Create User Groups for Access to Allowed Applications.....	17
Decrypt Traffic for Full Visibility and Threat Inspection.....	18
Transition Safely to Best Practice Security Profiles.....	21
Transition Vulnerability Protection Profiles Safely to Best Practices.....	22
Transition Anti-Spyware Profiles Safely to Best Practices.....	24
Transition Antivirus Profiles Safely to Best Practices.....	27
Transition WildFire Profiles Safely to Best Practices.....	28
Transition URL Filtering Profiles Safely to Best Practices.....	29
Transition File Blocking Profiles Safely to Best Practices.....	29
Create Best Practice Security Profiles for the Internet Gateway.....	31
Best Practice Internet Gateway File Blocking Profile.....	31
Best Practice Internet Gateway Antivirus Profile.....	33
Best Practice Internet Gateway Vulnerability Protection Profile.....	34
Best Practice Internet Gateway Anti-Spyware Profile.....	36
Best Practice Internet Gateway URL Filtering Profile.....	38
Best Practice Internet Gateway WildFire Analysis Profile.....	44
Define the Initial Internet Gateway Security Policy.....	46
Step 1: Create Rules Based on Trusted Threat Intelligence Sources.....	46
Step 2: Create the Application Allow Rules.....	48
Step 3: Create the Application Block Rules.....	52
Step 4: Create the Temporary Tuning Rules.....	54
Step 5: Enable Logging for Traffic That Doesn't Match Any Rules.....	57
Monitor and Fine-Tune the Policy Rulebase.....	58
Remove the Temporary Rules.....	60
Maintain the Rulebase.....	61

Best Practice Internet Gateway Security Policy

One of the cheapest and easiest ways for an attacker to gain access to your network is through users accessing the internet. By successfully exploiting an endpoint, an attacker can enter your network and move laterally towards the end goal: stealing source code, exfiltrating customer data, or taking down infrastructure. To protect your network from cyberattacks and improve your overall security posture, implement a best practice internet gateway security policy. A best practice policy allows you to safely enable applications, users, and content by controlling all traffic, across all ports, all the time.

- [What Is a Best Practice Internet Gateway Security Policy?](#)
- [Why Do I Need a Best Practice Internet Gateway Security Policy?](#)
- [How Do I Deploy a Best Practice Internet Gateway Security Policy?](#)
- [Identify Your Application Allow List](#)
- [Create User Groups for Access to Allowed Applications](#)
- [Decrypt Traffic for Full Visibility and Threat Inspection](#)
- [Transition Safely to Best Practice Security Profiles](#)
- [Create Best Practice Security Profiles](#)
- [Define the Initial Internet Gateway Security Policy](#)
- [Monitor and Fine Tune the Policy Rulebase](#)
- [Remove the Temporary Rules](#)
- [Maintain the Rulebase](#)

Refer to the Palo Alto Networks series of [best practices books](#), which include planning, deployment, and maintenance best practices advice on subjects such as:

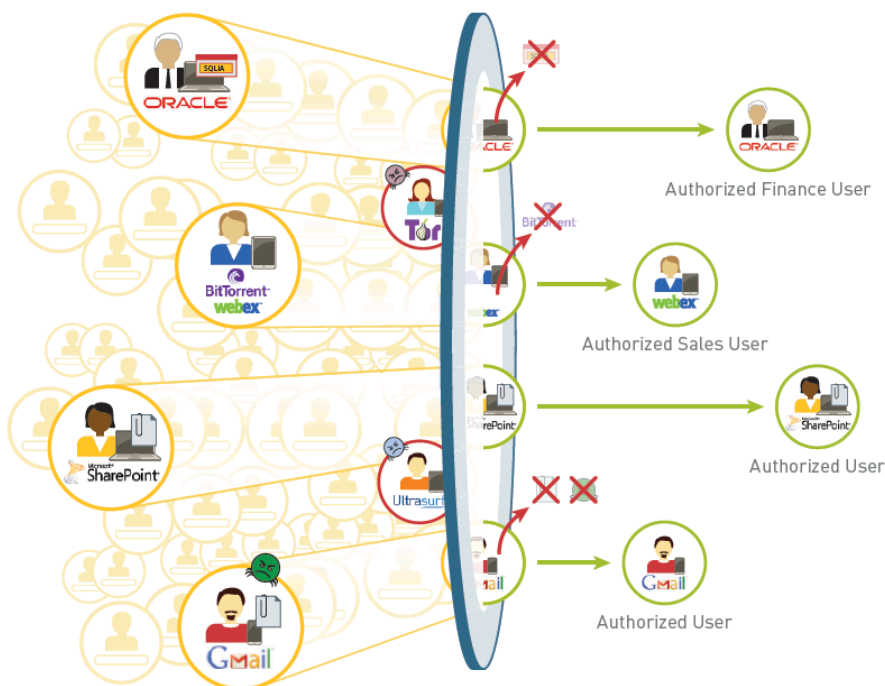
- [Decryption](#)
- [Security policy](#) (including Security policy rule construction, rulebase order and hygiene, the App-ID Cloud Engine (ACE), Policy Optimizer, SaaS Policy Recommendation, and IoT Policy Recommendation)
- [Zero Trust](#)
- [DoS & Zone Protection](#) (including Packet Buffer Protection)
- [Migrating to Application-Based Policy](#) (leveraging Policy Optimizer)
- [Administrative Access](#) to firewalls and management devices

What Is a Best Practice Internet Gateway Security Policy?

A best practice internet gateway security policy has two main security goals:

- **Minimize the chance of a successful intrusion**—Unlike legacy port-based security policies that either block everything in the interest of network security or enable everything in the interest of your business, a best practice security policy leverages App-ID, User-ID, Content-ID, and Device-ID (for IoT Security, which is beyond the scope of this book) to ensure safe enablement of applications across all ports, for all users, all the time, while simultaneously scanning all traffic for both known and unknown threats.
- **Identify the presence of an attacker**—A best practice internet gateway security policy provides built-in mechanisms to help you identify gaps in the rulebase and detect alarming activity and potential threats on your network.

To achieve these goals, a best practice internet gateway security policy uses application-based rules to allow user access to specific applications, scans all traffic to detect and block all known threats, and sends unknown files to WildFire to identify new threats and generate signatures to block them.



The best practice policy is based on the following methodologies, which ensure detection and prevention at multiple stages of the attack life cycle.

Best Practice Methodology	Why is this important?
<p>Inspect All Traffic for Visibility</p>	<p>Because you cannot protect against threats you cannot see, make sure you have full visibility into all traffic across all users and applications all the time:</p> <ul style="list-style-type: none"> • Deploy GlobalProtect to extend the next-generation security platform to users and devices no matter where they are located. • Enable decryption so the firewall can inspect encrypted traffic (every year a higher percentage of enterprise web traffic is encrypted and more malware campaigns use encryption). • Enable User-ID to map application traffic and associated threats to users/devices and to enable policy to follow users wherever they go. • If company policy allows users' devices on the network (BYOD or corporate devices without GlobalProtect or other security management applications installed), the unmanaged device access control on SaaS Security API enables users to access your cloud SaaS applications from personal devices, from any location, without inadvertently putting your data or organization at risk. Traffic is redirected through the firewall for policy enforcement and threat prevention. <p>With full visibility, the firewall can inspect all traffic—applications, threats, and content—and tie it to users, regardless of location or device type, port, encryption, or evasive techniques employed, thanks to native App-ID, Content-ID, and User-ID technologies.</p> <p>Complete visibility into the applications, content, and users on your network is the first step toward informed policy control.</p>
<p>Reduce the Attack Surface</p>	<p>After you gain context into the applications, content, and users on your network, create application-based Security policy rules to allow critical business applications and to block high-risk applications that have no legitimate business use case.</p> <p>To further reduce your attack surface, attach File Blocking and URL Filtering profiles to all rules that allow application traffic to prevent users from visiting threat-prone web sites and to prevent them from uploading or downloading dangerous file types (either knowingly or unknowingly). To prevent attackers from executing successful phishing attacks, configure credential phishing prevention.</p>
<p>Prevent Known Threats</p>	<p>Attach Security profiles to all allow rules so the firewall can detect and block network and application layer vulnerability exploits, buffer overflows, DoS attacks, port scans, and known malware variants, (including those hidden within compressed files</p>

Best Practice Methodology	Why is this important?
	<p>or compressed HTTP/HTTPS traffic). To enable inspection of encrypted traffic, enable decryption.</p> <p>In addition to application-based Security policy rules, create rules for blocking known malicious IP addresses based on threat intelligence from Palo Alto Networks and reputable third-party feeds.</p>
Detect Unknown Threats	<p>Forward all unknown files to WildFire for analysis. WildFire identifies unknown or targeted malware (also called <i>advanced persistent threats</i> or <i>APTs</i>) hidden within files by directly observing and executing unknown files in a virtualized environment in the cloud or on the WildFire appliance. If WildFire detects malware, it automatically develops a signature and can deliver it to you in real-time or at a time interval of your choice.</p>

Why Do I Need a Best Practice Internet Gateway Security Policy?

A best practice security policy allows you to enable applications safely by classifying all traffic, across all ports, all the time, including encrypted traffic. Determine the business use case for each application to create Security policy rules that allow and protect access to relevant applications. A best practice security policy leverages the next-generation technologies—App-ID, Content-ID, User-ID, and Device-ID (for [IoT Security](#), which is beyond the scope of this book)—on the Palo Alto Networks enterprise security platform and:

- Identifies applications regardless of port, protocol, evasive tactic or encryption.
- Identifies and control users regardless of IP address, location, or device.
- Protects against known and unknown application-borne threats.
- Provides fine-grained visibility and policy control over application access and functionality.
- Follows [IoT Security best practices](#) if you have an IoT deployment.

A best practice security policy uses a layered approach to ensure that you safely enable sanctioned applications while blocking applications with no legitimate use case. To mitigate the risk of breaking applications when you move from port-based enforcement to application-based enforcement, the best-practice rulebase includes temporary Security policy rules that identify gaps in the rulebase, detect alarming activity and potential threats, ensure applications don't break during the transition, and enable you to monitor application usage so you can craft appropriate rules. Some applications that a legacy port-based policy allowed might be applications that you don't want to allow or that you want to limit to a more granular set of users.

A best-practice security policy is easier to administer and maintain because each rule meets a specific business goal and allows access to an application or group of applications for a specific user group or users. Each rule's application and user match criteria make it easier to understand what traffic the rule enforces. A best-practice security policy rulebase also leverages tags and objects to make the rulebase easier to scan and easier to keep synchronized with your changing environment.

How Do I Deploy a Best Practice Internet Gateway Security Policy?

The goal is to architect an application-based best practice Security policy that aligns with your business goals and acceptable use policies, simplifies administration, reduces the chance of error, and applies [Zero Trust](#) principles to network access.

As with any technology, there is usually a gradual approach to a complete implementation. Plan deployment phases carefully to make the transition as smooth as possible, with minimal impact to end users. Generally, the workflow for implementing a best practice internet gateway security policy is:

- ❑ **Assess your business and identify what you need to protect**—The first step in deploying a security architecture is to assess your business. Identify your most valuable assets and the biggest threats to those assets. For example, if you are a technology company, your intellectual property is your most valuable asset. In this case, one of your biggest threats is source code theft.
- ❑ **Segment Your Network Using Interfaces and Zones**—Traffic can flow between zones only if a security policy rule allows it. A strong defense to prevent an attacker who has gained access to your network from moving laterally through the network is to define granular zones and only allow access only to the specific user groups that need access to an application or a resource in each zone. Segmenting your network into granular zones prevents an attacker from establishing a communication channel within your network (either via malware or by exploiting legitimate applications), which reduces the likelihood of a successful attack.
- ❑ **Identify Your Application Allow List**—Before you can create an internet gateway best practice security policy, create an inventory of the applications you want to allow on your network. Separately list applications that you administer, officially sanction for business, and tolerate for employee use. After you identify the applications you want to allow, if you are migrating from a port-based rulebase, map the applications to your port based rules. If a port-based rule has no application mapped to it, you may not need that rule.
- ❑ **Create User Groups for Access to Allowed Applications**—After you identify the applications you plan to allow, identify the user groups that require access to each application. Compromising an end user's system is one of the cheapest and easiest ways for an attacker to gain access to your network. To reduce your attack surface significantly, allow application access only to user groups that have a legitimate business need.
- ❑ **Decrypt Traffic for Full Visibility and Threat Inspection**—You can't protect your network against threats you can't see and inspect. Encrypted traffic is a common way for attackers to deliver threats. For example, an attacker may use a web application such as Gmail, which uses TLS encryption, to email an exploit or malware to employees accessing that application on the corporate network. Or an attacker may compromise a website that uses TLS encryption to silently download an exploit or malware to site visitors.
- ❑ **Create Best Practice Security Profiles for the Internet Gateway**—Legitimate applications deliver command and control traffic, CVEs, drive-by downloads of malicious content, phishing attacks, and APTs. To protect against known and unknown threats, attach strict Security profiles to all Security policy rules that allow traffic.
- ❑ **Define the Initial Internet Gateway Security Policy**—Using the application and user group inventory you created, define an initial policy that allows access to applications by user or user

group. The initial policy rulebase also includes rules for blocking known malicious IP addresses, as well as temporary rules that prevent applications you might not know about from breaking and identify policy gaps and security holes in your existing design.

- ❑ **Monitor and Fine Tune the Policy Rulebase**—After the temporary rules are in place, monitor traffic that matches to them so that you can fine tune your policy. Because the temporary rules are designed to uncover unexpected traffic on the network, such as traffic running on non-default ports or traffic from unknown users, you must assess the traffic matching these rules and adjust your application allow rules accordingly.
- ❑ **Remove the Temporary Rules**—After a monitoring period of several months, you should see less and less traffic hitting the temporary rules. When you reach the point where traffic no longer hits the temporary rules, remove them to complete your best practice internet gateway security policy.
- ❑ **Maintain the Rulebase**—Due to the dynamic nature of applications, you must continually monitor your application allow list, adapt your rules to accommodate new applications, and determine how [new or modified App-IDs impact policy](#). Because the rules in a best practice rulebase align with your business goals and leverage policy objects for simplified administration, adding support for a new application or a new or modified App-ID often is as simple as adding or removing an application from an [application group](#) or modifying an [application filter](#).

