paloalto TECHDOCS

Internet Gateway Best Practice Security Policy

Version 9.0 (EoL)

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support.html

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.

Last Revised

March 14, 2022

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 Whitelist Applications 12
Map Applications to Business Goals for a Simplified Rulebase 12
Use Temporary Rules to Tune the Whitelist 13
Application Whitelist Example 13
Create User Groups for Access to Whitelist Applications 16
Decrypt Traffic for Full Visibility and Threat Inspection 17
Transition Safely to Best Practice Security Profiles 19
Transition Vulnerability Protection Profiles Safely to Best Practices 20
Transition Anti-Spyware Profiles Safely to Best Practices 21
Transition Antivirus Profiles Safely to Best Practices 23
Transition WildFire Profiles Safely to Best Practices 23
Transition URL Filtering Profiles Safely to Best Practices 24
Transition File Blocking Profiles Safely to Best Practices 24
Create Best Practice Security Profiles for the Internet Gateway 26
Best Practice Internet Gateway File Blocking Profile 26
Best Practice Internet Gateway Antivirus Profile 27
Best Practice Internet Gateway Vulnerability Protection Profile 28
Best Practice Internet Gateway Anti-Spyware Profile 29
Best Practice Internet Gateway URL Filtering Profile 31
Best Practice Internet Gateway WildFire Analysis Profile 34
Define the Initial Internet Gateway Security Policy 36
Step 1: Create Rules Based on Trusted Threat Intelligence Sources 36
Step 2: Create the Application Whitelist Rules 39
Step 3: Create the Application Block Rules 43
Step 4: Create the Temporary Tuning Rules 45
Step 5: Enable Logging for Traffic that Doesn't Match Any Rules 47
Monitor and Fine Tune the Policy Rulebase 49
Remove the Temporary Rules 51
Maintain the Rulebase 52

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 take hold in your network and begin to move laterally towards the end goal, whether that is to steal your source code, exfiltrate your customer data, or take down your infrastructure. To protect your network from cyberattack 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 classifying all traffic, across all ports, all the time.

The following topics describe the overall process for deploying a best practice internet gateway security policy and provide detailed instructions for creating it.

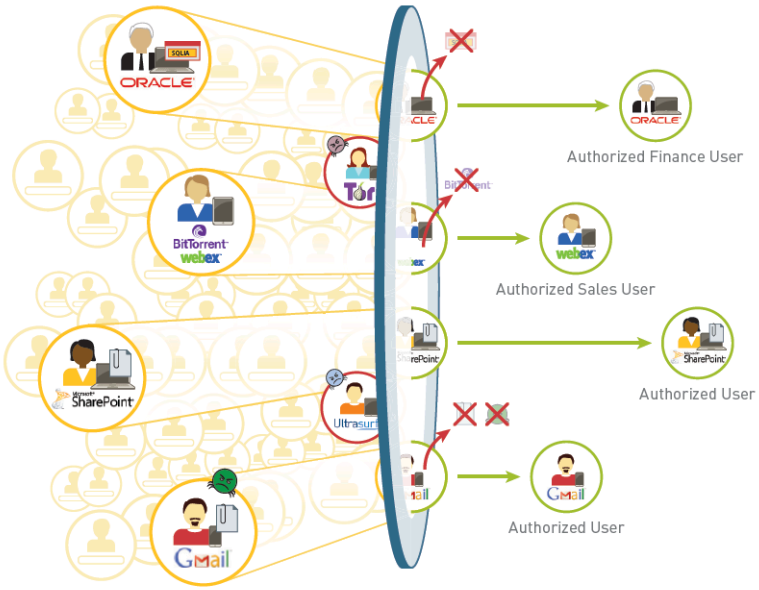
- What Is a Best Practice Internet Gateway Security Policy?
- Why Do I Need a Best Practice Internet Gateway Security Policy?
- How Do I Deploy a Best Practice Internet Gateway Security Policy?
- Identify Whitelist Applications
- Create User Groups for Access to Whitelist Applications
- Decrypt Traffic 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

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, and Content-ID 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, the best practice internet gateway security policy uses application-based rules to allow access to whitelisted applications by user, while scanning all traffic to detect and block all known threats, and send unknown files to WildFire to identify new threats and generate signatures to block them:



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

Best Practice Methodology	Why is this important?
Inspect All Traffic for Visibility	Because you cannot protect against threats you cannot see, you must make sure you have full visibility into all traffic across all users and applications all the time. To accomplish this:

Best Practice Methodology	Why is this important?
	• Deploy GlobalProtect to extend the next-generation security platform to users and devices no matter where they are located. • Enable SSL decryption so the firewall can inspect encrypted traffic (Gartner predicts that through 2019, more than 80% of enterprise web traffic will be encrypted and more than 50% of new malware campaigns will use various forms of encryption). • Enable User-ID to map application traffic and associated threats to users/devices. • If company policy allows users' devices on the network (BYOD or corporate devices without GlobalProtect or other management applications installed), the unsanctioned device access control service enables users to access your cloud applications from personal devices, from any location, without inadvertently putting your data or organization at risk. The service redirects traffic through the firewall for policy enforcement and threat prevention. The firewall can then inspect all traffic—inclusive of applications, threats, and content—and tie it to the user, regardless of location or device type, port, encryption, or evasive techniques employed using the native App-ID, Content-ID, and User-ID technologies. Complete visibility into the applications, the content, and the users on your network is the first step toward informed policy control.
Reduce the Attack Surface	After you have context into the traffic on your network—applications, their associated content, and the users who are accessing them—create application-based Security policy rules to allow those applications that are critical to your business and additional rules to block all high-risk applications that have no legitimate use case. To further reduce your attack surface, enable attach File Blocking and URL Filtering profiles to all rules that allow application traffic to prevent users from visiting threat-prone web sites and prevent them from uploading or downloading dangerous file types (either knowingly or unknowingly). To prevent attackers from executing successful phishing attacks (the cheapest and easiest way for them to make their way into your network), configure credential phishing prevention.
Prevent Known Threats	Enable the firewall to scan all allowed traffic for known threats by attaching security profiles to all allow rules to detect and block network and application layer vulnerability exploits, buffer overflows, DoS attacks, and port scans, known malware variants, (including those hidden within compressed files or compressed

Best Practice Methodology	Why is this important?
	HTTP/HTTPS traffic). To enable inspection of encrypted traffic, enable SSL decryption. 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.
Detect Unknown Threats	Forward all unknown files to WildFire for analysis. WildFire identifies unknown or targeted malware (also called *advanced persistent threats* or *APTs*) hidden within files by directly observing and executing unknown files in a virtualized sandbox environment in the cloud or on the WildFire appliance. WildFire monitors more than 250 malicious behaviors and, if it finds malware, it automatically develops a signature and delivers it to you in as little as five minutes (and now that unknown threat is a known threat).

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

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 allows you to safely enable applications by classifying all traffic, across all ports, all the time, including encrypted traffic. By determining the business use case for each application, you can create security policy rules to allow and protect access to relevant applications. Simply put, a best practice security policy is a policy that leverages the next-generation technologies—App-ID, Content-ID, and User-ID—on the Palo Alto Networks enterprise security platform to:

- Identify applications regardless of port, protocol, evasive tactic or encryption
- Identify and control users regardless of IP address, location, or device
- Protect against known and unknown application-borne threats
- Provide fine-grained visibility and policy control over application access and functionality

A best practice security policy uses a layered approach to ensure that you not only safely enable sanctioned applications, but also block applications with no legitimate use case. To mitigate the risk of breaking applications when moving from a port-based enforcement to an application-based enforcement, the best-practice rulebase provides built-in mechanisms to help you identify gaps in the rulebase and detect alarming activity and potential threats on your network. These temporary best practice rules ensure that applications your users are counting on don't break, while allowing you to monitor application usage and craft appropriate rules. You may find that some of the applications that were being allowed through existing port-based policy rules are not necessarily applications that you want to continue to allow or that you want to limit to a more granular set of users.

Unlike a port-based policy, a best-practice security policy is easy to administer and maintain because each rule meets a specific goal of allowing an application or group of applications to a specific user group based on your business needs. Therefore, you can easily understand what traffic the rule enforces by looking at the match criteria. Additionally, a best-practice security policy rulebase leverages tags and objects to make the rulebase more scannable and easier to keep synchronized with your changing environment.

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

Moving from a port-based security policy to an application-based security policy may seem like a daunting task. However, the security risks of sticking with a port-based policy far outweigh the effort required to implement an application-based policy. And, while legacy port-based security policies may have hundreds, if not thousands of rules (many of which nobody in the organization knows the purpose), a best practice policy has a streamlined set of rules that align with your business goals, simplifying administration and reducing the chance of error. Because the rules in an application-based policy align with your business goals and acceptable use policies, you can quickly scan the policy to understand the reason for each and every rule.

As with any technology, there is usually a gradual approach to a complete implementation, consisting of carefully planned deployment phases to make the transition as smooth as possible, with minimal impact to your 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 and identify what your most valuable assets are as well as what the biggest threats to those assets are. For example, if you are a technology company, your intellectual property is your most valuable asset. In this case, one of your biggest threats would be source code theft.
- Segment Your Network Using Interfaces and Zones—Traffic cannot flow between zones unless there is a security policy rule to allow it. One of the easiest defenses against lateral movement of an attacker that has made its way into your network is to define granular zones and only allow access to the specific user groups who need to access an application or resource in each zone. By segmenting your network into granular zones, you can prevent an attacker from establishing a communication channel within your network (either via malware or by exploiting legitimate applications), thereby reducing the likelihood of a successful attack on your network.
- Identify Whitelist Applications—Before you can create an internet gateway best practice security policy, you must have an inventory of the applications you want to allow on your network, and distinguish between those applications you administer and officially sanction and those that you simply want users to be able to use safely. After you identify the applications (including general types of applications) you want to allow, you can map them to specific best practice rules.
- Create User Groups for Access to Whitelist Applications—After you identify the applications you plan to allow, you must identify the user groups that require access to each one. Because compromising an end user's system is one of the cheapest and easiest ways for an attacker to gain access to your network, you can greatly reduce your attack surface by only allowing access to applications to the user groups that have a legitimate business need.
- Decrypt Traffic for Full Visibility and Threat Inspection—You can't inspect traffic for threats if you can't see it. And today SSL/TLS traffic flows account for 40% or more of the total traffic on a typical network. This is precisely why 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 SSL encryption, to email an exploit or malware to employees accessing that application on the corporate network. Or, an attacker may compromise a web site that uses SSL encryption

to silently download an exploit or malware to site visitors. If you are not decrypting traffic for visibility and threat inspection, you are leaving a very large surface open for attack.

- Create Best Practice Security Profiles for the Internet Gateway—Command and control traffic, CVEs, drive-by downloads of malicious content, phishing attacks, APTs are all delivered via legitimate applications. To protect against known and unknown threats, you must attach stringent security profiles to all Security policy allow rules.
- Define the Initial Internet Gateway Security Policy—Using the application and user group inventory you conducted, you can define an initial policy that allows access to all of the applications you want to whitelist by user or user group. The initial policy rulebase you create must also include rules for blocking known malicious IP addresses, as well as temporary rules to prevent other applications you might not have known about from breaking and to identify policy gaps and security holes in your existing design.
- Monitor and Fine Tune the Policy Rulebase—After the temporary rules are in place, you can begin monitoring 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, you can 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 whitelist and adapt your rules to accommodate new applications that you decide to sanction as well to determine how new or modified App-IDs impact your 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 sanctioned application or new or modified App-ID oftentimes is as simple as adding or removing an application from an application group or modifying an application filter.

