BEST PRACTICES

NETWORK – PROTECTING SYSTEMS AND APPLICATIONS FROM VULNERABILITIES

Preventing known threats

Vulnerabilities exist in nearly every piece of software, and they plague not only users of systems and applications who need to secure themselves against attackers but also the development teams who create and maintain secure products for their customers. Even when continuous code scanning and penetration testing is done, and vulnerabilities are found and fixed, introducing new code may create additional vulnerabilities that developers were not expecting. On top of all that, security researchers – or worse, attackers themselves – are constantly finding new zero-day vulnerabilities within previously trusted applications.

Application vulnerabilities represent one of the most common and significant threat vectors. Applications (as well as underlying systems software, such as databases and operating systems) are extremely complex, often containing millions or tens of millions of lines of code written by teams of developers. The growing number of connections between applications and other components in a network-based environment increases their complexity and, therefore, their vulnerability. As a result, vulnerabilities are inadvertently created that may be difficult to detect during code design, review and testing.

Application vulnerabilities provide attackers with an opportunity to insert malicious code into a system or escalate unauthorized user privileges that give them access to data or functions they should not have. Thus, these attacks are known as vulnerability exploits. Examples of server-based systems that are vulnerable to exploits include operating systems, web and email servers, programming platforms (such as .NET or Java), databases, and applications, such as Microsoft® Office, SharePoint® or Adobe® Flash®.

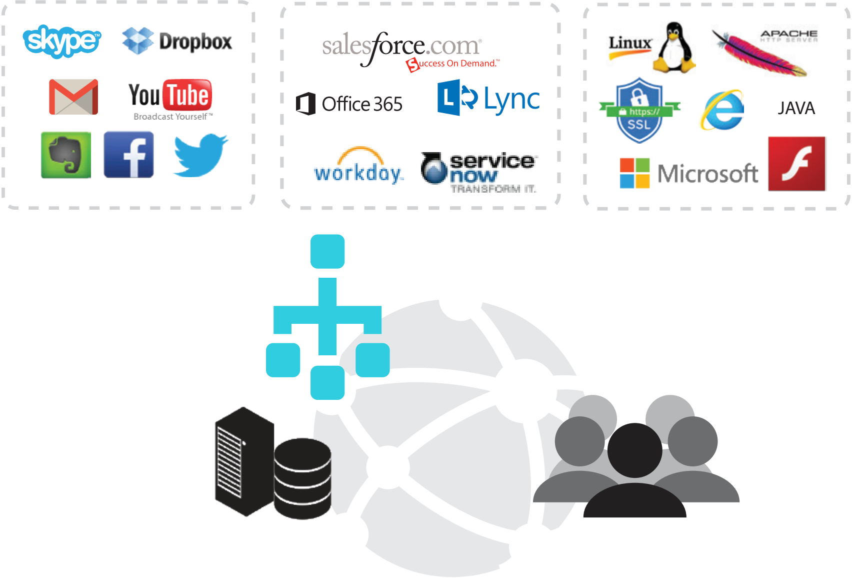


Figure 1: System and application vulnerabilities provide the means to compromise the parts of your network on which they reside, the users who have access to them, and the data within them

There is a wide variety of vulnerability exploits, and they are commonly used to covertly download malware viruses, which infect systems and execute code that affects system functions. Exploits may also contain spyware, or command-and-control (C2) software designed to take control of a system and then send information about the system or user back to the attacker. C2 software may be used to retrieve and upload additional malware, such as ransomware, or join in a distributed denial-of-service attack.

Tip: Consider patching, disabling or removing applications with known vulnerabilities. Removing a vulnerable application entirely eliminates any threat it may pose to your security. If your environment does not require Java®, Flash or other applications with known vulnerabilities, you should consider removing them entirely.

Palo Alto Networks® Threat Prevention subscription provides vulnerability protection, antivirus, and anti-spyware functions to detect and prevent known exploits, malware and C2 channels from being used by an attacker at the network level. The subscription stops malicious code that is attempting to exploit known vulnerabilities detects and blocks known viruses and can prevent an infected system from communicating with a malicious external server to prevent additional malware from being downloaded.

The Threat Prevention profiles comprise payload-based signatures. Payload-based signatures match on the malicious code within malware, including ransomware, trojans, etc., which may be installed on systems. The signatures detect and block multiple exploits targeting the same vulnerability and multiple variations of malware within the same family, providing more effective coverage for your assets.