Identify Your Application Allow List

The application allow list includes the sanctioned applications that you provision and administer for business, infrastructure, and user work purposes. It also includes tolerated applications that you choose to allow for personal use. Before you create your internet gateway security policy, create an inventory of the applications you want to allow.

There are many ways to create an application inventory. Your IT department might already have a list of sanctioned applications, but that doesn't necessarily mean that IT knows every application on your network. Involve stakeholders in different business areas to help identify the applications that you use in those business areas. For example, a stakeholder involved with finance applications probably doesn't know which applications your developers require for business purposes and vice-versa, so you need representatives from both areas to understand which applications to sanction, which applications to tolerate, and which applications you don't need to allow on your network.

Your business and your business goals help determine how to approach allowing applications. If your business is a security-first business such as a bank, to minimize the attack surface, you want to allow only the required business applications. However, if your business is an availability-first business such as a university, you probably want to be more liberal with allowed applications.

Strategies for identifying the applications that you actually need for business purposes include examining business goals to understand which applications are required to support your business and using temporary rules to help understand application usage.

- [Map Applications to Business Goals for a Simplified Rulebase](#)
- [Use Temporary Rules to Tune the Allow List](#)
- [Application Allow List Example](#)

Map Applications to Business Goals for a Simplified Rulebase

As you inventory the applications on your network, consider your business goals and acceptable use policies and identify the applications that correspond to each. This enables you to create a goal-driven rulebase. For example, a business goal might be to allow the sales and support groups access your customer database. Create an allow rule that corresponds to each goal and group all of the applications that align with the goal into a single rule. This approach enables you to create a rulebase with a smaller number of individual rules and each rule has a clear purpose.

Because the individual rules you create align with your business goals, you can use application objects to group allowed applications to further simplify administration of the rulebase:

- [Create application groups](#) for each set of sanctioned applications—Create application groups that explicitly include only sets of your sanctioned applications. Application groups simplify the administration of your policy because they enable you to add and remove sanctioned applications without modifying individual Security policy rules. Generally, if the applications that map to the same goal have the same access requirements (for example, they all have a destination address that points to the internet, they all allow access to any known user, and

you want to enable them only on their default ports), you add them to the same application group.



Tag all sanctioned applications with the predefined **Sanctioned** tag. Panorama and firewalls consider applications without the **Sanctioned** tag as unsanctioned applications.

- **Create an application filter** to allow each type of general application—In addition to applications you officially sanction, you need to decide which additional applications you want to allow users to access. Application filters allow you to safely enable certain categories of applications based on **tags**, category, subcategory, technology, risk factor, or characteristic. Separate different types of applications based on business and personal use. Create separate filters for each type of application to make it easier to understand each policy rule.

Use Temporary Rules to Tune the Allow List

The end goal of application-based Security policy is to explicitly allow the application traffic you want to allow and implicitly deny the traffic you don't want. However, the initial rulebase requires some temporary rules, which ensure that you have full visibility into all applications on your network so that you can properly tune policy. The initial rulebase needs the following types of rules:

- Allow rules for applications you officially sanction and deploy for business purposes.
- Allow rules for safely enabling access to tolerated applications you want to allow per your acceptable use policy.
- Block rules that block applications with no legitimate use case. These rules prevent malicious traffic from entering your network while the temporary rules discover applications that your policy rulebase doesn't account for yet.
- Temporary allow rules to give you visibility into all of the applications running on your network so that you can tune the rulebase.

Temporary rules:

- Provide visibility into applications you didn't know were on your network.
- Prevent legitimate applications you didn't know about from getting blocked.
- Identify unknown users, unknown applications, and applications running on non-standard ports (attackers commonly use standard applications on non-standard ports as an evasion technique for malicious activity).

Identify legitimate applications running on non-standard ports (for example, internally developed applications) so that you can either modify the ports the application uses or **create a custom application** to use in policy.



If you have Application Override policy rules that you created to define custom session timeouts for a set of ports, convert the application override policies to application-based policies by configuring **service-based session timeouts** to maintain the custom timeout for each application. Then migrate each rule to an application-based rule. Application override policies are port-based and don't provide application visibility into traffic, so you don't know or control which applications use the ports. Service-based session timeouts achieve custom timeouts while maintaining application visibility.

Application Allow List Example

You don't need to capture every application that might be in use on your network in your initial inventory. Instead, focus on the applications that you want to allow. Temporary rules catch other applications that might be on your network, so you're not inundated with complaints about broken applications during a transition to application-based policy. The following table shows an example application allow list for an enterprise gateway deployment.

Application Type	Best Practice for Securing
SaaS Applications	<p>SaaS application service providers own and manage the software and infrastructure, but you retain full control of the data, including who can create, access, share, and transfer it. To control SaaS applications, use SaaS Security (subscription required). If you use SaaS Security, use SaaS Policy Recommendation to control SaaS applications on the firewall.</p> <p>If you don't have a SaaS Security subscription, generate a SaaS application usage report to check if SaaS applications currently in use have unfavorable hosting characteristics such as past data breaches or lack of proper certifications. Based on business needs and the amount of risk you're willing to accept, use the information to:</p> <ul style="list-style-type: none"> • Block existing applications with unfavorable hosting characteristics immediately. • Create granular policies that block applications with unfavorable hosting characteristics to prevent future violations. • Identify network traffic trends of the top applications that have unfavorable hosting characteristics so you can adjust policy accordingly. <p>Many SaaS applications have enterprise and consumer (personal) versions, but unrestricted use increases the risk of sensitive data leaving your network. HTTP Header Insertion enables you to control which versions of SaaS applications you allow on your network. For example, you can allow the enterprise version of Box or Office 365 and block consumer versions. HTTP header insertion reduces the attack surface by allowing only the version of each SaaS application that you want to sanction or tolerate for the personal use of your users.</p>
Sanctioned Applications	<p>These are the applications that your IT department administers specifically for business use within your organization or to provide infrastructure for your network and applications. For example, in an internet gateway deployment these applications fall into the following categories:</p> <ul style="list-style-type: none"> • Infrastructure Applications—Applications that you must allow to enable networking and security, such as ping, NTP, SMTP, and DNS.

Application Type	Best Practice for Securing
	<ul style="list-style-type: none"> • IT Sanctioned Applications—Applications that you provision and administer for your users. These fall into two categories: <ul style="list-style-type: none"> • IT Sanctioned On-Premises Applications—Applications you install and host in your data center for business use. With IT sanctioned on-premise applications, the application infrastructure and the data reside on enterprise-owned equipment. Examples include Microsoft Exchange and active sync, as well as authentication tools such as Kerberos and LDAP. • IT Sanctioned SaaS Applications—SaaS applications that your IT department sanctions for business purposes, for example, Salesforce, Box, and GitHub. • Administrative Applications—Applications that only a specific group of administrative users should have access to in order to administer applications and support users (for example, remote desktop applications). <p>Tag all sanctioned applications with the predefined <i>Sanctioned</i> tag. Panorama and firewalls consider applications without the Sanctioned tag as unsanctioned applications.</p>
<p>Tolerated Types of Applications</p>	<p>In addition to applications you officially sanction, you also need to allow users to safely access other types of tolerated applications:</p> <ul style="list-style-type: none"> • General Business Applications—For example, allow access to software updates for tolerated applications and to web services such as WebEx, Adobe online services, and Evernote. • Personal Applications—For example, you might allow users to browse the web or safely use web-based mail, instant messaging, or social networking applications, including consumer versions of some SaaS applications. <p>Begin with broad application filters to understand which applications are on your network. Decide how much risk you are willing to assume and pare down the application allow list. For example, you might have multiple messaging applications in use, each with the inherent risk of data loss, transfer of malware-infected files, etc.</p> <p>The best approach is to sanction a single messaging application and then slowly transition from an allow policy to an alert policy, and after giving users ample warning, to a block policy to phase out the other messaging applications. You might also choose to enable a small group of users to continue using additional messaging applications as needed to perform job functions with partners.</p>
<p>Custom Applications Specific to Your Environment</p>	<p>Create custom applications for proprietary applications or applications that you run on non-standard ports. This enables you to allow the application as a sanctioned application (and apply the predefined Sanctioned tag) and lock it down to its default port. Otherwise, you</p>

Application Type	Best Practice for Securing
	<p>either have to open up additional ports (for applications running on non-standard ports) or allow unknown traffic (for proprietary applications), neither of which are recommended in a best practice Security policy.</p> <p>If you have existing Application Override policies that you created solely to define custom session timeouts for a set of ports, convert the existing Application Override policies to application-based policies by configuring service-based session timeouts to maintain the custom timeout for each application. Then migrate each rule to an application-based rule. Application override policies are port-based and don't provide application visibility into traffic, so you don't know or control which applications use the ports. Service-based session timeouts achieve custom timeouts while maintaining application visibility.</p>

Create User Groups for Access to Allowed Applications

Safely enabling applications means defining the list of applications you want to allow and enabling access only for users who have a legitimate business need. For example, some applications, such as SaaS applications that enable access to Human Resources services such as Workday or Service Now must be available to any known user on your network. However, for more sensitive applications, reduce your attack surface by enabling access only for users who need the applications for business purposes. For example, IT support personnel might legitimately need access to remote desktop applications, but most users do not. Limiting user access to applications prevents potential security gaps that an attacker might use to gain access and control over systems in your network.

To enable user-based access to applications:

- ❑ [Enable User-ID](#) in zones from which your users initiate traffic.
- ❑ For each application allow rule you define, identify the user groups that have a legitimate business need to access the applications. Mapping application allow rules to business goals (which includes considering which users have a business need for a particular type of application) results in a smaller number of rules to manage compared to mapping port-based rules to users.
- ❑ If you don't have existing user groups on your Active Directory (AD) server, alternatively, [create custom LDAP groups](#) to match groups of users who need access to a particular application.
- ❑ It takes just one end user to click on a phishing link and enter credentials to enable an attacker to gain access to your network. To defend against this simple and effective attack technique, [set up credential phishing protection](#) on all of your Security policy rules that allow user access to the internet. [Configure credential detection with the Windows-based User-ID agent](#) to ensure that you can detect when your users are submitting their corporate credentials to a site in an unauthorized category.

Decrypt Traffic for Full Visibility and Threat Inspection

Decrypt all traffic except sensitive categories, which include URL categories such as financial-services, health-and-medicine, government, and other traffic that you don't decrypt for business, legal, or regulatory reasons. Use [URL categories](#), [custom URL categories](#), and [External Dynamic Lists \(EDLs\)](#) to specify the traffic you don't decrypt.

Use decryption exceptions only where required. Be precise to ensure that you limit exceptions to specific applications or users based on need:

- If decryption breaks an important application, [create an exception](#) for the specific IP address, domain, or common name in the certificate associated with the application.
- If you need to exclude a specific user for regulatory, business, or legal reasons, create an exception for just that user.

To ensure that certificates presented during decryption are valid, [perform CRL/OCSP checks](#).

Add a strict Decryption profile to Decryption policy rules. Before you [configure SSL Forward Proxy](#), create a best practice Decryption Profile (**Objects > Decryption Profile**) to attach to your Decryption policy rules, and follow general [decryption best practices](#):

STEP 1 | Configure the **SSL Decryption > SSL Forward Proxy** settings to block exceptions during TLS negotiation and block sessions that can't be decrypted:

Decryption Profile ?

Name

SSL Decryption |
 No Decryption |
 SSH Proxy

SSL Forward Proxy |
 SSL Inbound Inspection |
 SSL Protocol Settings

Server Certificate Verification

- Block sessions with expired certificates
- Block sessions with untrusted issuers
- Block sessions with unknown certificate status
- Block sessions on certificate status check timeout
- Restrict certificate extensions Details
- Append certificate's CN value to SAN extension

Unsupported Mode Checks

- Block sessions with unsupported versions
- Block sessions with unsupported cipher suites
- Block sessions with client authentication

Failure Checks

- Block sessions if resources not available
- Block sessions if HSM not available
- Block downgrade on no resource

Client Extension

- Strip ALPN

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.

OK
Cancel

Block sessions if resources not available prevents allowing potentially dangerous connections when the firewall doesn't have the resources to perform decryption, but blocking traffic that you can't decrypt for this reason might affect user experience.

STEP 2 | Configure **SSL Decryption > SSL Protocol Settings** to block the use of vulnerable SSL/TLS versions (TLSv1.0, TLSv1.1, and SSLv3) and to avoid weak algorithms (MD5, RC4, and 3DES):

Decryption Profile ?

Name

SSL Decryption | No Decryption | SSH Proxy

SSL Forward Proxy | SSL Inbound Inspection | **SSL Protocol Settings**

Protocol Versions

Min Version

Max Version

Key Exchange Algorithms

RSA DHE ECDHE

Encryption Algorithms

3DES AES128-CBC AES128-GCM CHACHA20-POLY1305

RC4 AES256-CBC AES256-GCM

Authentication Algorithms

MD5 SHA1 SHA256 SHA384

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.

Use TLSv1.3 (the most secure protocol) when you can. Many mobile applications use certificate pinning that prevents decryption and causes the firewall to drop traffic. For that traffic, use TLSv1.2.

Review the sites you need to access for business purposes. If any of them use TLSv1.1, create a separate Decryption policy and profile for those sites so that only sites you must access for business purposes can use the less secure protocol.

Don't allow the SHA1 authentication algorithm unless you must. Create a separate Decryption policy rule and profile for sites that use SHA1 that you must access for business purposes.

STEP 3 | For traffic that you don't decrypt, configure the **No Decryption** settings to block encrypted sessions to sites with expired certificates or untrusted issuers:

The screenshot shows a configuration window titled "Decryption Profile" with a help icon. The "Name" field contains "Tight TLS Control". Below it are three tabs: "SSL Decryption", "No Decryption" (which is selected), and "SSH Proxy". Under the "Server Certificate Verification" section, there are two checked checkboxes: "Block sessions with expired certificates" and "Block sessions with untrusted issuers". At the bottom right, there are "OK" and "Cancel" buttons. A note at the bottom of the window reads: "Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead."