Identify Whitelist Applications

The application whitelist includes not only the applications you provision and administer for business and infrastructure purposes, but also other applications that your users may need to use in order to get their jobs done, and applications you may choose to allow for personal use. Before you can begin creating your best practice internet gateway security policy, you must create an inventory of the applications you want to whitelist.

- Map Applications to Business Goals for a Simplified Rulebase
- Use Temporary Rules to Tune the Whitelist
- Application Whitelist 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 will allow you to create a goal-driven rulebase. For example, one goal might be to allow all users on your network to access data center applications. Another goal might be to allow the sales and support groups access your customer database. You can then create a whitelist rule that correspond to each goal you identify and group all of the applications that align with the goal into a single rule. This approach allows you to create a rulebase with a smaller number of individual rules, each with a clear purpose.

In addition, because the individual rules you create align with your business goals, you can use application objects to group the whitelist to further simplify administration of the best practice rulebase:

- Create application groups for sanctioned applications for each set of sanctioned applications—Because you know exactly which applications you require and sanction for official use, create application groups that explicitly include only those applications. Using application groups also simplifies the administration of your policy because it allows you to add and remove sanctioned applications without requiring you to modify individual policy rules. Generally, if the applications that map to the same goal have the same requirements for enabling access (for example, they all have a destination address that points to your data center address group, they all allow access to any known user, and you want to enable them on their default ports only) you would 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 application filters to allow each type of general application—Besides the applications you officially sanctioned, you will also need to decide what additional applications you want to allow your users to access. Application filters allow you to safely enable certain categories of applications using application filters (based on category, subcategory, technology, risk factor, or characteristic). Separate the 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 at a glance.

Use Temporary Rules to Tune the Whitelist

Although the end-goal of a best-practice application-based policy is to use positive enforcement to safely enable your whitelist applications, the initial rulebase requires some additional rules designed to ensure that you have full visibility into all applications in use on your network so that you can properly tune it. The initial rulebase you create will have the following types of rules:

- Whitelist rules for the applications you officially sanction and deploy.
- Whitelist rules for safely enabling access to general types of applications you want to allow per your acceptable use policy.
- Blacklist rules that block applications that have no legitimate use case. You need these rules so that the temporary rules that "catch" applications that haven't yet been accounted for in your policy don't let anything bad onto your network.
- Temporary allow rules to give you visibility into all of the applications running on your network so that you can tune the rulebase.

The temporary rules are a very important part of the initial best practice rulebase. Not only will they give you visibility into applications you weren't aware were running on your network (and prevent legitimate applications you didn't know about from breaking), but they will also help you identify things such as unknown users and applications running on non-standard ports. Because attackers commonly use standard applications on non-standard ports as an evasion technique, allowing applications on any port opens the door for malicious content. Therefore, you must identify any legitimate applications running on non-standard ports (for example, internally developed applications) so that you can either modify what ports are used or create custom applications to enable them.

If you have existing Application Override policies that you created solely to define custom session timeouts for a set a 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 and then migrating the rule the an application-based rule. Application Override policies are port-based. When you use Application Override policies to maintain custom session timeouts for a set of ports, you lose application visibility into those flows, so you neither know nor control which applications use the ports. Service-based session timeouts achieve custom timeouts while also maintaining application visibility.

Application Whitelist Example

Keep in mind that you do not need to capture every application that might be in use on your network in your initial inventory. Instead you should focus on the applications (and general types of applications) that you want to allow. Temporary rules in the best practice rulebase will catch any additional applications that may be in use on your network so that you are not inundated with complaints of broken applications during your transition to application-based policy. The following is an example application whitelist for an enterprise gateway deployment.

Application Type	Best Practice for Securing
SaaS Applications	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. Generate a SaaS applications 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: • 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.

Sanctioned Applications	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:
	
	• **Infrastructure Applications**—These are the applications that you must allow to enable networking and security, such as ping, NTP, SMTP, and DNS.
	• **IT Sanctioned Applications**—These are the applications that you provision and administer for your users. These fall into two categories:
	  • **IT Sanctioned On-Premise Applications**—These are the 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**—These are SaaS applications that your IT department has sanctioned for business purposes, for example, Salesforce, Box, and GitHub.
	• **Administrative Applications**—These are 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).
	
	Tag all sanctioned applications with the predefined *Sanctioned* tag. Panorama and firewalls consider applications without the Sanctioned tag as unsanctioned applications.

Application Type	Best Practice for Securing
General Types of Applications	Besides the applications you officially sanction and deploy, you will also want to allow your users to safely use other types of applications: • **General Business Applications**—For example, allow access to software updates, and web services, such as WebEx, Adobe online services, and Evernote. • **Personal Applications**—For example, you may want to allow your users to browse the web or safely use web-based mail, instant messaging, or social networking applications, including consumer versions of some SaaS applications. Begin with wide application filters to gain an understanding of what applications are in use on your network. You can then decide how much risk you are willing to assume and begin to pare down the application whitelist. For example, suppose multiple messaging applications are in use, each with the inherent risk of data leakage, transfer of malware-infected files, etc. The best approach is to officially sanction a single messaging application and then begin to phase out the others by slowly transitioning from an allow policy to an alert policy, and finally, after giving users ample warning, a block policy for all messaging applications except the one you choose to sanction. In this case, you might also choose to enable a small group of users to continue using an additional messaging application as needed to perform job functions with partners.
Custom Applications Specific to Your Environment	If you have proprietary applications on your network or applications that you run on non-standard ports, it is a best practice to create custom applications for each of them. This way you can allow the application as a sanctioned application (and apply the predefined Sanctioned tag) and lock it down to its default port. Otherwise you would 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. If you have existing Application Override policies that you created solely to define custom session timeouts for a set a 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 and then migrating the rule the an application-based rule. Application Override policies are port-based. When you use Application Override policies to maintain custom session timeouts for a set of ports, you lose application visibility into those flows, so you neither know nor control which applications use the ports. Service-based session timeouts achieve custom timeouts while also maintaining application visibility.

Create User Groups for Access to Whitelist Applications

Safely enabling applications means not only defining the list of applications you want to allow, but also enabling access only for those 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 you can reduce your attack surface by ensuring that only users who need these applications can access them. For example, while IT support personnel may legitimately need access to remote desktop applications, the majority of your users do not. Limiting user access to applications prevents potential security holes for an attacker to gain access to 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 whitelist rule you define, identify the user groups that have a legitimate business need for the applications allowed by the rule. Keep in mind that because the best practice approach is to map the application whitelist rules to your business goals (which includes considering which users have a business need for a particular type of application), you will have a much smaller number of rules to manage than if you were trying to map individual port-based rules to users.
- If you don't have an existing group on your AD server, you can alternatively create custom LDAP groups to match the list of users who need access to a particular application.
- It just takes one end user to click on a phishing link and supply their credentials to enable an attacker to gain access to your network. To defend against this very 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-basedUser-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

The best practice security policy dictates that you decrypt all traffic except sensitive categories, which include Health, Finance, Government, and traffic that you don't decrypt for business, legal, or regulatory reasons.

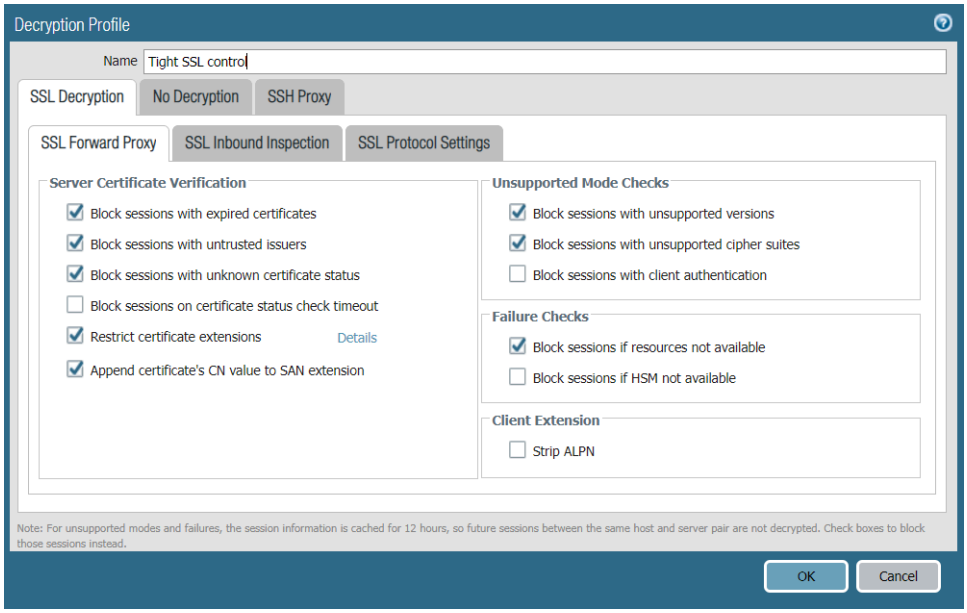
Use decryption exceptions only where required, and be precise to ensure that you are limiting the exception to a specific application or user based on need only:

- 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 a specific user needs to be excluded for regulatory or legal reasons, create an exception for just that user.

To ensure that certificates presented during SSL decryption are valid, configure the firewall to perform CRL/OCSP checks.

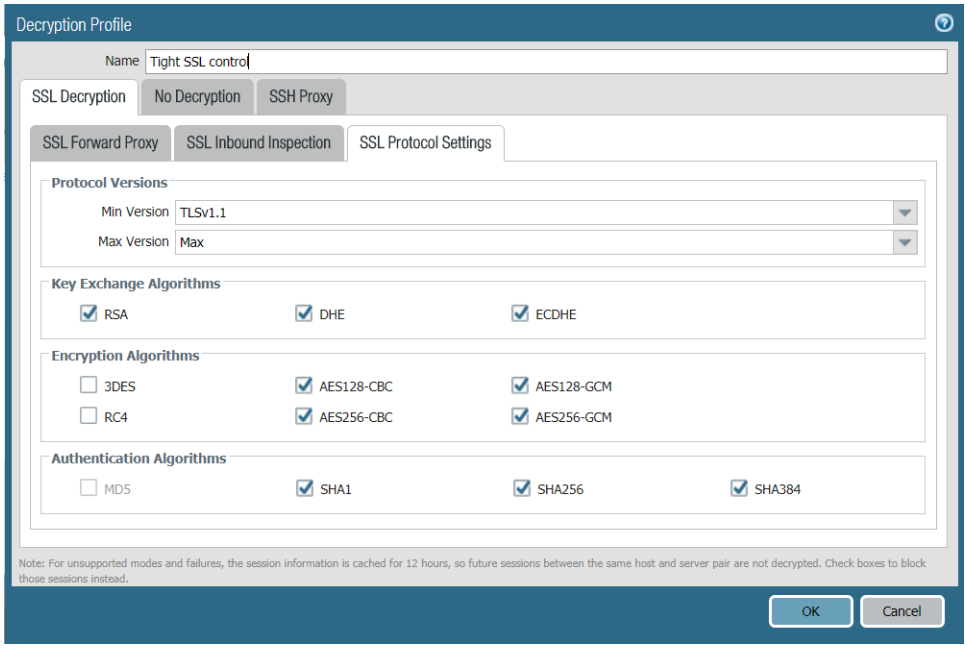
Best practice Decryption policy rules include a strict Decryption Profile. Before you configure SSL Forward Proxy, create a best practice Decryption Profile (**Objects** > **Decryption Profile**) to attach to your Decryption policy rules:

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



Block sessions if resources not available prevents allowing potentially dangerous connections but may affect the user experience.