Only use a No Decryption profile for TLSv1.2 and earlier versions. Do not attach a No Decryption profile to TLSv1.3 traffic that you don't decrypt. TLSv1.3 encrypts certificate information that was not encrypted in previous versions, so the firewall cannot block sessions based on certificate information.

Transition Safely to Best Practice Security Profiles

Security profiles enable you to inspect network traffic for threats such as vulnerability exploits, malware, command-and-control (C2) communication, and unknown threats, and prevent them from compromising your network using various types of threat signatures, machine learning, and AI (some protections require a [subscription](#)).

The end goal is to reach a best practice state for all of your Security profiles. However, to ensure the availability of business-critical applications, it might not be feasible to implement a full best practice Security profile configuration from the start. In most cases, you can safely block some signatures, file types, or protocols while alerting on others until you gain the information and confidence to finish a safe transition to best practice Security profiles without affecting availability.

The path to implementing best practice Security profiles is:

1. Use Strata Cloud Manager to run an [on-demand Best Practices Assessment \(BPA\) report](#) on your security posture or check Strata Cloud Manager's [Best Practices Dashboards](#) to assess the state of your current security best practices. Review your best practices adoption, identify gaps in adoption, and review Security profile configuration.
2. Use the following safe transition steps to move toward the [best practice](#) state for your Security profiles.

Ask yourself the following questions to help determine the right approach to enabling Security profiles for a given network segment or set of Security policy rules:

1. Do I already have Security profiles enabled on rules that protect similar applications or network segments? If the answer is yes, you might be able to duplicate those profile settings, including block actions you already deem safe to enable.
2. Is the network segment I'm protecting critical for my business? If the answer is yes and you don't have proven profiles enabled in similar segments, you might prefer to alert first, examine the traffic that causes the alerts to ensure the profile doesn't block critical applications, and then block when you're comfortable.
3. Am I deploying Security profiles to counter an immediate threat? If the answer is yes, you might want to block as the initial action instead of alerting.
4. Is there a firewall change process in place that allows investigation and remediation of false positives in a timely manner? If the answer is yes, you might be able to block as the initial action instead of alerting.



The majority of "false positives" are attempted attacks against a vulnerability that doesn't exist in your network. The attack is real, but the danger is not because the vulnerability isn't present, so the attack is often seen as a false positive. Brute-force attack signatures can also cause false positives if you set the attack threshold too low.

Consider your current security posture in combination with the guidance for each type of Security profile to decide how to deploy the profiles initially, and then move to the best practice guidance.

- [Transition Vulnerability Protection Profiles Safely to Best Practices](#)
- [Transition Anti-Spyware Profiles Safely to Best Practices](#)
- [Transition Antivirus Profiles Safely to Best Practices](#)

- [Transition WildFire Profiles Safely to Best Practices](#)
- [Transition URL Filtering Profiles Safely to Best Practices](#)
- [Transition File Blocking Profiles Safely to Best Practices](#)

Transition Vulnerability Protection Profiles Safely to Best Practices

The decision to block or alert when you first apply Vulnerability Protection profiles to traffic depends on your current security posture and your business requirements regarding security vs. availability. The following guidance helps determine whether to start with block or alert actions as you begin the transition to best practice Vulnerability Protection profiles.



Vulnerability Protection requires an Advanced Threat Prevention or active legacy Threat Prevention subscription.



To identify and prevent threats, the firewall must have visibility into application traffic. [Decrypt](#) as much traffic as local regulations, business considerations, privacy considerations, and technical ability allow. If you don't decrypt traffic, the firewall can't analyze encrypted headers and payload information.

In addition, follow [Threats Content Update](#) best practices to ensure that your Security profile signatures are up to date.

- **Business-critical applications**—It's usually best to set the initial rule **Action** to **alert** to ensure application availability. However, in some situations, you can use the **block** action from the start. For example, when you're already protecting similar applications with a Vulnerability Protection profile that blocks on vulnerability signatures, and you're confident the profile meets your business and security needs, you can use a similar profile to block vulnerabilities and protect the similar applications.



Alerting enables you to analyze Threat logs and create exceptions when necessary before you start blocking traffic. Alerting and monitoring before moving to blocking gives you confidence that:

- *The initial profile won't block business-critical applications when you deploy it.*
- *You create necessary exceptions as you transition to the blocking state to maintain application availability.*

Keep the length of time you maintain the initial alert action to a minimum to reduce the chance of a security breach. Transition to the blocking state as soon as you're comfortable that you've identified any exceptions you need to make and configured the profile accordingly.

- **Critical and high severity signatures**—False positive rates for critical and high severity signatures are typically low and usually indicate an attack against a vulnerability that doesn't exist on your network. For applications that aren't critical to your business, such as internet access, block (**reset-both**) critical and high severity signatures from the start.
- **Medium severity signatures**—These might generate false positives and require initial monitoring. Start by alerting on medium severity signatures and monitor the Threat logs (**Monitor > Logs > Threat**) to see if you should block applications for which you receive alerts or if you need to allow them.

- Fine-tune profile rules that alert before you transition to blocking them, especially for internet-facing and data center traffic. Move to blocking as soon as you comfortably can.
- Set signatures in the brute-force category to alert and then move to blocking as soon as you can. Brute-force events are aggregate events that trigger when an action takes place multiple times in a short time period. For example, one SSH login attempt is an informational event, but 100 login attempts in 10 seconds trigger the brute-force signature. Although it might take time to tune the profile so that normal network traffic doesn't trigger a brute-force signature, transition to blocking these signatures as soon as safely possible, based on your comfort level.

RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/> simple-server-critical-low	any	any	any	critical	alert	extended-capture
<input type="checkbox"/> simple-server-high-misc	any	any	any	high	alert	extended-capture
<input type="checkbox"/> simple-server-medium-low	any	any	any	medium	alert	extended-capture
<input type="checkbox"/> simple-client-critical	any	any	client	critical	reset-both	single-packet
<input type="checkbox"/> simple-client-high	any	any	client	high	reset-both	single-packet
<input type="checkbox"/> simple-client-medium	any	any	client	medium	alert	extended-capture
<input type="checkbox"/> simple-client-informational	any	any	client	informational	default	single-packet
<input type="checkbox"/> simple-client-low	any	any	client	low	default	single-packet
<input type="checkbox"/> simple-server-critical	any	any	server	critical	reset-both	single-packet
<input type="checkbox"/> simple-server-high	any	any	server	high	reset-both	single-packet
<input type="checkbox"/> simple-server-medium	any	any	server	medium	alert	extended-capture
<input type="checkbox"/> simple-server-informational	any	any	server	informational	default	single-packet
<input type="checkbox"/> simple-server-low	any	any	server	low	default	single-packet

Figure 1: Brute-force alert Vulnerability Protection profile

- The default **Action** for most low and informational severity signatures is **alert** or **allow**. Unless you have a specific need to alert on all low and informational signatures, configure the **Action** as **default**.
- If the resources are available, enable extended **packet capture** for critical, high, and medium severity signatures on which you alert. Enable single packet capture for blocked signatures and for low and informational severity signatures. Enabling packet capture enables you to investigate events in greater detail if necessary. As you move to best practice profiles, if informational events create too much packet capture activity (too large a volume of traffic) and the information isn't useful, transition to disabling packet capture on informational events.



*Packet captures consume management plane resources. Check system resources (for example, **Dashboard > System Resources**) to understand usage before and after you implement packet capture to ensure that your system has sufficient resources to take all the packet captures.*

- For **Inline Cloud Analysis**, use the same criteria for alerting versus blocking business applications that you use for the Vulnerability Protection rules. If you have existing controls,

you can replicate them to block traffic. For new controls, alert for at least a week before transitioning to blocking. Move to blocking as soon as you can.

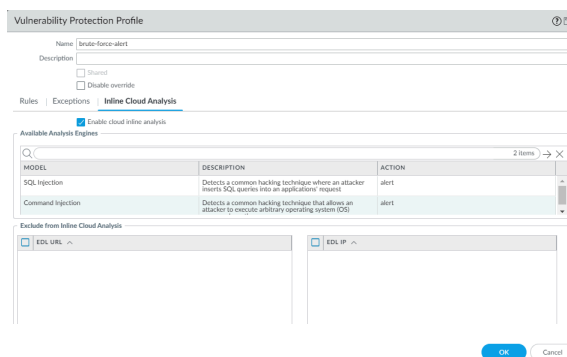


Figure 2: Inline Cloud Analysis alert Vulnerability Protection profile

When you have the initial profiles in place, monitor the Threat logs for enough time to gain confidence that you understand whether any business-critical applications cause alerts or blocks. Create exceptions (open a support ticket if necessary) in each profile as needed to remediate confirmed false positives before you transition to full [best practices Vulnerability Protection profiles](#). How fast you complete the transition to best practice profiles depends on your business, applications, and comfort level—be aware that some applications are only used weekly, monthly, quarterly, or yearly for audits, periodic events and meetings, etc.

Transition Anti-Spyware Profiles Safely to Best Practices

The following guidance helps determine whether to start with block or alert actions as you define the initial Anti-Spyware profiles and begin the transition to best practices profiles.



Anti-Spyware requires an Advanced Threat Prevention or active legacy Threat Prevention subscription.

To identify and prevent threats, the firewall must have visibility into application traffic. [Decrypt](#) as much traffic as local regulations, business considerations, privacy considerations, and technical ability allow. If you don't decrypt traffic, the firewall can't analyze encrypted headers and payload information.

In addition, follow [Threats Content Update](#) best practices to ensure that your Security profile signatures are up to date.

- **Business-critical applications**—Set the initial action to alert to ensure application availability. However, in some situations, you can use the **block** action from the start. For example, when you're already protecting applications with an Anti-Spyware profile that blocks critical, high,

and/or medium signatures, and you're confident the profile meets your business and security needs, you can use a similar profile to block spyware and protect those applications.



The alert action enables you to analyze Threat logs and create exceptions when necessary before moving to a block action. Alerting and monitoring before you move to blocking gives you confidence that:

- *The profile won't block business-critical applications when you deploy it.*
- *You create necessary exceptions as you transition to the blocking state to maintain application availability.*

Transition to the best practice state as soon as you're comfortable you've identified any exceptions you need to make and configure the profile accordingly.

- **Critical and high severity signatures**—False positive rates are typically low. For applications that aren't critical to your business, block critical and high severity signatures from the start.
- **Medium severity signatures**—These might generate false positives and require initial monitoring. Start by alerting on medium severity signatures for internal traffic and blocking medium severity signatures for external-facing traffic. Monitor the Threat logs (**Monitor > Logs > Threat**) to see if you should block applications for which you receive alerts or if you need to allow them.
- **Low and informational severity signatures**—The default action for most of these signatures is alert or allow. Unless you have a specific need to alert on all low and informational signatures, start with the default action.
- Enable single **packet capture** for all severity signatures during the transition if you have the resources. Enabling packet capture allows you to investigate events in greater detail if necessary. As you move to best practice profiles, if low and informational events create too much packet capture activity (too large a volume of traffic) and the information isn't useful, transition to disabling packet capture on these severities.



*Packet captures consume management plane resources. Check system resources (for example, **Dashboard > System Resources**) to understand usage before and after you implement packet capture to ensure that your system has sufficient resources to take all the packet captures.*

- If you treat internal applications differently than external applications, you might need an Anti-Spyware profile for internet-facing traffic and another Anti-Spyware profile for internal traffic.
- **DNS Policies:**
 - Set the **Policy Action** for DNS signatures to **Sinkhole** to identify potentially compromised hosts that attempt to access suspicious domains. DNS sinkhole enables you to track the hosts and prevent them from accessing those domains. (Enabling DNS sinkhole immediately is the best practice.) Set **Packet Capture** to **extended-capture**.
 - Sinkhole all of the **DNS Security** domain types and set **Packet Capture** as shown in [Figure 1](#) (PAN-OS 10.0 and later).
 - In addition, block all DNS record types used for Encrypted Client Hello (ECH) to maximize security. This prevents the client from initiating an ECH connection during the handshake

process, which might otherwise interfere with inspection of the client hello contents by Advanced DNS Security.

- Block all DoH requests by creating applicable App-ID and/or URL Filtering policies. If it is necessary to allow DoH traffic, create a sanctioned DoH resolver that uses DNS Security to inspect the DoH requests.



Allow traffic only to sanctioned DNS servers. Use the [DNS Security service](#) to prevent connections to malicious DNS servers.



On PAN-OS based systems, set the DNS sinkhole address as the FQDN, for example, `sinkhole.paloaltonetworks.com`, so that if the IP address changes, the setting is still valid. For Prisma Access, use the sinkhole IP address.

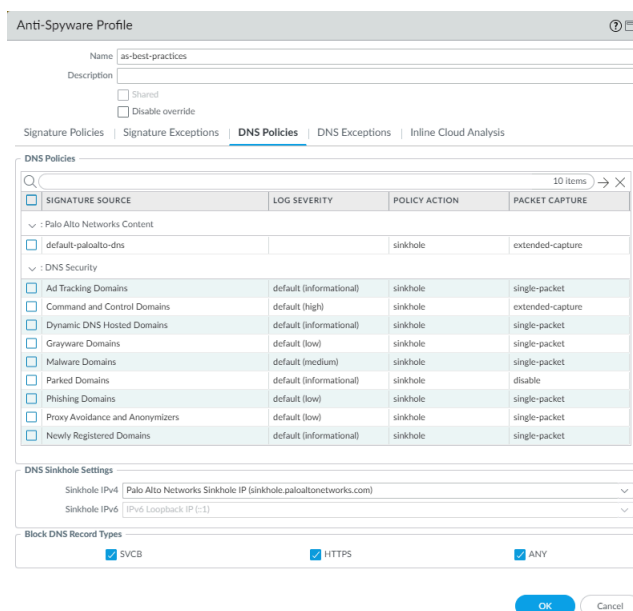


Figure 3: Anti-Spyware profile DNS Policies

- **Inline Cloud Analysis** (requires Advanced Threat Prevention subscription and PAN-OS 10.2 or later)—**Enable cloud inline analysis** on all outbound traffic. Set the **Action** to **reset-both** for all models.



Air-gapped environments cannot use Advanced Threat Prevention because it's a cloud service and requires a cloud connection.

When you have the initial profiles in place, monitor the Threat logs for enough time to gain confidence that you understand whether any business-critical applications cause alerts or blocks. Transition to [best practices Anti-Spyware profiles](#) as soon as you're comfortable doing so. Create exceptions (open a support ticket if necessary) in each profile as needed to remediate any confirmed false positives before you implement full best-practice Anti-Spyware profiles.

Transition Antivirus Profiles Safely to Best Practices

The following guidance helps determine whether to start with block or alert actions when you clone the default [Antivirus profile](#) and modify it to define the initial profiles and begin the transition to best practice profiles.



Antivirus requires an Advanced Threat Prevention or active legacy Threat Prevention subscription.

To identify and prevent threats, the firewall must have visibility into application traffic. [Decrypt](#) as much traffic as local regulations, business considerations, privacy considerations, and technical ability allow. If you don't decrypt traffic, the firewall can't analyze encrypted headers and payload information.

In addition, follow [Threats Content Update](#) best practices to ensure that your Security profile signatures are up to date.

- **Business-critical applications**—Set the initial action to alert to ensure application availability. However, in some situations you can block Antivirus signatures from the start. For example, when you're already protecting similar applications with an Antivirus profile and you're confident the profile meets your business and security needs, you can use a similar profile to protect similar applications because you already understand what you're blocking.



*The alert action enables you to analyze Threat logs (**Monitor > Logs > Threat**) and create exceptions when necessary before moving to a block action. Alerting and monitoring before moving to blocking gives you confidence that:*

- *The profile won't block business-critical applications when you deploy it.*
- *You create necessary exceptions as you transition to the blocking state to maintain application availability.*

Keep the length of time you maintain the initial alert action to a minimum to reduce the chance of a security incident. Transition to the best practice state as soon as you're comfortable you've identified any exceptions you need to make and configure the profile accordingly.

- **Critical and high severity signatures**—It's safe to deploy [best practices Antivirus profiles](#) to block malicious traffic for applications that aren't critical to your business right away because false positive rates are rare, so unnecessary blocking rarely occurs.
- If you treat internal applications differently than external applications, you might need an Antivirus profile for internet-facing traffic and another Antivirus profile for internal traffic.
- Enable real-time signature lookup globally on the device and in the Antivirus profile to hold files until the firewall receives the latest real-time antivirus signature from the cloud:
 - ❑ Enable [globally](#)—**Device > Setup > Content-ID > Content-ID Settings > Realtime Signature Lookup**, enable **Hold for WildFire Real Time Signature Look Up**, and set the **Action On Real**

Time Signature Timeout to Reset Both. You must enable real-time signature lookup globally to enable in Antivirus profiles.

- ❑ Enable in [Antivirus profile](#)—**Objects > Security Profiles > Antivirus** and enable **Hold for WildFire Real Time Signature Look Up**.

Holding files to ensure that WildFire gets the latest antivirus signatures protects you from zero-day malware and outdated antivirus signatures that you might be exposed to if you forward files without holding them for the latest signatures.

- WildFire Action settings in the Antivirus profile might impact traffic if the traffic generates a WildFire signature that results in a reset or drop action.

When you have the initial profiles in place, monitor the Threat logs for enough time to gain confidence that you understand whether any business-critical applications cause alerts or blocks. Also monitor the WildFire Submissions logs (**Monitor > Logs > WildFire Submissions**) for enough time to gain confidence that you understand whether any business-critical applications cause alerts or blocks due to the Antivirus profile WildFire Action. Create exceptions (open a support ticket if necessary) in each profile as needed to remediate any confirmed false positives before you implement full best-practice Antivirus profiles. The speed of your transition to best practices profiles depends on your business, applications, and comfort level—be aware that some applications are only used weekly, monthly, quarterly, or yearly for audits, periodic events and meetings, etc.

Transition WildFire Profiles Safely to Best Practices

The following guidance helps define the initial configuration of WildFire Analysis profiles.

Palo Alto Networks Next-Generation Firewalls include the basic WildFire service and don't require an Advanced WildFire (or active legacy WildFire) subscription. The basic service enables the firewall to forward PE files for analysis and retrieves Advanced WildFire signatures only with an antivirus and/or Threat Prevention update every 24-48 hours. An [Advanced WildFire subscription](#) (PAN-OS 10.0 or later) or legacy WildFire subscription includes many more features, such as receiving updates in real-time, support for more file types, and an API.



To identify and prevent threats, the firewall must have visibility into application traffic. [Decrypt](#) as much traffic as local regulations, business considerations, privacy considerations, and technical ability allow. If you don't decrypt traffic, the firewall can't analyze encrypted headers and payload information.

WildFire signature generation is highly accurate and false positives are rare. Deploying the default WildFire Analysis profile (which is the best practices profile) does not impact network traffic. (However, WildFire Action settings in the [Antivirus profile](#) might impact traffic if the traffic generates a WildFire signature that results in a reset or drop action.)

When you have the initial profiles in place, monitor the WildFire Submissions logs (**Monitor > Logs > WildFire Submissions**) for enough time to gain confidence that you understand whether any business-critical applications cause alerts or blocks due to the Antivirus profile WildFire Action. Create exceptions (open a support ticket if necessary) in the Antivirus profile as needed to remediate any confirmed false positives.

Transition URL Filtering Profiles Safely to Best Practices

The following guidance helps determine whether to start with block or alert actions as you define the initial URL Filtering profiles and begin the transition to best practice profiles. Apply URL Filtering files to internet traffic (do not apply URL Filtering profiles to internal traffic).



You must enable [decryption](#) to take advantage of URL Filtering because you must decrypt traffic to reveal the exact URL so the firewall can take the appropriate action. At the least, decrypt high- and medium-risk traffic.



Advanced URL Filtering requires a subscription.

- The predefined URL categories are accurate, so it's safe to implement URL Filtering profiles with category actions configured according to your company policy for allowing or denying access to different types of websites.
- Block **Site Access** and **User Credential Submission** from the start for known-bad URL categories, including: malware, command-and-control, copyright-infringement, extremism, phishing, ransomware, dynamic-dns, hacking (but make exceptions for internal PEN testers), and proxy-avoidance-and-anonymizers.
- For the URL categories unknown (sites PAN-DB has not yet identified), parked (often used for credential phishing), grayware (malicious or questionable), and newly-registered-domain (often used for malicious activity), alert initially so you can monitor the URL Filtering logs (**Monitor > Logs > URL Filtering**) in case legitimate websites trigger alerts before you move to the best practice of blocking these categories.
- Set all other URL categories to **alert** to generate logs for the traffic. The firewall doesn't log traffic when access is set to **allow**. Monitor the URL Filtering logs to see if you want to block any other categories.



You can combine the high-risk, medium-risk, and low-risk categories with other categories to determine what traffic to allow, block, and decrypt. For example, you could block access to all websites that are both high-risk and financial-services. Or if your firewall needs to conserve resources, you could decrypt all high-risk and medium-risk traffic for some categories and not decrypt low-risk traffic for those categories.

When you have the initial profiles in place, monitor the URL Filtering logs for enough time to gain confidence that you understand whether any business-critical sites will be blocked if you transition from alerting to blocking and to [best practices URL Filtering profiles](#). If you believe a given URL isn't categorized correctly, [request URL recategorization](#) to have the URL placed in the correct category. The speed of your transition to best practices profiles depends on your business, applications, and comfort level.

Transition File Blocking Profiles Safely to Best Practices

The following guidance helps determine whether to start with block or alert actions as you define the initial File Blocking profiles and begin the transition to best practice profiles. Alert instead of allowing file types to generate logs and gain visibility into the traffic.

- Best practices File Blocking profiles are often different for different types of applications and might be different for inbound, outbound, and internal traffic. For example:
 - If internal applications depend on file type transfers that the best practice File Blocking profile recommends blocking, allow those file types for those internal applications; .dll files are a good example. Allow those file transfer types only for the necessary internal applications, not for all applications.
 - For internet-based traffic, take a more restrictive approach to prevent attackers from delivering malicious files and to reduce the attack surface.
 - For data center traffic, take a more restrictive approach (except for internal applications that depend on file transfer types that you would otherwise block) to reduce the attack surface and protect your most valuable assets.
 - When you carve out exceptions, follow the principle of least privilege and apply the exceptions only to the applications and users and that need access to the file type for business purposes.
- **Business-critical applications**—Start with the alert action for all file types and move to [best practices File Blocking profiles](#) as soon as possible. If you already have blocking controls in place, replicate them and continue to block traffic that you already know you want to block.
- For applications that aren't business-critical, start the transition to a best practices File Blocking profile:
 - **Inbound and outbound traffic**—Set the **Action** to **block** for 7z, bat, chm, class, cpl, dll, dlp, hta, jar, ocx, pif, scr, torrent, vbe, and wsf files. Set the **Action** to **alert** for all other files.
 - **Internal traffic**—Block 7z, bat, chm, class, cpl, dlp, hta, jar, ocx, pif, scr, torrent, vbe, and wsf files (this is the same as the inbound/outbound profile except it alerts on .dll files instead of blocking them). Alert on all other files.
 - Block all of the following file types you can for users who don't need them for business purposes: cab, exe, flash, msi, Multi-Level-Encoding, PE, rar, tar, encrypted-rar, and encrypted-zip.



If necessary, create exceptions for IT groups and others who need legitimate business access to any of these file types. If you already block any other file types, continue to block them.

Transition to a best practices File Blocking profile as quickly as you are comfortable with doing so.

Fine-tune profile rules that alert and transition them to blocking as soon as you comfortably can, especially for internet-facing and data center traffic. Monitor the Data Filtering logs (**Monitor > Logs > Data Filtering**) to understand file type usage before configuring block actions for specific file types. As you learn which file types your business-critical and internal custom applications require, transition toward a best practice File Blocking configuration, modified as necessary to support your business needs.

Create Best Practice Security Profiles for the Internet Gateway

Most malware sneaks onto the network in legitimate applications or services. To safely enable applications, you must scan all allowed traffic for threats. Attach Security profiles to all Security policy rules that allow traffic so that you can detect threats—both known and unknown—in your network traffic. The following best practice recommendations focus on the tightest security. Attach a URL Filtering profile to all rules that allow internet-bound traffic and attach the other profiles to all allow rules.

More than 90 percent of web traffic is encrypted. Enable [decryption](#) to gain visibility into traffic, use Security profiles to inspect the payload, and prevent malicious events.



*Consider adding your best practice security profiles to a [default security profile group](#). When you name a security profile group **default**, the firewall automatically attaches it to every new Security policy rule you create and ensures that the firewall inspects the traffic for malicious activity.*

Also consider creating purpose-built Security profile groups for different types of traffic. Security profile groups make applying all the necessary profiles to Security policy rules easy and ensure that no critical profile is forgotten.

- [Best Practice Internet Gateway File Blocking Profile](#)
- [Best Practice Internet Gateway Antivirus Profile](#)
- [Best Practice Internet Gateway Vulnerability Protection Profile](#)
- [Best Practice Internet Gateway Anti-Spyware Profile](#)
- [Best Practice Internet Gateway URL Filtering Profile](#)
- [Best Practice Internet Gateway WildFire Analysis Profile](#)

Best Practice Internet Gateway File Blocking Profile

Use the predefined **strict file blocking** profile to block file types commonly included in malware attack campaigns that have no real use case for upload and download. Blocking these file types reduces the attack surface. The predefined strict profile blocks batch files, DLLs, Java class files, help files, Windows shortcuts (.lnk), BitTorrent files, .rar files, .tar files, encrypted-rar and encrypted-zip files, multilevel encoded files (files encoded or compressed up to four times), .hta files, and Windows Portable Executable (PE) files, which include .exe, .cpl, .dll, .ocx, .sys, .scr, .drv, .efi, .fon, and .pif files. The predefined strict profile alerts on all other file types for visibility into other file transfers so that you can determine if you need to make policy changes.



In some cases, the need to support critical applications might prevent you from blocking all of the strict profile's file types. Follow the [Transition File Blocking Profiles Safely to Best Practices](#) advice to help determine whether you need to make exceptions in different areas of the network. Review the data filtering logs (**Monitor > Logs > Data Filtering**) to identify file types and talk with business stakeholders about the file types their applications require. Based on this information, clone the strict profile and modify it as needed to allow only the other file type(s) that you need to support the critical applications. You can also use the **Direction** setting to restrict files types from flowing in both directions or block files in one direction but not in the other direction.

<input type="checkbox"/>	NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
<input type="checkbox"/>	basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp,hta, jar, oox, PE, pif, rar, scr, torrent, vbe, wsf	both	block
			Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
			Log all other file types	any	any	both	alert
<input checked="" type="checkbox"/>	strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp,hta, jar, msi, Multi-Level-Encoding, oox, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
			Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
			Log all other file types	any	any	both	alert

You might also require a few protocols often used for malicious purposes for activities such as Windows updates. The **strict file blocking** profile blocks .exe., .dll, .pe, and .cab files. To make exceptions to allow protocols for a specific activity such as Windows updates:

1. Create a specific Security policy rule that allows only the required users and business applications that use the protocols you want to block for other traffic.
2. Clone your strict File Blocking profile, modify it to allow the required protocols, and then attach it to the rule.
3. Place the rule above a Security policy rule with a File Blocking profile that blocks the protocols for all other traffic.

This method enables you to use potentially malicious file types in a safe way that enables business applications while blocking malicious traffic. Fine-tune the profiles and rulebase to allow any required exceptions.

Why Do I Need This Profile?