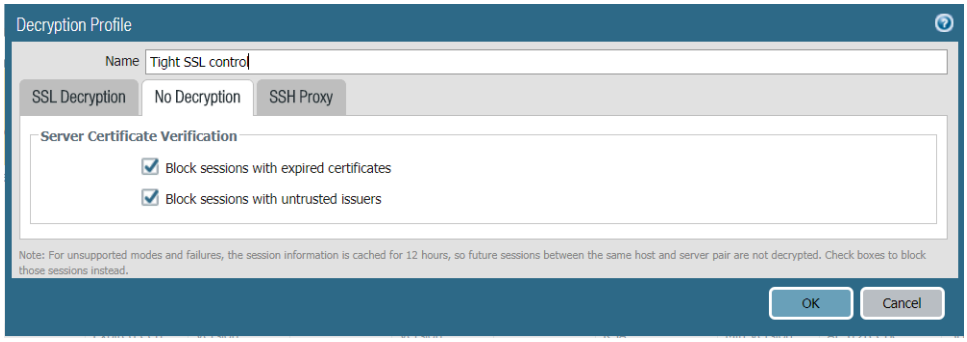
STEP 2 | Configure the **SSL Decryption** > **SSL Protocol Settings** to block use of vulnerable SSL/TLS versions (TLS 1.0 and SSLv3) and to avoid weak algorithms (MD5, RC4, and 3DES):



Some sites still use the TLSv1.1 protocol, but TLSv1.2 is more secure. Review the sites you need to access for business purposes. If most of them use TLSv1.2, then create separate Decryption policies and a separate Decryption profile for sites that use TLSv1.1 so that only the sites you legitimately need for business purposes can access your network using TLSv1.1.

The same is true about the SHA1 authentication algorithm—if you can use the more security SHA256 or greater algorithm, do it. If only a few sites that you need for business purposes use SHA1, create separate Decryption policies and a separate Decryption profile for them.

STEP 3 | For traffic that you are not decrypting, configure the **No Decryption** settings to block encrypted sessions to sites with expired certificates or untrusted issuers:



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 even unknown threats, and prevent them from compromising your network using various types of threat signatures (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 may 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. Run a Best Practice Assessment (BPA) on your configuration.
2. Review the Adoption Summary in the BPA results to see the current state of your Security profile adoption.
3. Identify gaps in adoption in the BPA results.
4. Review your Security profile configuration in the BPA results to see the best practice check results for each profile.
5. 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 may be able to duplicate those profile settings, including block actions you already deem to be 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 may prefer to alert first and examine the traffic that causes the alerts before blocking to ensure the profile won't block critical applications.
3. Am I deploying Security profiles to counter an immediate threat? If the answer is yes, you may 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 may 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 the attack threshold is set 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

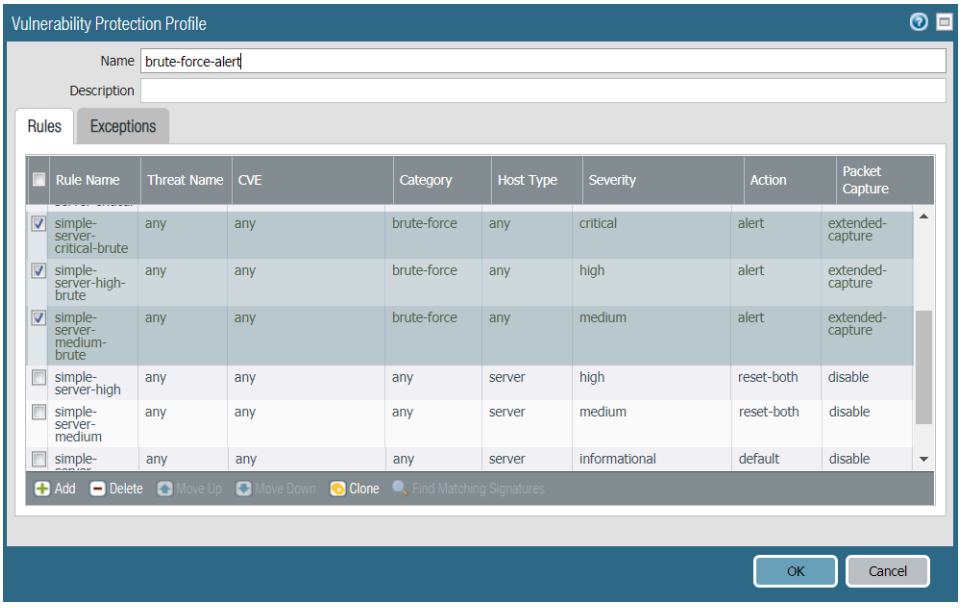
- Transition Anti-Spyware Profiles Safely to Best Practices
- Transition Antivirus Profiles Safely to Best Practices
- Transition WildFire Profiles Safely to Best Practices
- Transition URL Filtering Profiles Safely to Best Practices
- Transition File Blocking Profiles Safely to Best Practices

Transition Vulnerability Protection Profiles Safely to Best Practices

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

Vulnerability Protection requires a Threat Prevention subscription.

- 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 critical and high severity signatures from the start.
- Medium severity signatures may 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 can block applications for which you receive alerts or if you need to allow them.
- Set signatures in the brute-force category initially to alert and then fine-tune them to your environment before transitioning to blocking them.



- 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 default action from the start.

- For business-critical applications, it's usually best to 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 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.

  The alert action enables you to analyze Threat logs and create exceptions when necessary before moving to a block action. Alerting and monitoring before moving to blocking gives you confidence the profile won't block business-critical applications when you deploy the initial profile and that you'll maintain application availability by creating necessary exceptions as you transition to the best practice blocking state. 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 best practice state as soon as you're comfortable you've identified any exceptions you need to make and configure the profile accordingly.

Enable extended packet capture for critical, high, and medium severity signatures. Enable single packet capture for low and informational severity signatures. Enabling packet capture allows 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 particularly useful, you can transition to disabling packet capture on informational events.

When you have the initial profiles in place, monitor the Threat logs for enough time to gain confidence 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 any confirmed false positives before you implement full best-practice Vulnerability Protection profiles for the internet gateway or for the data center.

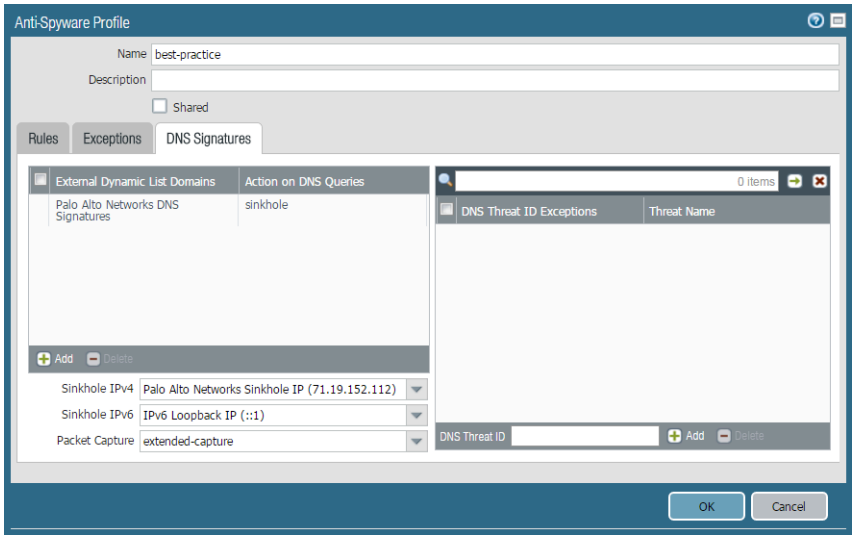
Transition Anti-Spyware Profiles Safely to Best Practices

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

Anti-Spyware requires a Threat Prevention subscription.

- False positive rates for critical and high severity signatures are typically low. For applications that aren't critical to your business, such as internet access, block critical and high severity signatures from the start.
- Medium severity signatures may 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 can block applications for which you receive alerts or if you need to allow them.
- Set the action for DNS signatures to sinkhole to identify potentially compromised hosts that attempt to access suspicious domains by tracking the hosts and preventing them from

accessing those domains. (This is the best practice configuration and you should configure DNS sinkhole right away.)



- 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 default action from the start.
- For business-critical applications, it's usually best to 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 similar 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 the similar 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 moving to blocking gives you confidence the profile won't block business-critical applications when you deploy the initial profile and that you'll maintain application availability by creating necessary exceptions as you transition to the best practice blocking state. 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 best practice state as soon as you're comfortable you've identified any exceptions you need to make and configure the profile accordingly.

Enable single packet capture for all severity signatures. 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 particularly useful, you can transition to disabling packet capture on these severities.

When you have the initial profiles in place, monitor the Threat logs for enough time to gain confidence 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 any confirmed false positives before you implement full best-practice Anti-Spyware profiles for the internet gateway or for the data center.

Transition Antivirus Profiles Safely to Best Practices

Use the following guidance to help determine whether to start with block or alert actions as you define the initial Antivirus profiles and begin the transition to best practice profiles.

Antivirus requires a Threat Prevention subscription.

- It's safe to deploy the best practice Antivirus profiles for applications that aren't critical to your business right away because false positive rates are rare.
- For business-critical applications, it's usually best to 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.

  *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 the profile won't block business-critical applications when you deploy the initial profile and that you'll maintain application availability by creating necessary exceptions as you transition to the best practice blocking state. 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 best practice state as soon as you're comfortable you've identified any exceptions you need to make and configure the profile accordingly.*
- WildFire Action settings in the Antivirus profile may 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 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 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 for the internet gateway or for the data center.

Transition WildFire Profiles Safely to Best Practices

Use the following guidance to help define the initial configuration of WildFire Analysis profiles.

PAN-OS includes basic WildFire service, which enables forwarding portable executable (PE) files for WildFire analysis and retrieving WildFire signatures with antivirus or Threat Prevention updates every 24-48 hours. A WildFire subscription includes many more features, such as receiving updates every five minutes, support for more file types, and an API.

- WildFire signature generation is highly accurate and false positives are rare. Deploying the best practice WildFire Analysis profile from the start does not impact network traffic. However, WildFire Action settings in the Antivirus profile may impact traffic if the traffic generates a WildFire signature that results in a reset or drop action.

- Exclude internal traffic such as software distribution applications if you deploy custom-built programs through these applications because WildFire may identify custom-built programs as malicious and generate a signature for them.

The default WildFire Analysis profile is the recommended best practice profile, including at the internet gateway and in the data center.

When you have the initial profiles in place, monitor the WildFire Submissions logs (**Monitor** > **Logs** > **WildFire Submissions**) for enough time to gain confidence 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

Use the following guidance to help 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).

URL Filtering requires a subscription to the PAN-DB URL filtering database.