Attackers can deliver malicious files in many ways:

- Attachments or links in corporate or personal email.
- Links or IMs in social media and other sources.
- Exploit Kits.
- File sharing applications (such as FTP, Google Drive, or Dropbox).
- USB drives.
-

Attaching a strict file blocking profile prevents these types of attacks and reduces your attack surface.

If you choose not to block all PE files, send all unknown files to WildFire for analysis. Set the Action to **continue** to prevent drive-by downloads, which is when an end user downloads content that installs malicious files, such as Java applets or executables, without the user's knowledge. Drive-by downloads can occur when users visit web sites, view email messages, or click pop-up windows meant to deceive them. Educate users that if they are prompted to continue with

a file transfer they didn't knowingly initiate, they might be subject to a malicious download. In addition, use file blocking with URL filtering to limit the categories in which users can transfer files to reduce the attack surface if you must allow file types that might carry threats.

Best Practice Internet Gateway Antivirus Profile

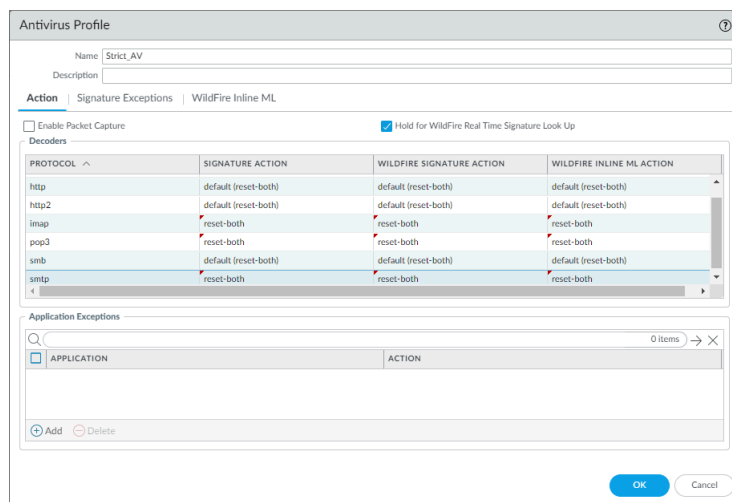
To ensure availability for business-critical applications, follow the [Transition Antivirus Profiles Safely to Best Practices](#) advice as you move from your current state to a best practices profile. The goal is to transition to profile as shown here and attach it to all Security policy rules that allow traffic. The Antivirus profile protocol decoders detect and prevent viruses and malware from being transferred over seven protocols: FTP, HTTP, HTTP2, IMAP, POP3, SMB, and SMTP.

Set WildFire Signature and WildFire Inline ML actions for all seven protocols (the Antivirus profile also enforces actions based on WildFire signatures) and if you haven't already done it, enable real-time signature lookup as shown in [Transition Antivirus Profiles Safely to Best Practices](#).

Configure the cloned Antivirus profile to reset both the client and the server for all seven protocol decoders and WildFire actions, and then attach the profile to the Security policy allow rules.



If you treat internal applications differently than external applications, you might need an Antivirus profile for internet-facing traffic and a different Antivirus profile for internal traffic.



Enable real-time signature lookup globally and in the Antivirus profile to hold files until the firewall receives the latest real-time antivirus signature from the cloud:

- Enable **globally**: **Device > Setup > Content-ID > Content-ID Settings > Realtime Signature Lookup**, enable **Hold for WildFire Real Time Signature Look Up** and set the **Action on Real Time Signature Timeout** to **Reset Both**. You must enable real-time signature lookup globally to enable it in Antivirus profiles.
- Enable **Hold for WildFire Real Time Signature Lookup** in the Antivirus profile. Holding files to ensure that WildFire gets the latest antivirus signatures protects you from zero-day malware and outdated antivirus signatures that you might be exposed to if you forward files without holding them for the latest signatures.

Why do I need this profile?

By attaching Antivirus profiles to all Security rules, you block known malicious files (malware, ransomware bots, and viruses) as they come into the network. Common ways for users to receive malicious files include email attachments, links to download malicious files, and silent compromise facilitated by Exploit Kits that exploit a vulnerability and then automatically download malicious payloads to the end user's device.

Best Practice Internet Gateway Vulnerability Protection Profile

Attach a [Vulnerability Protection profile](#) to all allowed traffic to protect against buffer overflows, illegal code execution, and other attempts to exploit client- and server-side vulnerabilities. To ensure availability for business-critical applications, follow the [Transition Vulnerability Protection Profiles Safely to Best Practices](#) advice as you move from your current state to the best practice profile. Clone the predefined strict Vulnerability Protection profile and edit it to create the best practice profile:

- Change the **Action** in the three brute force rules to **reset-both** and **Packet Capture** to **single-packet** to transition from alerting on brute-force attack events to blocking them.
- Consolidate critical, high, and medium severity events for servers and clients into one rule. Set the **Action** to **reset-both** and set **Packet Capture** to **single-packet**. This simplifies the profile and works because the profile uses the same action and the same packet capture settings for these severities.



*For profiles that control internal (east-west) traffic, blocking medium severity events might impact business applications. If blocking impacts business applications, create a separate rule in the profile for medium severity events with the **Action** set to **alert**. Apply the profile only to internal traffic.*

- To simplify the profile, consolidate low severity events for servers and clients into one rule. Set the **Action** to **default** and set **Packet Capture** to **single-packet**.
- Consolidate informational events for servers and clients into one rule. Set the **Action** to **default** and set **Packet Capture** to **disable**.

PCAPs for informational events generate a relatively high volume of traffic that usually isn't useful compared captures about potential threats.

- Apply extended PCAP instead of single PCAP to high-value traffic to which you apply the **alert** Action. Apply PCAP using the same logic you use to decide what traffic to log and take PCAPs of the traffic you log. Apply single PCAP to traffic you block. The default number of packets that extended PCAP records and sends to the management plane is five packets, which is the recommended value. In most cases, capturing five packets provides enough information to analyze a threat. If too much PCAP traffic goes to the management plane, then capturing more than five packets might result in dropping PCAPs.



*If you want more granularity for fine-tuning the profile, create separate rules with the **Action** and **Packet Capture** settings as described. For example, create a rule for critical, high, and medium severities for servers and another similar rule for clients, or create separate rules for each severity for clients and for servers to achieve the level of granularity and control you want.*



Packet captures consume management plane resources. Check system resources (for example, **Dashboard > System Resources**) to understand usage before and after you implement packet capture to ensure that your system has sufficient resources to take the packet captures you want.

Enable **packet capture (PCAP)** for each rule so you can track down the source of potential attacks. Download **content updates** automatically and install them as soon as possible so that the signature set is always up to date.

RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
simple-server-critical-brute	any	any	any	critical	reset-both	single-packet
simple-server-high-brute	any	any	any	high	reset-both	single-packet
simple-server-medium-brute	any	any	any	medium	reset-both	single-packet
simple-critical-high-medium	any	any	any	critical	reset-both	single-packet
simple-low	any	any	any	low	default	single-packet
simple-informational	any	any	any	informational	default	disable

For **Inline Cloud Analysis**, set the **Action** to **reset-both** to block common hacking techniques

MODEL	DESCRIPTION	ACTION
SQL Injection	Detects a common hacking technique where an attacker inserts SQL queries into an applications' request	reset-both
Command Injection	Detects a common hacking technique that allows an attacker to execute arbitrary operating system (OS)	reset-both

Why do I need this profile?

Without strict vulnerability protection, attackers can leverage client- and server-side vulnerabilities to compromise end-users. For example, an attacker could leverage a vulnerability to install malicious code on client systems or use an Exploit Kit to automatically deliver malicious payloads to end users. Vulnerability Protection profiles prevent an attacker from using vulnerabilities on internal hosts to move laterally within your network.

Best Practice Internet Gateway Anti-Spyware Profile

Attach an [Anti-Spyware profile](#) to all allowed traffic to detect command-and-control traffic (C2) initiated from malicious code running on a server or endpoint and prevent compromised systems from establishing an outbound connection from your network. Clone the predefined strict Anti-Spyware profile and edit it. To ensure availability for business-critical applications, [transition Anti-Spyware Profiles Safely to Best Practices](#). Edit the profile to enable DNS sinkhole and [packet capture](#) (PCAP) to help you track down endpoints that attempt to resolve malicious domains. Retain the default **Action** to reset the connection when the firewall detects a medium, high, or critical severity threat, and enable single PCAP for those threats.



Allow traffic only to sanctioned DNS servers. Use the [DNS Security service](#) to prevent connections to malicious DNS servers.



If you treat internal applications differently than external applications, you might need an Anti-Spyware profile for internet-facing traffic and a different Anti-Spyware profile for internal traffic.

POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/> simple-critical	critical	reset-both	single-packet
<input type="checkbox"/> simple-high	high	reset-both	single-packet
<input type="checkbox"/> simple-medium	medium	reset-both	single-packet
<input type="checkbox"/> simple-informational	informational	default	disable
<input type="checkbox"/> simple-low	low	default	disable

Don't enable PCAP for informational activity because it generates a relatively high volume of traffic and isn't usually useful compared to PCAPs for potential threats. Apply extended PCAP instead of single PCAP to high-value traffic to which you apply the **alert** Action. Apply PCAP using the same logic you use to decide what traffic to log and take PCAPs of the traffic you log. Apply single PCAP to traffic you block. The default number of packets that extended PCAP records and sends to the management plane is five packets, which is the recommended value. In most cases, capturing five packets provides enough information to analyze a threat. If too much PCAP traffic goes to the management plane, then capturing more than five packets might result in dropping PCAPs.



*Packet captures consume management plane resources. Check system resources (for example, [Dashboard](#) > **System Resources**) to understand usage before and after you implement packet capture to ensure that your system has sufficient resources to take all the packet captures you want.*

Configure DNS Policies to protect your network from DNS queries to malicious domains. For best security use the [DNS Security service](#) to secure your DNS traffic. Otherwise, use locally available, downloadable DNS signature sets (packaged with the antivirus and WildFire updates).

Sinkhole malicious traffic instead of blocking it to identify potentially compromised hosts that attempt to access suspicious domains by tracking the hosts and preventing them from accessing those domains. For domain categories that pose a greater threat, configure a higher log severity level and/or packet capture settings to help determine if the attack was successful, identify the attack methods, and provide better overall context.

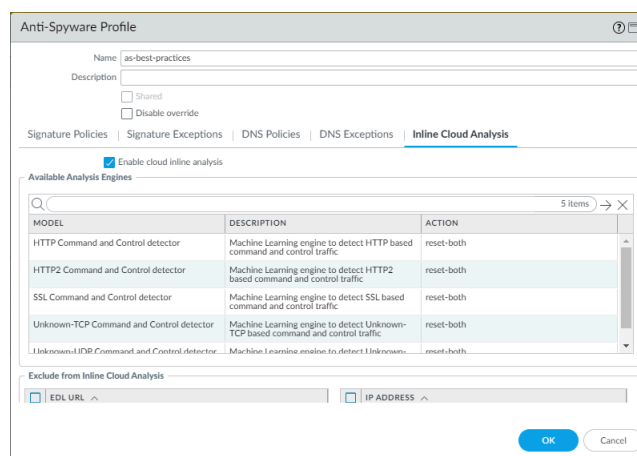
Configure the default Palo Alto Networks DNS and the individual [DNS signature source categories](#) (PAN-OS 10.0 and later):

DNS Signature Source	Log Severity	Policy Action	Packet Capture
Palo Alto Networks Content			
default-paloalto-dns	default	sinkhole	extended-capture
DNS Security			
Command And Control Domains	high (default)	sinkhole	extended-capture
Dynamic DNS Hosted Domains	informational (default)	sinkhole	single-packet
Grayware Domains	low (default)	sinkhole	single-packet
Malware Domains	medium (default)	sinkhole	single-packet
Parked Domains	informational (default)	sinkhole	disable (default)
Phishing Domains	low (default)	sinkhole	single-packet
Proxy Avoidance and Anonymizers	low (default)	sinkhole	single-packet
Newly Registered Domains	informational (default)	sinkhole	single-packet
Ad Tracking Domains	informational (default)	sinkhole	single-packet

For **Inline Cloud Analysis** (requires Advanced Threat Prevention subscription), **Enable cloud inline analysis** on all outbound traffic. Set the **Action** to **reset-both** for all models.



Air-gapped environments can't use Advanced Threat Prevention because it's a cloud service and requires a cloud connection.



Best Practice Internet Gateway URL Filtering Profile

Use [Advanced URL filtering](#) to prevent access to web content at high-risk for malicious activity. Attach a [URL Filtering profile](#) to all rules that allow access to web-based applications to protect against URLs that Palo Alto Networks has observed hosting malware, potential malware, liability risk, and exploitive content.



You must enable [decryption](#) to take advantage of URL Filtering because you must decrypt traffic to reveal the exact URL so the firewall can take the appropriate action. At the least, decrypt high- and medium-risk traffic.