- The pre-defined URL categories are very 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 sites.
- Block known-bad URL categories from the start, including malware, command-and-control, copyright-infringement, extremism, phishing, and proxy-avoidance-and-anonymizers.
- For the URL categories dynamic-dns (these sites are often used to deliver malware payloads or command-and-control traffic), 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), it's best to 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.
- Configure the security-focused high-risk and medium-risk based URL categories to alert (this is the default action). Monitor the URL Filtering logs to see if you want to allow access to the sites these categories control, if you want to block these categories completely, or if you want to allow access to some sites and block the rest.

When you have the initial profiles in place, monitor the URL Filtering logs for enough time to gain confidence you understand whether any business-critical sites will be blocked if you transition from alerting to blocking and to best practice 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.

Transition File Blocking Profiles Safely to Best Practices

Use the following guidance to help 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.

- The best practice File Blocking profile will likely be different for different types of applications and for different areas of the network. For example:
  - If internal applications depend on file type transfers that the best practice File Blocking profile recommends blocking, you need to allow those file types for those internal applications. Don't allow those file transfer types for all applications, allow them only for the necessary internal applications.
  - For internet-based traffic, take a more restrictive approach from the start to prevent attackers from delivering malicious files and to reduce the attack surface.
  - For data center traffic, take a more restrictive approach (with the exception of internal applications that depend on file transfer types that you would otherwise block) to reduce the attack surface and protect your most valuable assets.
- For business-critical applications, start off with the alert action for all file types.

Monitor the Data Filtering logs (**Monitor** > **Logs** > **Data Filtering**) to understand the file type usage before configuring block actions for specific file types. As you understand which file types your business-critical and internal custom applications require, transition toward the best practice File Blocking configuration for the internet gateway or the data center, 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. Therefore, to safely enable applications you must scan all traffic allowed into the network for threats. To do this, 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 are the recommended best practice settings for each of the security profiles that you should attach to every Security policy rule on your internet gateway policy rulebase.

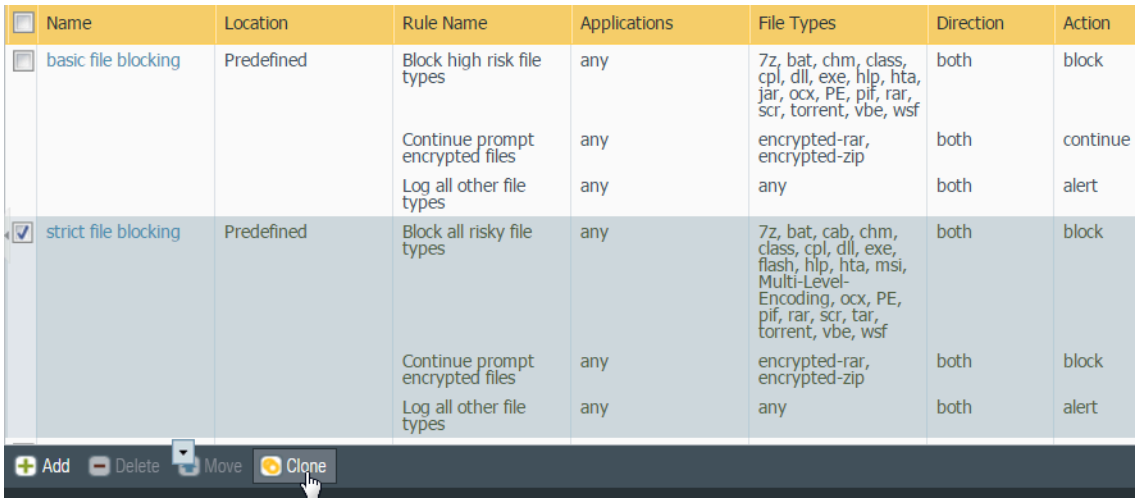
Consider adding the best practice security profiles to a default security profile group so that it will automatically attach to any new Security policy rules you create.

- 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 files that are commonly included in malware attack campaigns and that have no real use case for upload/download. Blocking these files 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, multi-level 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 may 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, if necessary, 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.*



Why do I need this profile?

There are many ways for attackers to deliver malicious files: as attachments or links in corporate email or in webmail, links or IMs in social media, Exploit Kits, through file sharing applications (such as FTP, Google Drive, or Dropbox), or on USB drives. Attaching the strict file blocking profile reduces your attack surface by preventing these types of attacks.

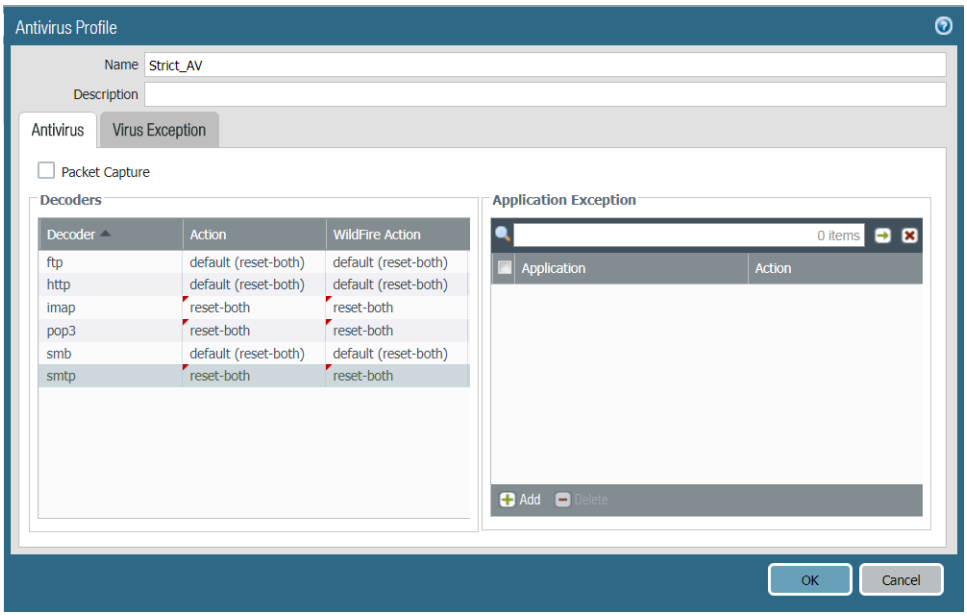
What if I can't block all of the file types covered in the predefined strict profile?

If you have mission-critical applications that prevent you from blocking all of the file types included in the predefined strict profile, you can clone the profile and modify it for those users who must transfer a file type covered by the predefined profile. If you choose not to block all PE files per the recommendation, make sure you send all unknown files to WildFire for analysis. Additionally, 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 knowing they are doing it. Drive-by downloads can occur when users visit web sites, view email messages, or click into pop-up windows meant to deceive them. Educate your users that if they are prompted to continue with a file transfer they didn't knowingly initiate, they may be subject to a malicious download. In addition, using file blocking in conjunction with URL filtering to limit the categories in which users can transfer files is another good way to reduce the attack surface when you find it necessary to allow file types that may carry threats.

Best Practice Internet Gateway Antivirus Profile

Clone the default Antivirus profile and edit it. 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 the best practice profile. To achieve the best practice profile, modify the default profile as shown here and attach it to all security policy rules that allow traffic. The Antivirus profile has decoders that detect and prevent viruses and malware from being transferred over six protocols: HTTP, SMTP, IMAP, POP3, FTP, and SMB. You can set WildFire actions for all six protocols because the Antivirus profile also enforces actions based on WildFire signatures.

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

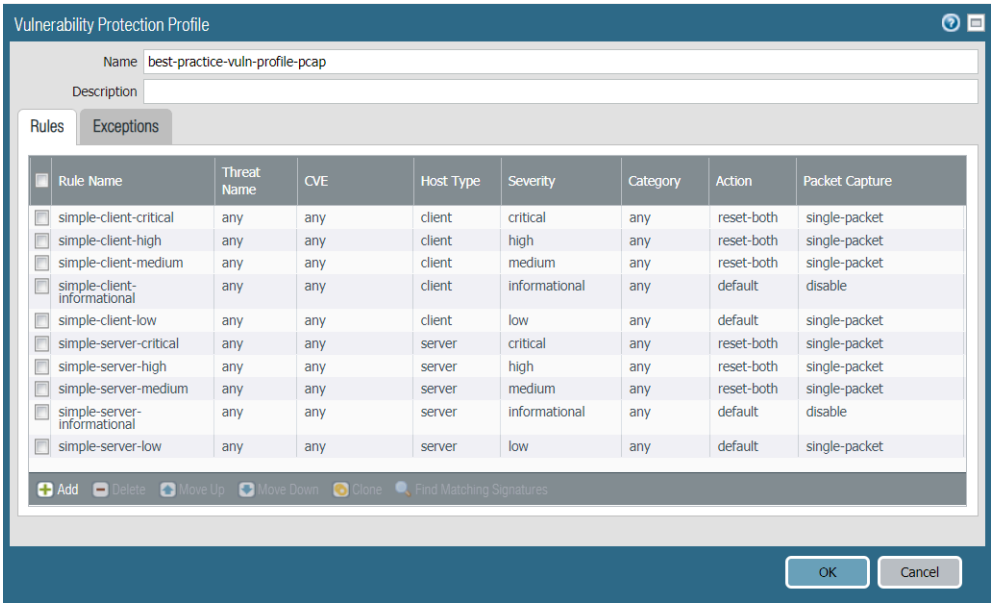


Why do I need this profile?

By attaching Antivirus profiles to all Security rules you can block known malicious files (malware, ransomware bots, and viruses) as they are coming into the network. Common ways for users to receive malicious files include malicious attachments in email, links to download malicious files, or 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. Clone the predefined strict Vulnerability Protection profile. 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. For the best practice profile, for each rule except **simple-client-informational** and **simple-server-informational**, double-click the **Rule Name** and change **Packet Capture** from **disable** to **single-packet** to enable packet capture (PCAP) for each rule so you can track down the source of potential attacks. Don't change the rest of the settings. Download content updates automatically and install them as soon as possible so that the signature set is always up-to-date.



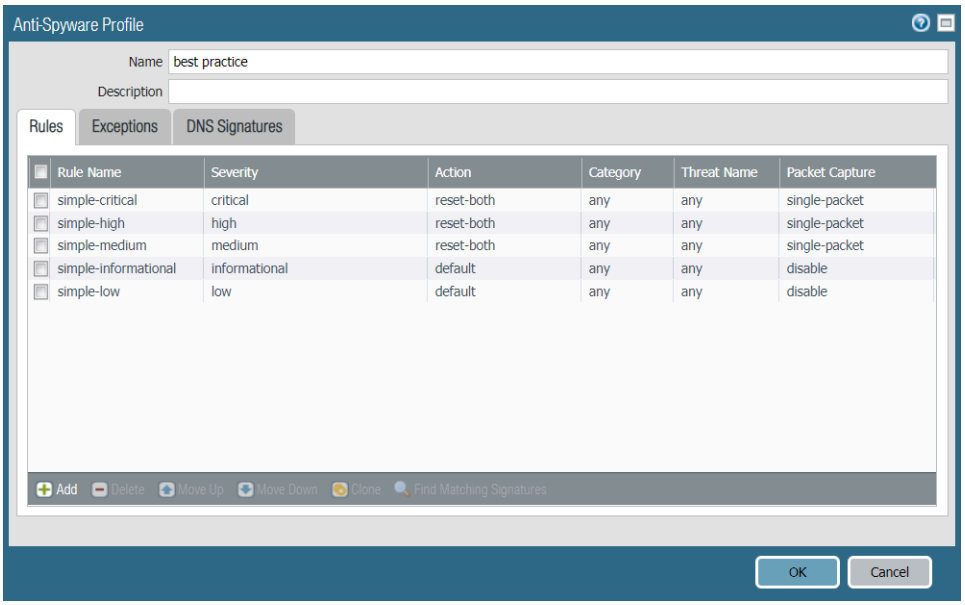
Why do I need this profile?