To ensure availability for business-critical applications, [Transition URL Filtering Profiles Safely to Best Practices](#). A best practices URL Filtering profile sets all known dangerous URL categories and credential submissions to block. The goal is to block the following categories:

- Set all actions for malicious URL categories to block both Site Access and User Credential Submission. Make appropriate exceptions for PEN testing, threat research, and infosec as needed:
 - **command-and-control**—URLs and domains that malware or compromised systems use to communicate with an attacker’s remote server.
 - **grayware**—These sites don’t meet the definition of a virus or pose a direct security threat, but they influence users to grant remote access or perform other unauthorized actions. Grayware sites include scams, illegal activities, criminal activities, adware, and other unwanted and unsolicited applications, including “typosquatting” domains.
 - **malware**—Sites known to host malware or used for command-and-control activities.
 - **phishing**—Sites known to host credential and personal information phishing pages, including technical support scams and scareware.
 - **ransomware**—Sites that are known to distribute ransomware.
 - **scanning-activity**—Sites that probe for existing vulnerabilities or conduct targeted attacks.
- Some URL categories have the strong potential to be malicious but aren't definitely malicious. Set all actions for these URL categories to block both Site Access and User Credential

Submission. Make appropriate exceptions for PEN testing, threat research, and infosec as needed:

- **dynamic-dns**—Systems with dynamically assigned IP addresses that are often used to deliver malware payloads or command-and-control malware.
 - 📋 *If you have a business purpose for a dynamic DNS domain, then make sure you allow those URLs in your URL Filtering profile.*
- **hacking**—Sites relating to illegal or questionable access to or use of equipment and software. Includes sites that facilitate the bypass of licensing and digital rights systems.
 - 📋 *Make exceptions to this category for the appropriate PEN testing and threat research users.*
- **insufficient-content**—Websites and services that present test pages, no content, provide API access not intended for end-user display, or require authentication without displaying any other content.
- **newly-registered-domains**—Domains that domain generation algorithms often generate or bad actors generate for malicious activity.
- **not-resolved**—If the PAN-DB cloud is unreachable and the URL isn't in the firewall's URL Filtering cache, the firewall can't resolve and identify the URL category.
 - 📋 *For highest security, enable **Hold client request for category lookup** to give the firewall more time to resolve the URL category. This extends the time the firewall has to query the category type from the cloud and results in better security but might increase latency.*
- **parked**—Domains that will often be used for credential phishing or personal information theft.
- **proxy-avoidance-and-anonymizers**—URLs and services often used to bypass content filtering products.
- **unknown**—Sites not yet identified by Palo Alto Networks (PAN-DB).
 - 📋 *PAN-DB real-time updates learn unknown sites after the first attempt to access an unknown site, so the firewall identifies unknown URLs quickly and then handles them based on the actual URL category of the site.*

If availability is critical to your business and you must allow traffic from unknown sites, apply the strictest Security profiles to the traffic and investigate all alerts for the traffic.

- Set the action for Site Access and User Credential Submission to block the following URL categories based on legal or business requirements and potential liability risk. If you don't block these sites, alert on and apply strict Security profiles to the traffic.
 - **abused-drugs**—Sites that promote illegal and legal drug abuse.
 - **adult**—All sites that contain adult content of any kind, including games and comics as well as sexually explicit material, media, art, forums, and services.
 - **copyright-infringement**—Domains with illegal content that poses a liability risk.
 - **extremism**—Websites promoting terrorism, racism, child exploitation, etc.
 - **gambling**—Lottery and gambling sites.
 - **peer-to-peer**—Peer-to-peer sharing of torrents, download programs, media files, or other software applications. (Doesn't include shareware or freeware sites.)
 - **questionable**—Sites that promote tasteless humor, offensive content targeting specific demographics.
 - **weapons**—Sale, review, descriptions of, or instructions regarding weapons and their use.

Also consider how you want to handle the cryptocurrency and alcohol-and-tobacco URL categories. Either alert on them and apply strict Security profiles to the traffic or block them, depending on your business needs.

- Block User Credential Submission for the high-risk category. (Do not block Site Access for the high-risk category.)

In addition to blocking known bad categories, alert on all other categories so you have visibility into the sites your users visit. If you need to phase in a block policy, set categories to continue and [create a custom response page](#) to educate users about your acceptable use policies and alert them to the fact they are visiting a site that might pose a threat. This paves the way for you to block the categories after a monitoring period.

NAME	LOCATION	SITE ACCESS	USER CREDENTIAL SUBMISSION
<input type="checkbox"/> default	Predefined	Allow Categories (59) Alert Categories (5) Continue Categories (0) Block Categories (11) Override Categories (0)	Allow Categories (75) Alert Categories (0) Continue Categories (0) Block Categories (0)
<input checked="" type="checkbox"/> best-practices	lab-DG	Allow Categories (0) Alert Categories (54) Continue Categories (0) Block Categories (21) Override Categories (0)	Allow Categories (0) Alert Categories (53) Continue Categories (0)

Value >

Block Categories

- abused-drugs
- adult
- command-and-control
- copyright-infringement
- dynamic-dns
- extremism
- gambling
- grayware
- hacking
- insufficient-content
- malware
- newly-registered-domain
- not-resolved
- parked
- peer-to-peer
- phishing
- proxy-avoidance-and-anonymizers
- questionable
- ransomware
- unknown
- weapons

Disable **Log Container Page Only** in the profile, which is enabled by default. If you only log container pages, you lose visibility into functional applications such as posting, uploading,

downloading, etc. Disable **Log Container Page Only** to see the complete log so that you see the real functional application.

If your environment is a school that takes federal funding, enable **Safe Search Enforcement** (legal requirement).

If you run PAN-OS 9.0.4 or later, enable the option to hold client requests (enter **config** then **set deviceconfig setting ctd hold-client-request yes**) to ensure that the firewall handles user web requests as securely as possible. By default, the firewall allows requests while it looks up an uncached URL category in **PAN-DB** and then enforces the appropriate policy when the server responds. Hold requests during this lookup to maximize security (this might increase latency but is the most secure option). For details, see [Configure URL Filtering](#).

What if I can't block all of the recommended categories?

If users need access to sites in blocked categories for business purposes, create an allow list for just the specific sites in a rule that allows only the necessary users and applications, if you feel the risk is justified. Understand local laws and regulations that govern the types of sites you can block, can't block, and must block. On risky categories for which you decide to allow access, [set up credential phishing protection](#) to ensure that users don't submit corporate credentials to a site that might host a phishing attack.

If you allow traffic to malicious and potentially malicious URL categories or to websites that pose potential liability issues, the risks include:

- Malicious URL categories:
 - **command-and-control**—Command-and-control URLs and domains used by malware and/or compromised systems to surreptitiously communicate with an attacker's remote server to receive malicious commands or exfiltrate data.
 - **grayware**—Websites and services that don't meet the definition of a virus but are malicious or questionable and might degrade device performance and cause security risks. Prior to Content release version 8206, the firewall placed grayware in either the malware or questionable URL category. If you are unsure about whether to block grayware, start by alerting on grayware, investigate the alerts, and then decide whether to block grayware or continue to alert on grayware.
 - **malware**—Sites known to host malware or used for command and control (C2) traffic and that might exhibit Exploit Kits.
 - **phishing**—Known to host credential phishing pages or phishing for personal identification.
 - **ransomware**—Sites that are known to distribute ransomware.
 - **scanning-activity**—Sites that probe for existing vulnerabilities or conduct targeted attacks.
- Potentially malicious URL categories:
 - **dynamic-dns**—Hosts and domain names for systems with dynamically assigned IP addresses and which are oftentimes used to deliver malware payloads or C2 traffic. Also, dynamic

DNS domains don't go through the same vetting process as domains that are registered by a reputable domain registration company, and are therefore less trustworthy.

- **hacking**—Sites relating to illegal or questionable access to or use of equipment and software. Includes sites that facilitate the bypass of licensing and digital rights systems.



Make exceptions to this category for the appropriate PEN testing and threat research users.

- **insufficient-content**—Websites and services that present test pages, no content, provide API access not intended for end-user display, or require authentication without displaying any other content.
- **newly-registered-domain**—Newly registered domains are often generated purposely or by domain generation algorithms and used for malicious activity.
- **not-resolved**—If the PAN-DB cloud is unreachable and the URL isn't in the firewall's URL Filtering cache, the firewall can't resolve and identify the URL category.



*For highest security, enable **Hold client request for category lookup** to give the firewall more time to resolve the URL category. This extends the time the firewall has to query the category type from the cloud and results in better security but might increase latency.*

- **parked**—Domains registered by individuals, oftentimes later found to be used for credential phishing. These domains might be similar to legitimate domains, for example, pal0alto0netw0rks.com, with the intent of phishing for credentials or personal identify information. Or, they might be domains that an individual purchases rights to in hopes that it might be valuable someday, such as panw.net.
- **proxy-avoidance-and-anonymizers**—URLs and services often used to bypass content filtering products.
- **unknown**—Sites that have not yet been identified by PAN-DB. If availability is critical to your business and you must allow the traffic, alert on unknown sites, apply the best practice Security profiles to the traffic, and investigate the alerts.



PAN-DB Real-Time Updates learns unknown sites after the first attempt to access an unknown site, so unknown URLs are identified quickly and become known URLs that the firewall can then handle based on the actual URL category.

- URL categories with potential liability risk:
 - **abused-drugs**—Websites that promote the abuse of legal and illegal drugs, the sale and use of drug paraphernalia, and manufacturing or selling drugs.
 - **adult**—Websites that might not be appropriate in the workplace.
 - **copyright-infringement**—Domains with illegal content, such as content that allows illegal download of software or other intellectual property, which poses a potential liability risk. This category was introduced to enable adherence to child protection laws required in the education industry as well as laws in countries that require internet providers to prevent users from sharing copyrighted material through their service.
 - **extremism**—Websites promoting terrorism, racism, fascism, or other extremist views discriminating against people or groups of different ethnic backgrounds, religions or other beliefs. This category was introduced to enable adherence to child protection laws required

in the education industry. In some regions, laws and regulations might prohibit allowing access to extremist sites, and allowing access might pose a liability risk.

- **gambling**—Lottery or gambling websites that facilitate the exchange of real and/or virtual money. Also websites that provide tutorials, advice, or other information about gambling, including betting odds and pools.
- **peer-to-peer**—Websites that clients for or access to peer-to-peer sharing of torrents, download programs, media files, or other software applications, primarily to protect against bitTorrent download capabilities. Does not include shareware or freeware sites.
- **questionable**—Websites containing potentially offensive content targeting specific demographics of individuals or groups, criminal activity, illegal activity, and get rich quick schemes.
- **weapons**—Websites that sell, review, describe, or provide instructions about weapons and their use that might not be appropriate in the workplace.



The default URL Filtering profile blocks the malware, phishing, and command-and-control URL categories, but not the rest of the categories recommended categories to block. The default URL Filtering profile also blocks the abused-drugs, adult, gambling, questionable, and weapons URL categories. Whether to block these URL categories depends on your business requirements. For example, a university probably won't restrict student access to most of these sites because availability is important, but a business that values security first might block all of them.

URL Filtering Examples

URL Filtering works with file blocking, decryption, external dynamic lists (EDLs), logging, and other security capabilities to create granular policies that can go beyond simply blocking or allowing entire URL categories. Use the [URL Filtering safe transition steps](#) to evaluate what sites you want to allow and what sites you want to block, then implement policies that fit your business requirements. For example:

- Use risk-based URL categories (high-risk, medium-risk, and low-risk) in combination with other URL categories to target decryption or to target blocking traffic. For example, you can:
 - Block traffic to high-risk websites in the financial-services category.
 - Decrypt all high-risk and medium-risk web traffic.
 - Decrypt high-risk and medium-risk traffic to specific URL categories if the firewall doesn't have sufficient resources to decrypt all the traffic you want to decrypt.
- Log all user agents and referrers, all URLs, and all file downloads for high-risk and medium-risk category domains to increase visibility.
- Allow access to categories such as personal-sites-and-blogs while applying a File Blocking profile to the traffic to prevent downloading risky content such as .exe, .scr, and other potentially malicious files.
- Use the predefined **Palo Alto Networks - Bulletproof IP addresses** EDL to prevent access to sites hosted on Bulletproof ISPs, especially if you allow access to high-risk or medium-risk finance sites.
- Use combinations of URL categories to simplify policy.

Best Practice Internet Gateway WildFire Analysis Profile

Forward files to WildFire for analysis to protect your network from unknown threats. Without this protection, attackers can infiltrate your network and exploit vulnerabilities in the applications your employees use everyday. Because WildFire protects against unknown threats, it's your best defense against advanced persistent threats (APTs).

Set up [WildFire appliance content updates](#) to download and install automatically in real-time so that you always have the most recent support.

The best practices [WildFire Analysis profile](#) sends all files in both directions (upload and download) to WildFire for analysis. Specifically, make sure you are sending all PE files (if you're not blocking them in accord with file blocking best practices), Adobe Flash and Reader files (PDF, SWF), Microsoft Office files (PowerPoint, Excel, Word, RTF), Java files (Java, .CLASS), and Android files (.APK).

WildFire Analysis Profile
?

Name

Description

1 item → ×

<input type="checkbox"/>	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
<input type="checkbox"/>	Send all	any	any	both	public-cloud

+ Add
- Delete

OK
Cancel

Set up [alerts for malware](#) through email, SNMP, or a syslog server so that the firewall immediately notifies you when it encounters a potential issue. The faster you isolate a compromised host, the lower the chance the previously unknown malware has spread to other data center devices, and the easier it is to remediate the issue.

If necessary, you can restrict the applications and file types sent for analysis based on the traffic's direction.



*WildFire Action settings in the Antivirus profile might impact traffic if the traffic generates a WildFire signature that results in a reset or a drop action. You can exclude internal traffic such as software distribution applications through which you deploy custom-built programs to [transition safely](#) to best practices (otherwise, WildFire might identify custom-built programs as malicious and generate a signature for them). Check **Monitor > Logs > WildFire Submissions** to see if any internal custom-built programs trigger WildFire signatures.*

Define the Initial Internet Gateway Security Policy

The goal of a best practices internet gateway security policy is to use positive enforcement of allowed applications. However, it takes time to identify the exact applications that run on your network, which applications are critical to your business, and who needs to access to each application. To create a Security policy based on application allow rules, start with a rulebase that liberally allows the applications you officially sanction for users, and tolerated general business applications and personal applications (if appropriate for your business).

The initial policy includes rules that explicitly block known malicious IP addresses and applications, and temporary allow rules that help refine your policy and preserve application availability while you transition to a best practices policy.



To apply consistent security policy across multiple locations, you [reuse templates and template stacks](#) so that the same policies apply to every internet gateway firewall at every location. Templates use variables to apply device-specific values such as IP addresses, FQDNs, etc., while maintaining a global security policy and reducing the number of templates and template stacks you need to manage.