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 (Angler, Nuclear, Fiesta, KaiXin) to automatically deliver malicious payloads to the end user. Vulnerability Protection profiles also prevent an attacker from using vulnerabilities on internal hosts to move laterally within your network.

Don't enable PCAP for informational activity because it generates a relatively high volume of that traffic and it's not particularly useful compared to potential threats. Apply extended PCAP (as opposed to 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—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 the threat. If too much PCAP traffic is sent to the management plane, then capturing more than five packets may result in dropping PCAPs.

Best Practice Internet Gateway Anti-Spyware Profile

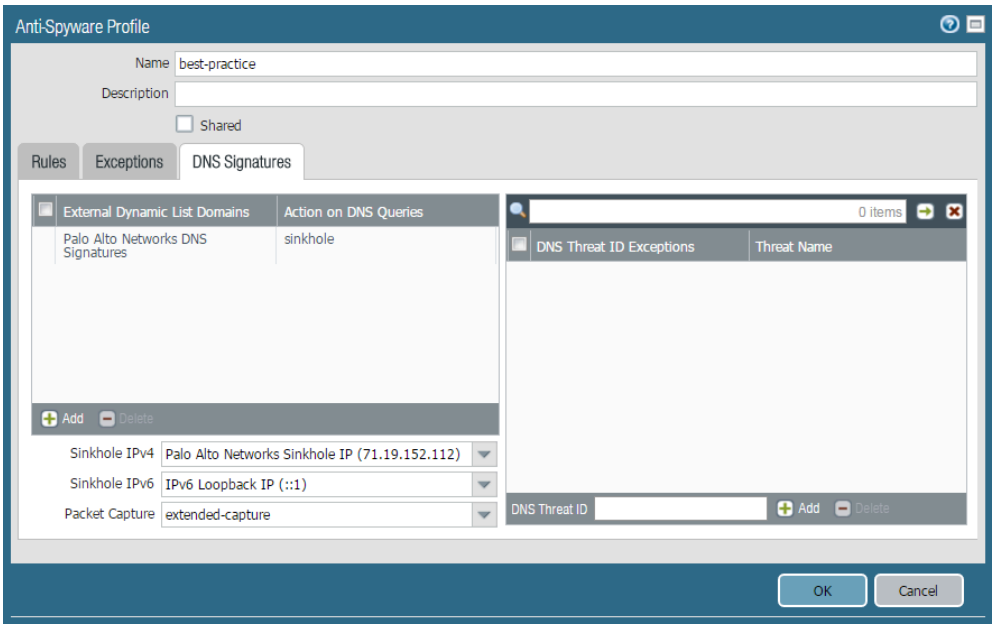
Attach an Anti-Spyware profile to all allowed traffic to detect command and control traffic (C2) initiated from malicious code running on a server or endpoint and prevent compromised systems from establishing an outbound connection from your network. Clone the predefined strict Anti-Spyware profile and edit it. To ensure availability for business-critical applications, follow the Transition Anti-Spyware Profiles Safely to Best Practices advice as you move from your current state to the best practice profile. Edit the profile to enable DNS sinkhole and packet capture to help you track down the endpoint that attempted to resolve the malicious domain. The best practice Anti-Spyware profile retains the default **Action** to reset the connection when the firewall detects a medium, high, or critical severity threat, and enables single packet capture (PCAP) for those threats.



Don't enable PCAP for informational activity because it generates a relatively high volume of that traffic and it's not particularly useful compared to potential threats. Apply extended PCAP (as opposed to 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—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 the threat. If too much PCAP traffic is sent to the management plane, then capturing more than five packets may result in dropping PCAPs.

The best practice **Action on DNS Queries** is to block or to sinkhole DNS queries for known malicious domains. It is also a best practice to enable PCAPs.

Enabling DNS sinkhole identifies potentially compromised hosts that attempt to access suspicious domains by tracking the hosts and preventing them from accessing those domains. Enable DNS sinkhole when the firewall can't see the originator of the DNS query (typically when the firewall is north of the local DNS server) so that you can identify infected hosts. Don't enable DNS sinkhole when the firewall can see the originator of the DNS query (typically when the firewall is south of the local DNS server; in this case, the firewall's blocking rules and logs provide visibility into the traffic) or on traffic you block.



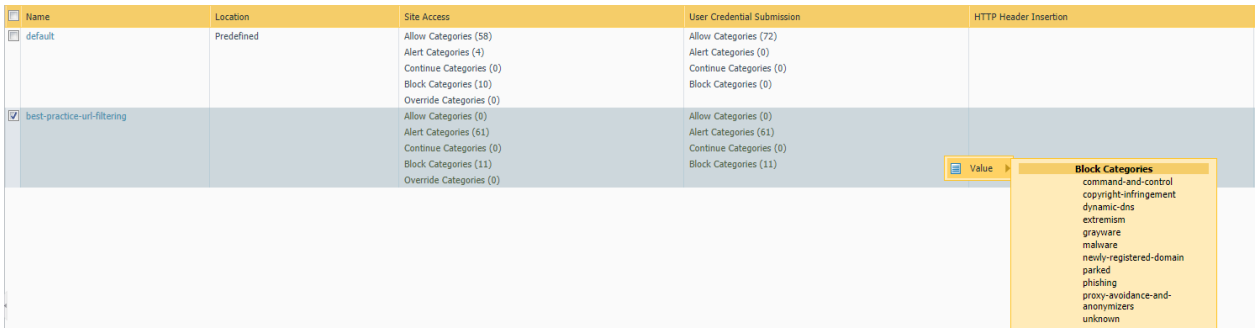
Best Practice Internet Gateway URL Filtering Profile

Use PAN-DB URL filtering to prevent access to web content high-risk for being malicious. 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 or exploitive content.

To ensure availability for business-critical applications, follow the Transition URL Filtering Profiles Safely to Best Practices advice as you move from your current state to the best practice profile. The best practice URL Filtering profile sets all known dangerous URL categories to block. These include command-and-control, copyright-infringement, dynamic-dns, extremism, malware, phishing, proxy-avoidance-and-anonymizers, unknown, newly-registered-domain, grayware, and parked. Failure to block these dangerous categories puts you at risk for exploit infiltration, malware download, command-and-control activity, and data exfiltration.

If you have a business purpose for a dynamic DNS domain, then make sure you whitelist those URLs in your URL Filtering profile.

In addition to blocking known bad categories, alert on all other categories so you have visibility into the sites your users are visiting. 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 may pose a threat. This paves the way for you to outright block the categories after a monitoring period.



If you are running PAN-OS 9.0.4 or later, ensure that the firewall handles user web requests as securely as possible by enabling the option to hold client requests (enter **`config`** then **`set deviceconfig setting ctd hold-client-request yes`**). 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. Maximize security by opting to hold requests during this lookup. For details, see Configure URL Filtering.

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

If users need access to sites in the blocked categories, consider creating an allow list for just the specific sites, if you feel the risk is justified. Be aware of local laws and regulations that govern the types of sites you can block, can't block, and must block. On categories you decide to allow, make sure you set up credential phishing prevention to ensure that users aren't submitting their corporate credentials to a site that may be hosting a phishing attack.

Allowing traffic to a recommended block category poses the following risks:

- **malware**—Sites known to host malware or used for command and control (C2) traffic. May also exhibit Exploit Kits.
- **phishing**—Known to host credential phishing pages or phishing for personal identification.
- **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 do not go through the same vetting process as domains that are registered by a reputable domain registration company, and are therefore less trustworthy.
- **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.
- **newly-registered-domain**—Newly registered domains are often generated purposely or by domain generation algorithms and used for malicious activity.
- **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.
- **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 may prohibit allowing access to extremist sites, and allowing access may pose a liability risk.
- **proxy-avoidance-and-anonymizers**—URLs and services often used to bypass content filtering products.
- **grayware**—Websites and services that do not meet the definition of a virus but are malicious or questionable and may 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.
- **parked**—Domains registered by individuals, oftentimes later found to be used for credential phishing. These domains may be similar to legitimate domains, for example, pal0alto0netw0rks.com, with the intent of phishing for credentials or personal identify information. Or, they may be domains that an individual purchases rights to in hopes that it may be valuable someday, such as panw.net.

The default URL Filtering profile blocks the malware, phishing, and command-and-control URL categories, but not the rest of the categories recommended to block as a best practice. The default URL Filtering profile also blocks the abused-drugs, adult, gambling, hacking, 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 may block some or 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 use the power of the Palo Alto Networks platform to implement policies that fit your business requirements. For example, you can:

- Use risk-based URL categories (high-risk, medium-risk, and low-risk) to simplify policy. If (after monitoring the traffic) you determine that you can block high-risk and/or medium-risk categories completely, you can quickly and simply tighten security. This enables you to control large numbers of potentially risky sites with one policy.
- Use risk-based URL categories to simplify decryption. If you determine that you can decrypt the sites in the high-risk and/or medium-risk categories, instead of creating decryption rules for many different applications, you can decrypt these risk categories in one simple rule.
- Log all user agents and referrers, all URLs, and all file downloads for high-risk and medium-risk category domains to increase visibility.

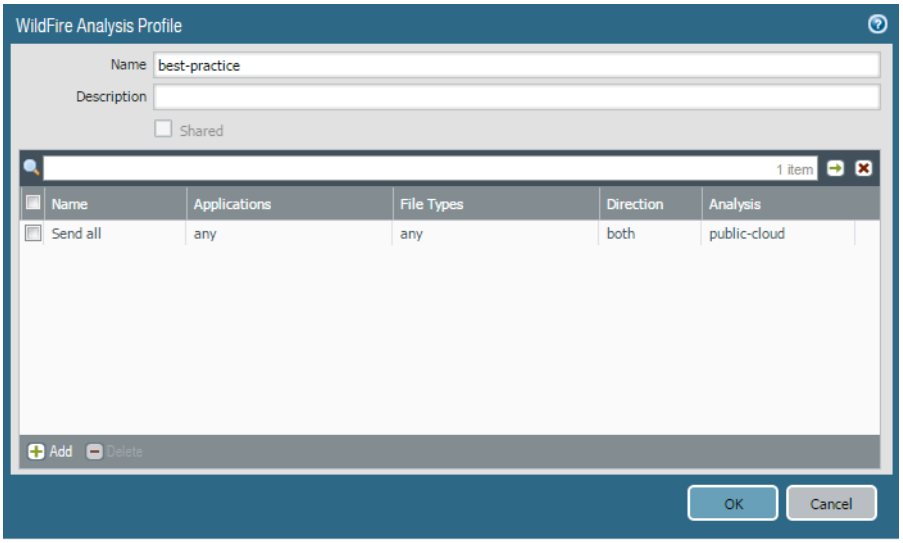
- Allow access to categories such as personal-sites-and-blogs while applying a File Blocking profile to the traffic to prevent downloading risky content such as .exe, .scr, and other potentially malicious files.
- If you can't block high-risk and/or medium-risk categories, apply a File Blocking profile to prevent downloading risky files.
- Allow all finance sites and use the predefined **Palo Alto Networks - Bulletproof IP addresses** EDL to prevent access to sites hosted on Bulletproof ISPs.
- Allow newly registered domains (if your business requires it) and automatically decrypt those sites and inspect the traffic. This method of applying decryption to entire categories works for any URL category you need to allow but that may pose risk.
- Use combinations of URL categories to simplify policy.

Best Practice Internet Gateway WildFire Analysis Profile

While the rest of the best practice security profiles significantly reduce the attack surface on your network by detecting and blocking known threats, the threat landscape is ever changing and the risk of unknown threats lurking in the files we use daily—PDFs, Microsoft Office documents (.doc and .xls files)—is ever growing. And, because these unknown threats are increasingly sophisticated and targeted, they often go undetected until long after a successful attack. To protect your network from unknown threats, you must configure the firewall to forward files to WildFire for analysis. Without this protection, attackers have free reign to infiltrate your network and exploit vulnerabilities in the applications your employees use everyday. Because WildFire protects against unknown threats, it is your greatest defense against advanced persistent threats (APTs).

Set up WildFire appliance content updates to download and install automatically every minute so that you always have the most recent support. For example, support for Linux and SMB files were first delivered in WildFire appliance content updates.

The best practice 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 per the file blocking best practice), Adobe Flash and Reader files (PDF, SWF), Microsoft Office files (PowerPoint, Excel, Word, RTF), Java files (Java, .CLASS), and Android files (.APK).



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 that 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 may 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, because WildFire may 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 overall goal of a best practice internet gateway security policy is to use positive enforcement of whitelist applications. However, it takes some time to identify exactly what applications are running on your network, which of these applications are critical to your business, and who the users are that need access to each one. The best way to accomplish the end goal of a policy rulebase that includes only application allow rules is to create an initial policy rulebase that liberally allows both the applications you officially provision for your users as well as other general business and, if appropriate, personal applications. This initial policy also includes additional rules that explicitly block known malicious IP addresses, bad applications as well as some temporary allow rules that are designed to help you refine your policy and prevent applications your users may need from breaking while you transition to the best practices.

To apply consistent security policy across multiple locations, you can reuse templates and template stacks so that the same policies apply to every internet gateway firewall at every location. The 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 and describe why each rule is necessary and what the risks are of not following the best practice recommendation:

- Step 1: Create Rules Based on Trusted Threat Intelligence Sources
- Step 2: Create the Application Whitelist 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

Before you allow and block traffic by application, block traffic from hosts that Palo Alto Networks and trusted third-party sources have proven to be malicious. With an active Threat Prevention license, Palo Alto Networks provides built-in external dynamic lists that contain these malicious IP addresses and that you can use in policy. The lists are compiled and dynamically updated based on the latest threat intelligence.

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

Why do I need these rules?	Rule Highlights
❑ 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.	• One rule blocks outbound traffic to known malicious IP addresses, while another 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
	outbound traffic rule, and as the Source address for the inbound traffic rule. • Deny traffic that match these rules. • Enable logging for traffic matching these rules so that you can investigate potential threats on your network. • Because these rules are intended to catch malicious traffic, they match traffic from any user running on any port.

			Source				Destination						
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
Drop Outbound PANW Malicious IP	none	universal	any	any	any	any	any	Palo Alto Netw...	any	any	Deny	none	
Drop Inbound PANW Malicious IP	none	universal	any	Palo Alto Netw...	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
❑ This rule protects you against IP addresses that Palo Alto Networks has shown to belong to Bulletproof hosting providers. Bulletproof hosting providers have no or very limited restrictions on content and don't log events. This makes Bulletproof sites ideal places from which to launch command-and-control (C2) attacks and illegal activity because anything goes and nothing is tracked.	• 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 match these rules. • Enable logging for traffic matching these rules so that you can investigate potential threats on your network. • Because these rules are intended to catch malicious traffic, they match traffic from any user running on any port.

		Source			Destination						
Name	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
Drop Outbound Bulletproof...	universal	any	any	any	any	Palo Alto Networks - Bulletpro...	any	any	Deny	none	
Drop Inbound Bulletproof IP	universal	any	Palo Alto Networks - Bulletpro...	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
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. ❑ 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 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.	• 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 practice Security profiles. • Because this rule is intended to block malicious traffic, it matches traffic to and from any user, running on any port, and for any application.

		Source			Destination						
Name	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
Block Outbound High Risk IPs	universal	any	any	any	any	Palo Alto Networks - High risk IP addresses	any	any	Deny	none	
Block Inbound High Risk IPs	universal	any	Palo Alto Networks - High risk IP addresses	any	any	any	any	any	Deny	none	

STEP 4 | (MineMeld users only) Block traffic from inbound IP addresses that trusted third-party feeds have identified as malicious.

Why do I need this rule?	Rule Highlights
❑ Block traffic from malicious IP addresses based on block lists compiled by Spamhaus and the Internet Storm Center, a branch of the SANS Institute. The lists contain IP addresses that attackers use to spread malware, Trojans, and botnets, and to carry out large-scale infrastructure attacks.	• To enforce this rule: 1. Use MineMeld to forward the IP addresses from the following sources (known as miners in MineMeld), spamhaus.DROP, spamhaus.EDROP, and dshield.block, to an external dynamic list 2. Configure the firewall to access an ExternalDynamicList, using the URL that MineMeld provides for the list. 3. Set the external dynamic list as the Source address for the rule. • 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 misuse of applications and potential threats on your network.

Why do I need this rule?	Rule Highlights
	• Because this rule is intended to catch malicious traffic, it matches to traffic from any user running on any port.

			Source				Destination						
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
Drop Minemeld Inbound IPs	none	universal	any	MM-inbound-IPs	any	any	any	any	any	any	Drop	none	

Step 2: Create the Application Whitelist Rules

After you Identify Whitelist Applications you are ready to create the next part of the best practice internet gateway security policy rulebase: the application whitelist rules. Every whitelist rule you create must allow traffic based on application (not port) and, with the exception of certain infrastructure applications that require user access before the firewall can identify the user, must only allow access to known users. Whenever possible, Create User Groups for Access to Whitelist Applications so that you can limit user access to the specific users or user groups who have a business need to access the application.

To convert port-based rules to application-based rules, use Policy Optimizer, which provides an intuitive way to view the applications on port-based rules and convert them to application-based rules so you can safely enable applications. Best Practices for Migrating to Application-Based Policy shows you how to use Expedition to perform a like-for-like migration from a legacy (port-based) firewall to a Palo Alto Networks firewall (or Panorama) and then use Policy Optimizer to convert the port-based policy to an application-based policy.

When creating the application whitelist rules, make sure to place more specific rules above more general rules. For example, the rules for all of your sanctioned and infrastructure applications would come before the rules that allow general access to certain types of business and personal applications. This first part of the rulebase includes the allow rules for the applications you identified as part of your application whitelist:

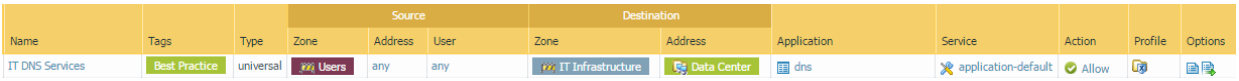
- Sanctioned applications you provision and administer for business and infrastructure purposes
- General business applications that your users may need to use in order to get their jobs done
- General applications you may choose to allow for personal use

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

Every application whitelist rule also requires that you attach the best practice security profiles to ensure that you are scanning all allowed traffic for known and unknown threats. If you have not yet created these profiles, then Create Best Practice Security Profiles for the Internet Gateway. And, because you can't inspect what you can't see, you must also make sure you have configured the firewall to Decrypt Traffic for Full Visibility and Threat Inspection.

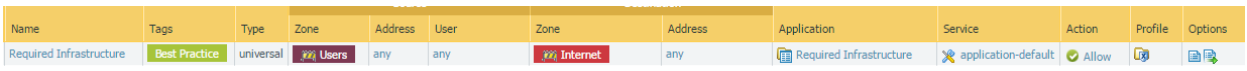
STEP 1 | Allow access to your corporate DNS servers.

Why do I need this rule?	Rule Highlights
❑ Access to DNS is required to provide network infrastructure services, but it is commonly exploited by attackers. ❑ Allowing access only on your internal DNS server reduces your attack surface.	• Because this rule is very specific, place it at 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 will need access to these services before they are logged in, you must allow access to any user.



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

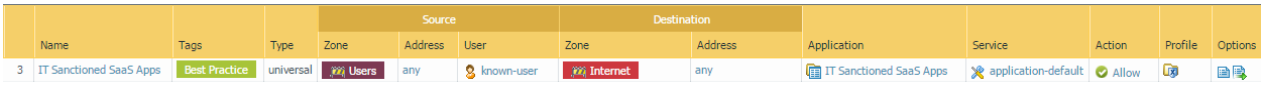
Why do I need this rule?	Rule Highlights
❑ Enable the applications that provide your network infrastructure and management functions, such as NTP, OCSP, STUN, and ping. ❑ While DNS traffic allowed in the preceding rule is restricted to the destination address in the data center, these applications may not reside in your data center and therefore require a separate rule.	• Because these applications run on the default port, allow access to any user (users may not yet be a known-user because of when these services are needed), and all have a destination address of any, contain them in a single application group and create a single rule to enable access to all of them. • Users may not have logged in yet at the time they need access to the infrastructure applications, so make sure this rule allows access to any user.



STEP 3 | Allow access to IT sanctioned SaaS applications.

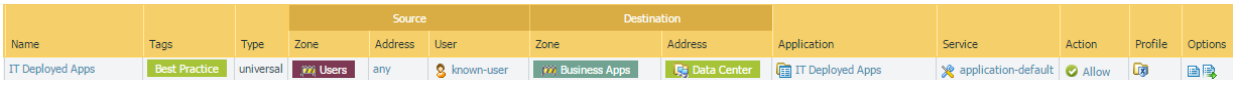
Why do I need this rule?	Rule Highlights
❑ With SaaS applications, your proprietary data is in the cloud. This rule ensures that only your known users have access to these applications (and the underlying data).	• Create an application group to group all sanctioned SaaS applications. • SaaS applications should always run on the application default port.

Why do I need this rule?	Rule Highlights
❑ Scan allowed SaaS traffic for threats.	• Restrict access to your known users. See Create User Groups for Access to Whitelist Applications.



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

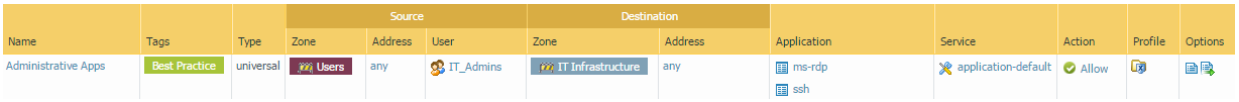
Why do I need this rule?	Rule Highlights
❑ Business-critical data center applications are often leveraged in attacks during the exfiltration stage, using applications such as FTP, or in the lateral movement stage by exploiting application vulnerabilities. ❑ Many data center applications use multiple ports; setting the Service to application-default safely enables the applications on their standard ports. You should not allow applications on non-standard ports because it is often associated with evasive behavior.	• Create an application group to group all data center applications. • Create an address group for your data center server addresses. • Restrict access to your known users. See Create User Groups for Access to Whitelist Applications.