The following topics describe how to create the initial rulebase, describe why each rule is necessary, and illuminate the risks of ignoring best practices recommendations:

- [Step 1: Create Rules Based on Trusted Threat Intelligence Sources](#)
- [Step 2: Create the Application Allow Rules](#)
- [Step 3: Create the Application Block Rules](#)
- [Step 4: Create the Temporary Tuning Rules](#)
- [Step 5: Enable Logging for Traffic that Doesn't Match Any Rules](#)

Step 1: Create Rules Based on Trusted Threat Intelligence Sources

Block traffic from hosts that Palo Alto Networks and trusted third-party sources have proven malicious. An Advanced Threat Prevention license (or an active legacy Threat Prevention license) includes [built-in external dynamic lists](#) (EDLs) that contain known malicious IP addresses. Use EDLs in policy to block malicious traffic. Palo Alto Networks compiles and dynamically updates the lists based on the latest threat intelligence. Firewalls receive and implement Dynamic Updates without the need for a reboot.

STEP 1 | Block traffic to and from IP addresses that Palo Alto Networks identifies as malicious.

Why Do I Need These Rules?	Rule Highlights
<ul style="list-style-type: none"> ❑ This rule protects you against IP addresses that Palo Alto Networks has proven to be used almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks. 	<ul style="list-style-type: none"> • One rule blocks outbound traffic to known malicious IP addresses, while the other rule blocks inbound traffic to those addresses. • Set the external dynamic list Palo Alto Networks - Known malicious IP addresses as the Destination address for the

Why Do I Need These Rules?	Rule Highlights
	<p>outbound traffic rule, and as the Source address for the inbound traffic rule.</p> <ul style="list-style-type: none"> Deny traffic that matches these rules. Enable logging for traffic matching these rules so you can investigate potential threats on your network. Because these rules stop malicious traffic, they protect traffic from any user running on any port.

NAME	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Drop Outbound Malicious IP	universal	any	any	any	any	any	Palo Alto Networks - Known malicio...	any	any	any	Deny	none	
Drop Inbound Malicious IP	universal	any	Palo Alto Networks - Known malic...	any	any	any	any	any	any	any	Deny	none	

STEP 2 | Block traffic to and from Bulletproof hosting providers.

Why Do I Need These Rules?	Rule Highlights
<p>□ This rule protects you against IP addresses that Palo Alto Networks has shown to belong to Bulletproof hosting providers.</p> <p>Bulletproof hosting providers have no or limited restrictions on content and don't log events. Bulletproof sites are ideal places from which to launch command-and-control (C2) attacks and illegal activity because anything goes and nothing is tracked.</p>	<ul style="list-style-type: none"> One rule blocks outbound traffic to known Bulletproof hosting IP addresses, while another rule blocks inbound traffic to those addresses. Set the external dynamic list Palo Alto Networks - Bulletproof IP addresses as the Destination address for the outbound traffic rule, and as the Source address for the inbound traffic rule. Deny traffic that matches these rules. Enable logging for traffic matching these rules so that you can investigate potential threats on your network. Because these rules stop malicious traffic, they protect traffic from any user running on any port.

NAME	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Drop Outbound Bulletproof IP	universal	any	any	any	any	any	Palo Alto Networks - Bulletproof IP ...	any	any	any	Deny	none	
Drop Inbound Bulletproof IP	universal	any	Palo Alto Networks - Bulletproof L...	any	any	any	any	any	any	any	Deny	none	

STEP 3 | Block and log traffic to and from high-risk IP addresses from trusted threat advisories.


Why Do I Need These Rules?	Rule Highlights
<p>Although Palo Alto Networks has no direct evidence of the maliciousness of the IP addresses in the high-risk IP address feed, threat advisories have linked them to malicious behavior.</p> <ul style="list-style-type: none"> ❑ Block and log the traffic as shown in this example. ❑ If you must allow a high-risk IP address for business reasons, create a Security policy rule with strict Security profiles that allows only that IP address and place it in front of the high-risk IP address block rule in the rulebase. Closely monitor and log any high-risk IP addresses that you choose to allow. 	<ul style="list-style-type: none"> • One rule logs blocked outbound traffic to high-risk IP addresses and another rule logs blocked inbound traffic to those addresses. • Set the external dynamic list Palo Alto Networks - High risk IP addresses as the Destination address for the outbound traffic rule and as the Source address for the inbound traffic rule. • If you allow the traffic, apply best practices Security profiles. • Because these rules stop malicious traffic, they protect traffic from any user running on any port, for any application.

NAME	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Block Outbound High Risk IPs	universal	any	any	any	any	any	Palo Alto Networks - High risk IP addresses	any	any	any	Deny	none	Log, Alert
Block Inbound High Risk IPs	universal	any	Palo Alto Networks - Known malicious IP addresses	any	any	any	any	any	any	any	Deny	none	Log, Alert

STEP 4 | Similarly, create two rules that block and log traffic to and from Tor exit nodes, which are often (but not always) associated with malicious activity, especially in enterprise environments, using the **Palo Alto Networks - Tor exit IP addresses** external dynamic list.

Step 2: Create the Application Allow Rules


Identify Your Application Allow List before you create application allow rules. Create allow rules based on applications, not on ports. Except for certain infrastructure applications that require user access before the firewall can identify the user, allow access only to known users. [Create User Groups for Access to Allowed Applications](#) and limit user access to only the specific users or user groups who have a business need to access each application.

 *To convert port-based rules to application-based rules or to migrate from a port-based firewall, follow the advice in [Best Practices for Migrating to Application-Based Policy](#), which leverages [Policy Optimizer](#). Policy Optimizer helps you analyze port-based rules and show you the exact applications that match those rules. It also helps you find unused rules, rules with unused applications (over-provisioned rules), and existing port-based rules.*

Place specific rules above general rules in the Security policy rulebase. Otherwise, a general rule might shadow a specific rule. (Shadowing is when you place a broad rule that includes the same match criteria as a more specific rule higher in the rulebase than the specific rule, so traffic intended to match the specific rule instead matches the general rule.)


This part of the rulebase includes the allow rules for applications you identified as part of your application allow list, including:

- Sanctioned applications you provision and administer for business and infrastructure purposes.
- General business applications users might need to get their jobs done.
- Tolerated applications you choose to allow for personal use.

 **Tag all sanctioned applications with the predefined Sanctioned tag.** Panorama and firewalls consider applications without the Sanctioned tag as unsanctioned applications.

Attach best practices Security profiles to scan all allowed traffic for known and unknown threats. If you haven't created these profiles, then [Create Best Practice Security Profiles for the Internet Gateway](#). Because you can't inspect what you can't see, configure the firewall to [Decrypt Traffic for Full Visibility and Threat Inspection](#).

STEP 1 | Allow access to your corporate DNS servers.

 Allow traffic only to sanctioned DNS servers. Use the [DNS Security service](#) to prevent connections to malicious DNS servers.

Why Do I Need This Rule?							Rule Highlights						
<ul style="list-style-type: none"> ❑ Access to DNS provides network infrastructure services and is commonly exploited by attackers. ❑ Allowing access only on your internal DNS server reduces your attack surface. 							<ul style="list-style-type: none"> • Because this rule is very specific, place it near the top of the rulebase. • Create an address object to use for the destination address to ensure that users only access the DNS server in your data center. • Because users need access to these services before they log in, allow access to any user. 						

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
IT DNS Services	Best Practice	universal	Users	any	any	any	IT Infrastructure	DNS Servers	any	dns	application-default	Allow		

STEP 2 | Allow access to other required IT infrastructure resources.

Why Do I Need This Rule?		Rule Highlights	
<ul style="list-style-type: none"> ❑ Enable applications that provide network infrastructure and management functions, such as NTP, OCSP, STUN, and ping. ❑ The preceding rule restricts allowed DNS traffic to the destination address in the data center, these applications might not 		<ul style="list-style-type: none"> • Because these applications run on the default port, allow access to any user (users might not yet be logged in and known because of when these services are needed), and have a destination address of any, add them to one application group and 	

Why Do I Need This Rule?	Rule Highlights
reside in your data center and therefore require a separate rule.	create one rule to enable access to all of them.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Required Infrastructure	Best Practice	universal	Users	any	any	any	Internet	any	any	Required Infrastructure	application-default	Allow		

STEP 3 | Allow access to IT sanctioned SaaS applications.

Why Do I Need This Rule?	Rule Highlights
<ul style="list-style-type: none"> ❑ With SaaS applications, proprietary data resides in the cloud. This rule ensures that only known users have access to these applications (and the underlying data). ❑ Scan allowed SaaS traffic for threats. 	<ul style="list-style-type: none"> • Create an application group to control all sanctioned SaaS applications. • SaaS applications should always run on the application-default port. • Restrict access to known users. See Create User Groups for Access to Allowed Applications.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
IT Sanctioned SaaS Apps	Best Practice	universal	Users	any	known-user	any	Internet	any	any	IT Sanctioned SaaS Applica...	application-default	Allow		

STEP 4 | Allow access to IT provisioned on-premises applications.

Why Do I Need This Rule?	Rule Highlights
<ul style="list-style-type: none"> ❑ Attacks often use business-critical data center applications such as FTP during the exfiltration stage or exploit application vulnerabilities to move laterally. ❑ Many data center applications use multiple ports. Setting the Service to application-default safely enables applications on their standard ports. Don't allow applications on non-standard ports, which is often associated with evasive behavior. 	<ul style="list-style-type: none"> • Create an application group to group all data center applications. • Create an address group for your data center server addresses. • Restrict access to known users. See Create User Groups for Access to Allowed Applications.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
IT Deployed Apps	Best Practice	universal	Users	any	known-user	any	Business Apps	Data Center	any	IT Deployed Apps	application-default	Allow		

STEP 5 | Allow access to applications your administrative users need.

Why Do I Need This Rule?			Rule Highlights										
<ul style="list-style-type: none"> To reduce your attack surface, create user groups for access to allowed applications. Because administrators often need access to sensitive account data and remote access to other systems (for example RDP), to reduce your attack surface, allow access only to administrators who have a business need. 			<ul style="list-style-type: none"> This rule restricts access to users in the IT_admins group. Create a custom application for each internal application or application that runs on non-standard ports so you can enforce them on their default ports rather than opening additional ports on your network. If you have different user groups for different applications, create separate rules for granular control. 										

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Administrative Apps	Best Practice	universal	Users	any	IT_Admins	any	IT Infrastructure	any	any	ms-rdp ssh	application-default	Allow		

STEP 6 | Allow access to general business applications.

Why Do I Need This Rule?			Rule Highlights										
<ul style="list-style-type: none"> In addition to applications you sanction and administer for users, users often need access to other business applications, such as Zoom, Adobe online services, or G Suite. This rule enables you to safely allow web browsing while scanning for threats. See Create Best Practice Security Profiles for the Internet Gateway. 			<ul style="list-style-type: none"> Restrict access to only known users. See Create User Groups for Access to Allowed Applications. For visibility, create an application filter for each type of application you want to allow. Attach best practices Security profiles to prevent known and unknown threats in all traffic. 										

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
General Business Apps	Best Practice	universal	Users	any	known-user	any	Internet	any	any	browser-based businesses office programs update software	application-default	Allow		

STEP 7 | (Optional) Allow access to personal applications.

Why Do I Need This Rule?			Rule Highlights										
<ul style="list-style-type: none"> As the lines blur between work and personal devices, that all applications your users access are safely enabled and free of threats. 			<ul style="list-style-type: none"> Restrict access to only known users. See Create User Groups for Access to Allowed Applications. For visibility, create an application filter for each type of application you want to allow. 										

Why Do I Need This Rule?	Rule Highlights
<ul style="list-style-type: none"> Use application filters to safely enable access to personal applications when you create this initial rulebase. After you assess the applications in use, use the information to decide whether to remove the filter and allow a smaller subset of personal applications appropriate for your acceptable use policies. 	<ul style="list-style-type: none"> Attach best practices Security profiles to prevent known and unknown threats in all traffic.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Allow Personal Apps	Best Practice	universal	Users	any	any	any	Internet	any	any	audio video gaming client-server internet utility instant messaging social-networking webmail	application-default	Allow		

STEP 8 | Allow general web browsing.

Why Do I Need This Rule?	Rule Highlights
<ul style="list-style-type: none"> The previous rule allowed access to personal applications (many of them browser-based). This rule allows general web browsing. General web browsing is more risk-prone than other types of application traffic. Create best practices Security profiles and attach them to this rule in order to safely enable web browsing. Because threats often hide in encrypted traffic, decrypt traffic for full visibility and threat inspection to safely enable web browsing. 	<ul style="list-style-type: none"> Use the same best practice security profiles as the other rules and tighten the URL Filtering profile as much as possible. To help prevent devices with malware or embedded devices from reaching the internet, allow only known users. Use application filters to allow access to general types of applications. Explicitly allow SSL as an application to allow users to browse to HTTPS sites that you choose to exclude from decryption. Set the Service to application-default.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
General Web Browsing	Best Practice	universal	Users	any	known-user	any	Internet	any	any	general browsing ssl yahoo-web-analytics	application-default	Allow		

Step 3: Create the Application Block Rules

Application block rules protect you from evasive and commonly exploited applications while you develop and tune your Security policy rulebase. [Temporary tuning rules](#) help find gaps in policy and identify possible attacks. Because they catch application traffic you didn't know was running on your network, they allow traffic that could pose security risks. The following block rules explicitly block potentially malicious applications and protocols that attackers commonly use,

such as public DNS and SMTP, encrypted tunnels, remote access, and non-sanctioned file-sharing applications.

STEP 1 | Block Quick UDP Internet Connections (QUIC) protocol.

Why Do I Need This Rule?	Rule Highlights
<ul style="list-style-type: none"> ❑ Chrome and some other browsers establish sessions using QUIC instead of TLS. QUIC uses proprietary encryption that the firewall can't decrypt, so potentially dangerous encrypted traffic might enter the network. ❑ Blocking QUIC forces the browser to fall back to TLS and enables the firewall to decrypt the traffic. 	<ul style="list-style-type: none"> • Create a Service (Objects > Services) that specifies UDP ports 80 and 443. • The first rule blocks QUIC on its UDP service ports (80 and 443) and uses the Service you created to specify those ports. • The second rule blocks the QUIC application.