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

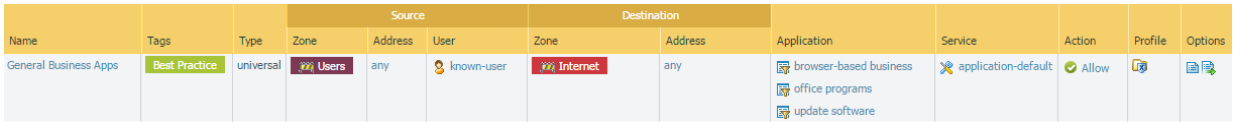
Why do I need this rule?	Rule Highlights
❑ To reduce your attack surface, Create User Groups for Access to Whitelist Applications. ❑ Because administrators often need access to sensitive account data and remote access to other systems (for example RDP), you can greatly reduce your attack surface by only allowing access to the administrators who have a business need.	• 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 that you can enforce them on their default ports rather than opening additional ports on your network.

Why do I need this rule?	Rule Highlights
	• If you have different user groups for different applications, create separate rules for granular control.



STEP 6 | Allow access to general business applications.

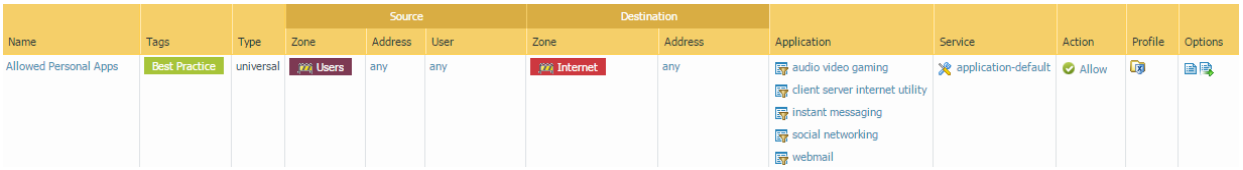
Why do I need this rule?	Rule Highlights
❑ Beyond the applications you sanction for use and administer for your users, there are a variety of applications that users may commonly use for business purposes, for example to interact with partners, such as WebEx, Adobe online services, or Evernote, but which you may not officially sanction. ❑ Because malware often sneaks in with legitimate web-based applications, this rule allows you to safely allow web browsing while still scanning for threats. See Create Best Practice Security Profiles for the Internet Gateway.	• Restrict access to your known users. See Create User Groups for Access to Whitelist Applications. • For visibility, Create an application filter for each type of application you want to allow. • Attach the best practice security profiles to ensure that all traffic is free of known and unknown threats. See Create Best Practice Security Profiles for the Internet Gateway.



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

Why do I need this rule?	Rule Highlights
❑ As the lines blur between work and personal devices, you want to ensure that all applications your users access are safely enabled and free of threats. ❑ By using application filters, you can safely enable access to personal applications when you create this initial rulebase. After you assess what applications are in use, you can use the information to decide whether to remove the filter and allow a smaller subset of personal applications	• Restrict access to your known users. See Create User Groups for Access to Whitelist Applications. • For visibility, create an application filter for each type of application you want to allow. • Scan all traffic for threats by attaching your best practice security profile group. See Create Best Practice Security Profiles for the Internet Gateway.

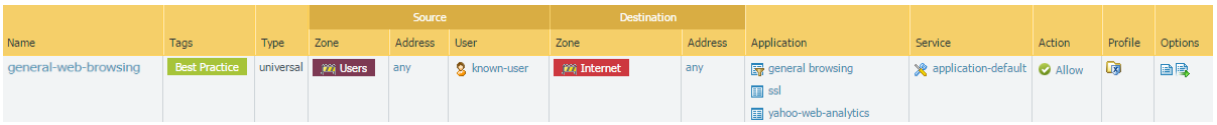
Why do I need this rule?	Rule Highlights
appropriate for your acceptable use policies.	



Name	Tags	Type	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Application	Service	Action	Profile	Options
Allowed Personal Apps	Best Practice	universal	Users	any	any	Internet	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
❑ While 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. You must Create Best Practice Security Profiles for the Internet Gateway and attach them to this rule in order to safely enable web browsing. ❑ Because threats often hide in encrypted traffic, you must Decrypt Traffic for Full Visibility and Threat Inspection if you want to safely enable web browsing.	• Use the same best practice security profiles as the other rules, except the Best Practice Internet Gateway File Blocking Profile profile, which is more stringent because general web browsing traffic is more vulnerable to threats, and the URL Filtering profile, which you should tighten as much as possible. • Allow only known users, to prevent devices with malware or embedded devices from reaching the internet. • 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 are excluded from decryption. • Set the Service to **application-default**



Name	Tags	Type	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Application	Service	Action	Profile	Options
general-web-browsing	Best Practice	universal	Users	any	known-user	Internet	any	general browsing ssl yahoo-web-analytics	application-default	Allow		

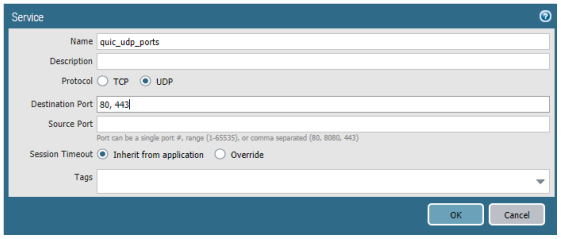
Step 3: Create the Application Block Rules

Although the overall goal of your security policy is to safely enable applications using application whitelist rules (also known as *positive enforcement*), the initial best practice rulebase must also include rules to help you find gaps in your policy and identify possible attacks. Because these rules are designed to catch things you didn't know were running on your network, they allow traffic that could also pose security risks on your network. Therefore, before you can create the temporary rules, you must create rules that explicitly blacklist applications designed to evade or bypass security or that are commonly exploited by attackers, such as public DNS and SMTP, encrypted tunnels, remote access, and non-sanctioned file-sharing applications.

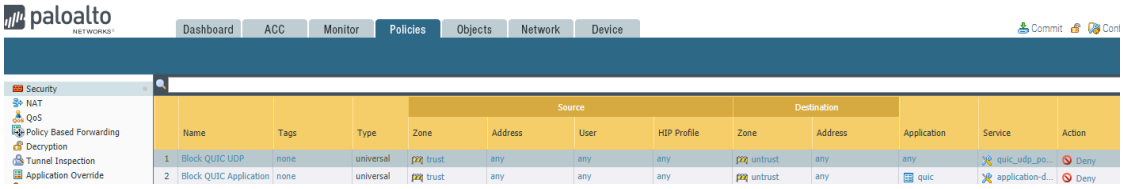
Each of the tuning rules you will define in Step 4: Create the Temporary Tuning Rules are designed to identify a specific gap in your initial policy. Therefore some of these rules will need to go above the application block rules and some will need to go after.

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

Why do I need this rule?	Rule Highlights
❑ Chrome and some other browsers establish sessions using QUIC instead of TLS, but QUIC uses proprietary encryption that the firewall can't decrypt, so potentially dangerous encrypted traffic may enter the network. ❑ Blocking QUIC forces the browser to fall back to TLS and enables the firewall to decrypt the traffic. ❑ It requires two Security policy rules to ensure that QUIC is blocked.	• Before you create the policy rules, you must first 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.



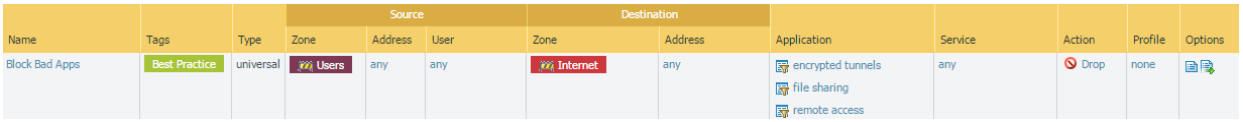
Notice that the Service specifies the UDP ports to block for QUIC in the first rule:



STEP 2 | Block applications that do not have a legitimate use case.

Why do I need this rule?	Rule Highlights
❑ Block nefarious applications such as encrypted tunnels and peer-to-peer file sharing, as well as web-based file sharing applications that are not IT sanctioned. ❑ Because the tuning rules that follow are designed to allow traffic with malicious intent or legitimate traffic that is not matching your policy rules as expected, these rules could also allow risky or	• 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 misuse of applications and potential threats on your network.

Why do I need this rule?	Rule Highlights
malicious traffic into your network. This rule prevents that by blocking traffic that has no legitimate use case and that could be used by an attacker or a negligent user.	• Because this rule is intended to catch malicious traffic, it matches to traffic from any user running on any port.



Name	Tags	Type	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Application	Service	Action	Profile	Options
Block Bad Apps	Best Practice	universal	Users	any	any	Internet	any	encrypted tunnels file sharing remote access	any	Drop	none	

STEP 3 | Block public DNS and SMTP applications.

Why do I need this rule?	Rule Highlights
❑ Block public DNS/SMTP applications to avoid DNS tunneling, command and control traffic, and remote administration.	• 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 matching this rule so that you can investigate a potential threat on your network.

Name	Tags	Type	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Application	Service	Action
Block Public DNS and SMTP	Best Practice	universal	Users	any	any	Internet	any	dns smtp	any	Reset Both

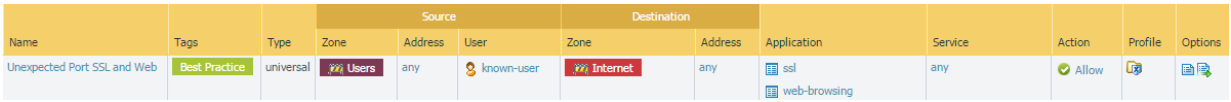
Step 4: Create the Temporary Tuning Rules

The temporary tuning rules are explicitly designed to help you monitor the initial best practice rulebase for gaps and alert you to alarming behavior. For example, you will create temporary rules to identify traffic that is coming from unknown user or applications running on unexpected ports. By monitoring the traffic matching on the temporary rules you can also gain a full understanding of all of the applications in use on your network (and prevent applications from breaking while you transition to a best practice rulebase). You can use this information to help you fine tune your whitelist, either by adding new whitelist rules to allow applications you weren't aware were needed or to narrow your whitelist rules to remove application filters and instead allow only specific applications in a particular category. When traffic is no longer hitting these rules you can Remove the Temporary Rules.

Some of the temporary tuning rules must go above the rules to block bad applications and some must go after to ensure that targeted traffic hits the appropriate rule, while still ensuring that bad traffic is not allowed 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.

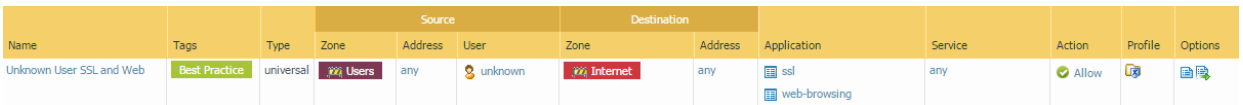
Why do I need this rule?	Rule Highlights
❑ This rule helps you determine if you have any gaps in your policy where users are unable to access legitimate applications because they are running on non-standard ports. ❑ You must monitor all traffic that matches this rule. For any traffic that is legitimate, you should tune the appropriate allow rule to include the application, and creating a custom application where appropriate.	• Unlike the whitelist rules that allow applications on the default port only, this rule allows web-browsing and SSL traffic on any port so that you can find gaps in your whitelist. • Because this rule is intended to find gaps in policy, limit it to known users on your network. See Create User Groups for Access to Whitelist Applications. • Make sure you also explicitly allow SSL as an application here if you want to allow users to be able to browse to HTTPS sites that aren't decrypted (such as financial services and healthcare sites). • You must add this rule above the application block rules or no traffic will hit this rule.



			Source			Destination						
Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
Unexpected Port SSL and Web	Best Practice	universal	Users	any	known-user	Internet	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.

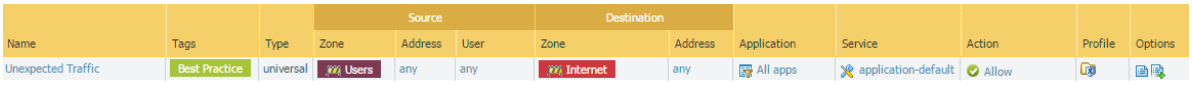
Why do I need this rule?	Rule Highlights
❑ This rule helps you determine whether you have gaps in your User-ID coverage. ❑ This rule also helps you identify compromised or embedded devices that are trying to reach the internet. ❑ It is important to block non-standard port usage, even for web-browsing traffic, because it is usually an evasion technique.	• While the majority of the application whitelist 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. • Because it is an allow rule, you must attach the best practice security profiles to scan for threats.



			Source			Destination						
Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
Unknown User SSL and Web	Best Practice	universal	Users	any	unknown	Internet	any	ssl web-browsing	any	Allow		

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

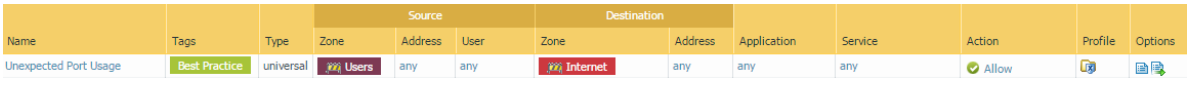
Why do I need this rule?	Rule Highlights
❑ This rule provides visibility into applications that you weren't aware were running on your network so that you can fine-tune your application whitelist. ❑ Monitor all traffic matching this rule to determine whether it represents a potential threat, or whether you need to modify your whitelist rules to allow the traffic.	• 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 are running PAN-OS 7.0.x or earlier, to appropriately identify unexpected applications, you must create an application filterthat includes all applications, instead of setting the rule to allow **any** application.



			Source			Destination						
Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
Unexpected Traffic	Best Practice	universal	Users	any	any	Internet	any	All apps	application-default	Allow		

STEP 4 | Allow any application on any port to identify applications running where they shouldn't be.

Why do I need this rule?	Rule Highlights
❑ This rule helps you identify legitimate, known applications running on unknown ports. ❑ This rule also helps you identify unknown applications for which you need to create a custom application to add to your application whitelist. ❑ Any traffic matching this rule is actionable and requires that you track down the source of the traffic and ensure that you are not allowing any unknown tcp, udp or non-syn-tcp traffic.	• Because this is a very general rule that allows any application from any user on any port, it must come at the end of your rulebase. • Enable logging for traffic matching this rule so that you can investigate for misuse of applications and potential threats on your network or identify legitimate applications that require a custom application.



			Source			Destination						
Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
Unexpected Port Usage	Best Practice	universal	Users	any	any	Internet	any	any	any	Allow		

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

Traffic that does not match any of the rules you defined will match the predefined interzone-default rule at the bottom of the rulebase and be denied. For visibility into the traffic that is not matching any of the rules you created, enable logging on the interzone-default rule:

STEP 1 | Select the interzone-default row in the rulebase and click **Override** to enable editing on this rule.

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 click **OK**.

STEP 4 | Create a custom report to monitor traffic that hits this rule.

1. Select **Monitor** > **Manage Custom Reports**.
2. **Add** a report and give it a descriptive **Name**.
3. Set the **Database** to **Traffic Summary**.
4. Select the **Scheduled** check box.
5. Add the following to the Selected Columns list: **Rule**, **Application**, **Bytes**, **Sessions**.
6. Set the desired **Time Frame**, **Sort By** and **Group By** fields.
7. Define the query to match traffic hitting 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

A best practice security policy is iterative. It is a tool for safely enabling applications, users, and content by classifying all traffic, across all ports, all the time. As soon as you Define the Initial Internet Gateway Security Policy, you must begin to monitor the traffic that matches the temporary rules designed to identify policy gaps and alarming behavior and tune your policy accordingly. By monitoring traffic hitting these rules, you can make appropriate adjustments to your rules to either make sure all traffic is hitting your whitelist application allow rules or assess whether particular applications should be allowed. As you tune your rulebase, you should see less and less traffic hitting these rules. When you no longer see traffic hitting these rules, it means that your positive enforcement whitelist rules are complete and you can Remove the Temporary Rules.

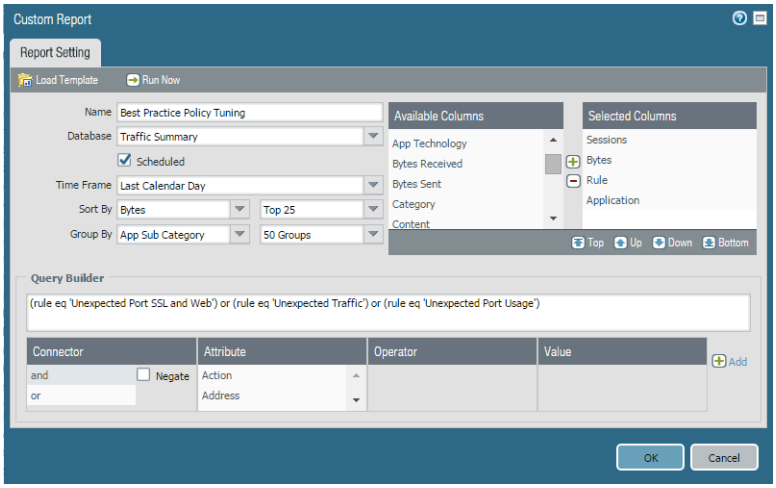
Because new App-IDs are added in weekly content releases, you should review the impact App-ID changes have on your policy.

STEP 1 | Create custom reports that let you monitor traffic that hits the rules designed to identify policy gaps.

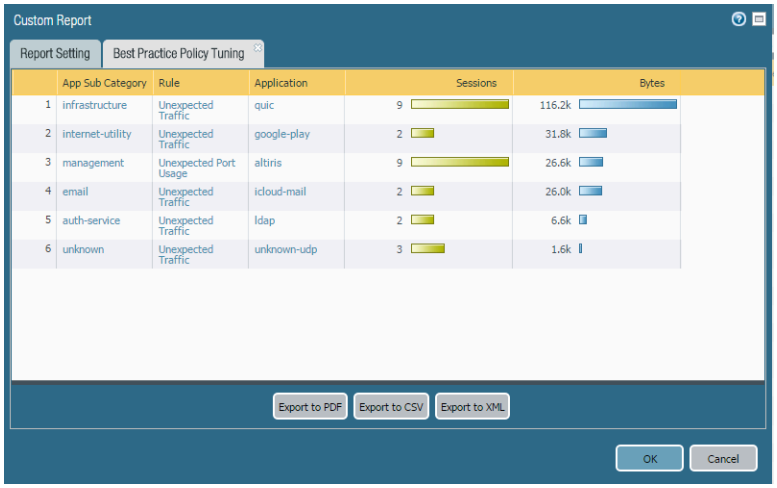
1. Select **Monitor** > **Manage Custom Reports**.
2. **Add** a report and give it a descriptive **Name** that indicates the particular policy gap you are investigating, such as Best Practice Policy Tuning.
3. Set the **Database** to **Traffic Summary**.
4. Select the **Scheduled** check box.
5. Add the following to the Selected Columns list: **Rule**, **Application**, **Bytes**, **Sessions**.
6. Set the desired **Time Frame**, **Sort By** and **Group By** fields.
7. Define the query to match traffic hitting the rules designed to find policy gaps and alarming behavior. You can create a single report that details traffic hitting any of the

rules (using the **or** operator), or create individual reports to monitor each rule. Using the rule names defined in the example policy, you would enter the corresponding queries:

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



STEP 2 | Review the report regularly to make sure you understand why traffic is hitting each of the best practice policy tuning rules and either update your policy to include legitimate applications and users, or use the information in the report to assess the risk of that application usage and implement policy reforms.



Remove the Temporary Rules

After several months of monitoring your initial internet gateway best practice security policy, you should see less and traffic hitting the temporary rules as you make adjustments to the rulebase. When you no longer see any traffic hitting these rules, you have achieved your goal of transitioning to a fully application-based Security policy rulebase. At this point, you can finalize your policy rulebase by removing the temporary rules, which includes the rules you created to block bad applications and the rules you created for tuning the rulebase.

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

STEP 2 | Select the rule and click **Delete**.

Alternatively, **Disable** the rules for a period of time before deleting them. This would allow you to **Enable** them again if traffic logs show traffic matching the interzone-default rule.

STEP 3 | **Commit** the changes.

Maintain the Rulebase

Because applications are always evolving, your application whitelist also needs to evolve. Each time you make a change in what applications you sanction, you must make a corresponding policy change. As you do this, instead of just adding a new rule as you would do with a port-based policy, identify and modify the rule that aligns with the application's business use case. Because the best practice rules leverage policy objects for simplified administration, adding support for a new application or removing an application from your whitelist typically means modifying the corresponding application group or application filter accordingly.

On Panorama or an individual firewall, 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, it indicates traffic that matches the rule may already be on the network even though you haven't activated the application, or that you may 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, you can monitor firewall health to compare devices to their baseline performance and to each other to identify deviations from normal behavior.

Palo Alto Networks sends content updates that you should download automatically and schedule for installation on firewalls as soon as possible. Most content updates contain updates to threat content (antivirus, vulnerabilities, anti-spyware, etc.) and may contain modified App-IDs. On the third Tuesday of each month, the content update also contains new App-IDs. You can set separate thresholds to delay installing regular content updates and to delay installing the once-a-month update that contains new App-IDs for a specified period of time after the download. Delaying installation enables you to install content updates that don't include new App-IDs as quickly as possible to get the latest threat signatures, while also providing more time to examine new App-IDs before installing them.

The content updates on the third Tuesday of each month that contain new App-IDs may cause changes in Security policy enforcement. Before you install new or modified App-IDs, review the policy impact, stage updates to test impact, and modify existing Security policy rules if necessary. The most efficient way to control downloading and installing content updates on firewalls is loading them on and pushing them from Panorama if you use Panorama.

Follow the general content update best practices, but keep in mind that on internet gateways, security is critical because any traffic could attempt to gain entrance to your network from the internet, so you want to roll out content updates as fast as possible:

- Quickly test content updates in a safe area of the network before you install them on an internet gateway.

- For content updates that don't contain new App-IDs, set the installation threshold to no more than two hours after the automatic download and conduct testing within that period.
- For content updates that contain new App-IDs, set the installation threshold no more than eight hours after the automatic download and conduct testing within that period.
- Configure Log Forwarding for all content updates.

STEP 1 | Before installing a new content update, review new and modified App-IDs to determine if there is policy impact.

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 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 or to add new sanctioned applications to or remove applications from your whitelist rules.