The Service specifies the UDP ports to block for QUIC.

The first rule specifies the Service you configured for QUIC and the second rule blocks the QUIC application:

	NAME	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
1	Block QUIC UDP	universal	🏠 I3-vlan-trust	any	any	any	🏠 I3-untrust	any	any	any	🔗 quic_udp_ports	🚫 Deny	none	📄 📄
2	Block QUIC	universal	🏠 I3-vlan-trust	any	any	any	🏠 I3-untrust	any	any	📄 quic	🔗 application-default	🚫 Deny	none	📄 📄

STEP 2 | Block applications that don't have a legitimate use case.

Why Do I Need This Rule?	Rule Highlights
<ul style="list-style-type: none"> ❑ Block potentially malicious applications such as encrypted tunnels, peer-to-peer file sharing, and web-based file sharing applications that IT hasn't sanctioned. ❑ Because the temporary tuning rules might allow traffic with malicious intent as well as legitimate traffic that doesn't match your 	<ul style="list-style-type: none"> • Use the Drop Action to silently drop the traffic without sending a signal to the client or the server. • Enable logging for traffic matching this rule so that you can investigate potential threats and misuse of applications on your network.

Why Do I Need This Rule?	Rule Highlights
<p>policy rules as expected, they could allow risky or malicious traffic. This rule blocks traffic that has no legitimate use case and that an attacker or a negligent user could use.</p>	<ul style="list-style-type: none"> Because this rule is intended to catch malicious traffic, it matches traffic from any user running on any port.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Block Bad Apps	Best Practice	universal	Users	any	any	any	Internet	any	any	encrypted tunnels file sharing remote access	any	Drop	none	

STEP 3 | Block public DNS and SMTP applications.



Allow traffic only to sanctioned DNS servers. Use the [DNS Security service](#) to prevent connections to malicious DNS servers.

Why Do I Need This Rule?	Rule Highlights
<p>Block public DNS/SMTP applications to avoid DNS tunneling, command-and-control traffic, and remote administration applications.</p>	<ul style="list-style-type: none"> Use the Reset both client and server Action to send a TCP reset message to both the client-side and server-side devices. Enable logging for traffic that matches this rule so that you can investigate potential threats.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Block Public DNS and SMTP	Best Practice	universal	Users	any	any	any	Internet	any	any	dns smtp	any	Reset Both	none	

Step 4: Create the Temporary Tuning Rules

The temporary tuning rules help you monitor the initial best practices rulebase for gaps and alert you to alarming behavior.

For example, temporary rules identify traffic that comes from unknown users or from applications running on unexpected ports. Monitor traffic that matches the temporary rules to gain a full understanding of all of the applications in use on your network (and ensure application availability while you transition to a best practice rulebase). Use this information to help you fine-tune your allow list, either by adding new allow rules for applications you weren't aware you needed or to narrow your allow rules and replace application filters with application groups or specific applications. When traffic no longer matches these rules, you can [remove the temporary rules](#).



Some temporary tuning rules go above the rules that **block bad applications** and some go after to ensure that targeted traffic matches the appropriate rule, while ensuring that bad traffic doesn't get onto your network.

STEP 1 | Allow web-browsing and SSL on non-standard ports for known users to determine if there are any legitimate applications running on non-standard ports.

Why Do I Need This Rule?	Rule Highlights
<ul style="list-style-type: none"> ❑ This rule helps determine if you have gaps in your policy where users can't access legitimate applications because they run on non-standard ports. ❑ Monitor all traffic that matches this rule. For legitimate traffic, add the appropriate applications to the appropriate allow rules. Create a custom application when appropriate. 	<ul style="list-style-type: none"> • Unlike allow rules that allow applications only on the default port, this rule allows web-browsing and SSL traffic on any port to find gaps in your allow list. • Because this rule finds gaps in policy, limit it to known users on your network. • Explicitly allow SSL as an application in this rule if you want to allow users to be able to browse HTTPS sites that aren't decrypted (for example, financial services and healthcare sites). • Attach best practices security profiles to scan for threats. • Add this rule above the application block rules or no traffic will match this rule.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Unexpected Port SSL and Web	Best Practice	universal	Users	any	known-user	any	Internet	any	any	ssl web-browsing	any	Allow		

STEP 2 | Allow web-browsing and SSL traffic on non-standard ports from unknown users to highlight all unknown users regardless of port.

Why Do I Need This Rule?	Rule Highlights
<ul style="list-style-type: none"> ❑ This rule helps determine whether you have gaps in your User-ID coverage. ❑ This rule helps identify compromised or embedded devices that try to reach the internet. 	<ul style="list-style-type: none"> • While the majority of the application allow rules apply to known users or specific user groups, this rule explicitly matches traffic from unknown users. • This rule must go above the application block rules or traffic will never hit it.

Why Do I Need This Rule?

- It's important to block non-standard port usage, even for web-browsing traffic, because it is an evasion technique.

Rule Highlights

- Attach best practices security profiles to scan for threats.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Unknown User SSL and Web	Best Practice	universal	Users	any	unknown	any	Internet	any	any	ssl web-browsing	any	Allow		

STEP 3 | Allow all applications on the application-default port to identify unexpected applications.

Why Do I Need This Rule?

- This rule provides visibility into applications that you weren't aware were running on your network so that you can fine-tune your application allow list.
- Monitor all traffic that matches this rule to determine whether it represents a potential threat or whether you need to modify your allow rules to enable access to more applications.

Rule Highlights

- Because this rule allows all applications, you must add it after the application block rules to prevent bad applications from running on your network.
- If you run PAN-OS 7.0.x or earlier, to appropriately identify unexpected applications, [create an application filter](#) that includes all applications, instead of setting the rule to allow any application.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Unexpected Traffic	Best Practice	universal	Users	any	any	any	Internet	any	any	All apps	application-default	Allow		

STEP 4 | Allow any application on any port to identify applications running on non-standard ports.

Why Do I Need This Rule?

- This rule helps identify legitimate, known applications running on unknown ports.
- This rule helps identify unknown applications for which you need to create a custom application and add to your application allow rules.
- Traffic that matches this rule is actionable. Track down the source of the traffic and ensure that you don't allow unknown tcp, udp, or non-syn-tcp traffic.

Rule Highlights

- Because this is a very general rule that allows any application from any user on any port, place it at the bottom of the rulebase.
- Enable logging for traffic that matches this rule so that you can investigate misuse of applications and potential threats or identify legitimate applications that require a custom application.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Unexpected Port Usage	Best Practice	universal	Users	any	any	any	Internet	any	any	any	any	Allow		

Step 5: Enable Logging for Traffic That Doesn't Match Any Rules

Internet gateway traffic that flows between zones and that doesn't match the rules you defined matches the predefined interzone-default rule at the bottom of the rulebase and is denied. (The predefined intrazone-default allow rule matches traffic within the same zone by default; only traffic between different zones is denied by default.) To gain visibility into the traffic that doesn't match the allow and block rules you created, enable logging on the interzone-default rule:

STEP 1 | Select the row with the interzone-default rule in the rulebase and **Override** the rule to edit it.

STEP 2 | Select the **interzone-default** rule name to open the rule for editing.

STEP 3 | On the **Actions** tab, select **Log at Session End** and then click **OK**.

STEP 4 | To view the log information in one place, create a custom report to monitor traffic that matches the **interzone-default** rule:

1. Select **Monitor > Manage Custom Reports**.
2. **Add** a report and give it a **Name** that describes the content and purpose of the report.
3. Set the **Database** to **Traffic Summary**.
4. Select the **Scheduled** check box.
5. Set the **Time Frame** to specify the time period each report covers, set **Sort By** to sort the information by bytes, sessions, packets, or threats, and set **Group By** to determine how the information is grouped (by time, application, risk, etc.).
6. Add **Rule**, **Application**, **Bytes**, and **Sessions** to the Selected Columns list.
7. Define the query to match traffic that matches the **interzone-default** rule:

(rule eq 'interzone-default')

STEP 5 | **Commit** the changes you made to the rulebase.

Monitor and Fine-Tune the Policy Rulebase

Creating a best practice security policy is an iterative process. After you [define the initial internet gateway Security policy](#), monitor traffic that matches the temporary rules that identify policy gaps and alarming behavior, and tune your policy accordingly. Monitoring traffic that matches these rules enables you to make appropriate adjustments to the permanent rules and either make sure all traffic matches your application allow rules or assess whether you should allow applications that match no rules.

As you tune your rulebase, you should see less and less traffic that you want to allow matching the temporary rules. When you no longer see traffic that you want to allow matching these rules, your positive enforcement allow rules are complete and you can [remove the temporary rules](#) (the interzone-default deny rule automatically denies traffic that no rule explicitly allows).



Because monthly content releases add new App-IDs, [review the impact App-ID changes have on your Security policy](#).

STEP 1 | Create custom reports to monitor traffic that matches rules which identify policy gaps.

1. Select **Monitor > Manage Custom Reports**.
2. **Add** a report and give it a descriptive **Name** that indicates the policy gap you're investigating.
3. Set the **Database** to **Traffic Summary**.
4. Select **Scheduled**.
5. Add **Rule, Application, Bytes, Sessions** to the Selected Columns list.
6. Set the desired **Time Frame, Sort By, and Group By** fields.
7. Define the query to match traffic that matches the rules which find policy gaps and alarming behavior. You can create a single report which details traffic that matches any

of the rules (using the **or** operator) or create individual reports to monitor each rule. The following example queries use the rule names defined in the example policy:

- **(rule eq 'Unexpected Port SSL and Web')**
- **(rule eq 'Unknown User SSL and Web')**
- **(rule eq 'Unexpected Traffic')**
- **(rule eq 'Unexpected Port Usage')**

Custom Report

Report Setting

Load Template → Run Now

Name: Best Practice Policy Tuning

Description:

Database: Traffic Summary

Scheduled

Time Frame: Last Calendar Day

Sort By: Bytes Top 25

Group By: App Sub Category 50 Groups

Available Columns: Sessions, Source Address, Source Category, Source Country, Source Dynamic Address Group

Selected Columns: Application, Bytes, Rule, Sessions

Query Builder

(rule eq 'Unexpected Port SSL and Web') or (rule eq 'Unknown User SSL and Web') or (rule eq 'Unexpected Traffic') or (rule eq 'Unexpected Port Usage')

Filter Builder

OK Cancel

STEP 2 | Review the report regularly to understand why traffic matches each of the tuning rules. Either update rules to include legitimate applications and users or use the information in the report to assess the application's risk and implement policy reforms.

Remove the Temporary Rules

After several months of monitoring your initial internet gateway best practice security policy and tuning the rulebase, you should see less and less traffic that you want to allow matching the temporary rules. Keep in mind that some applications are only used quarterly or yearly for periodic meetings and events. Before you stop allowing an application by removing it from the temporary rules without adding it to another allow rule, make sure that it's not used only periodically and make sure that it's not an application that's critical to your business

When you no longer see traffic that you want to allow matching the temporary rules, you have achieved your goal of transitioning to a fully application-based Security policy rulebase. You can now remove the temporary rules, including the [application block rules](#) for applications that don't have a legitimate use case and for public DNS and SMTP applications because the default interzone-default deny rule automatically blocks that traffic since it matches no explicit allow rules. (Keep the rules that block QUIC for SSL Forward Proxy.)

STEP 1 | Select **Policies > Security**.

STEP 2 | Select the rule's row and click **Delete**.

Alternatively, **Disable** the temporary rules for a period of time before deleting them. Examine the Traffic logs for traffic that matches the **interzone-default** deny rule. If the Traffic logs reveal that traffic you want to allow matches the **interzone-default**, you can **Enable** them again, add the desired application to an existing allow rule, or create a new allow rule for the application.

STEP 3 | **Commit** the changes.

Maintain the Rulebase

Businesses and applications evolve, so your Security policy rulebase also needs to evolve. When your sanctioned applications change, make corresponding changes to existing policy rules that align with the application's business use case whenever possible instead of adding new rules. Often, the change is as simple as adding a new application to an application group or removing a deprecated application from an application group.



On Panorama or standalone firewalls, use the [policy rule hit counter](#) to analyze changes to the rulebase. For example, when you add a new application, before you allow that application's traffic on the network, add the allow rule to the rulebase. If traffic hits the rule and increments the counter, either traffic that matches the rule is already on the network even though you haven't activated the application, or you might need to tune the rule. Follow up by checking the **ACC > Threat Activity > Applications Using Non Standard Ports** and the **ACC > Threat Activity > Rules Allowing Apps On Non Standard Ports** widgets to see if traffic on non-standard ports caused the unexpected rule hits.

The key to using the policy rule hit counter is to reset the counter when you make a change, such as introducing a new application or changing a rule's meaning. Resetting the hit counter ensures that you see the result of the change, not results that include the change and events that happened before the change.



If you use Panorama to manage firewalls, [monitor firewall health](#) to compare devices to their baseline performance and to each other to identify deviations from normal behavior.

Set Palo Alto Networks content updates to download automatically and schedule installation on firewalls as soon as possible. [Applications and Threats content updates](#) occur whenever Security profile signatures need updating. The content updates sent on the third Tuesday of each month also contain new and modified App-IDs (application updates; in rare cases, an application update might be delayed one or two days). Evaluate how new and modified App-IDs affect your Security policy rulebase in a non-production environment and modify rules as needed.

Follow [content update best practices](#), install updates as soon as you can to protect your internet gateway, and configure [Log Forwarding](#) for all content updates.

- STEP 1 |** Before installing a new content update, [review new and modified App-IDs](#) to determine if the changes impact policy.
- STEP 2 |** If necessary, modify existing [Security policy](#) rules to accommodate the App-ID changes. You can [disable selected App-IDs](#) if some App-IDs require more testing and install the rest of the new and modified App-IDs. Finish testing and any necessary policy revisions before the next monthly content release with new App-IDs arrives (third Tuesday of each month) to avoid overlap.
- STEP 3 |** [Prepare policy updates](#) to account for App-ID changes included in a content release, to add new sanctioned applications, to or remove applications from your allow rules.