Because Threat Prevention relies on previously detected signatures, it should be combined with tools, such as WildFire™ cloud-based malware analysis environment and Traps™ advanced endpoint protection, designed to detect and prevent advanced persistent threats in order to provide comprehensive protection against previously unknown attacks.

A Phased Approach to Protecting Vulnerable Systems and Applications

Whether you have recently started implementing Palo Alto Networks products or have been administering them for years, make sure you are maximizing their full value by reviewing our best practices for protecting vulnerable systems and applications.

As with any technology, there is usually a gradual approach to a complete implementation, consisting of carefully planned deployment phases meant to make the transition as smooth as possible with minimal impact to your end users. With this approach in mind, we have recommended our best practices for preventing vulnerability exploits and corresponding infection in three phases, each building on the recommendations before it. The ultimate goal for your Threat Prevention implementation should be to end up with thorough threat inspection profiles for all allowed traffic to safely enable systems and applications you and your users rely on.

Tip: Decrypt encrypted (HTTPS) web traffic whenever you can in order to scan it for threats. Encrypted web traffic is a favored vector for surreptitiously delivering file-based exploits and infecting machines with malware.

PHASE 1: PLANNING

Threat Prevention software is included in all Palo Alto Networks Next-Generation Firewall (NGFW) deployments and activated through a subscription license. Therefore, the first thing you should do is activate this component by entering a valid license key using the Administrative Console. We highly recommend deploying the NGFW with valid Threat Prevention licenses in-line, as opposed to out-of-band, because it will be able to actively block malicious traffic containing known exploits, malware, and command-and-control communications, instead of allowing it through and merely detecting and alerting you after the fact.

Planning also involves deciding which security profiles you want to configure. Applying a security profile to an application-based security rule allows you to scan network traffic for threats and determine how you want to handle traffic that potentially contains them, for instance dropping the packets or resetting the server and/or client connections. The Palo Alto Networks NGFW provides default security profiles for vulnerability protection, antivirus, and spyware (command-and-control) protection that you can use, out of the box, to begin protecting your network from threats. As you develop a better understanding about the security needs on your network, you can create custom profiles.

Other available profiles and tools, which are beyond the scope of this chapter, include: URL Filtering, WildFire analysis, data filtering, file blocking, external dynamic lists, and denial of service (DoS) protection.

Administrator's Guide:

- Security Profiles
- Create Best Practice Security Profiles

PHASE 2: IMPLEMENTING ALERT-ONLY POLICIES

Initially, you should set up antivirus, anti-spyware, and vulnerability protection security profiles to alert only, so that you can get a sense of what kind of traffic these signatures match, and you can estimate any impact to your users and operations team. For example, if you notice that there are a high number of threat alerts for a specific application or IP address, you have the opportunity to research and verify that they are indeed threats to your organization. You can then decide whether you want to block some or all of the traffic containing them, or you may opt to block the application or IP address altogether.

Tip: Configure User-ID™ to enable the identification of usernames. This will allow you to quickly identify which user is running an infected machine, instead of having to manually map an IP address to a workstation.

You can choose how to respond to a threat event:

- **Default** – Typically, an alert or a reset-both.
- **Allow** – Permits the application traffic and does not generate an alert.
- **Alert** – Permits the application traffic and generates an alert.
- **Drop** – Drops the application traffic.
- **Reset client** – Either resets (TCP) or drops (UDP) the client-side connection.
- **Reset server** – Either resets (TCP) or drops (UDP) the server-side connection.
- **Reset both** – Either resets (TCP) both client and server ends or drops (UDP) the connection.

Vulnerability Protection Profiles

The vulnerability protection profile blocks and logs attempts to exploit system flaws or gain unauthorized access to systems. While anti-spyware profiles help identify infected hosts as traffic leaves the network, vulnerability protection profiles protect against threats entering the network, such as buffer overflows, remote code execution, and other attempts to exploit system vulnerabilities. The default vulnerability protection profile protects clients and servers from known critical, high and medium-severity threats. You can also create exceptions, which allow you to change the response to a specific signature.

Tip: You can add security profiles that are commonly applied together to a security profile group; this set of profiles can be treated as a unit and added to security policy rules in one step.

Antivirus Profiles

All antivirus signatures are created by WildFire, our cloud-based malware analysis environment, which analyzes files from thousands of customers and threat intelligence feeds around the world, and delivers signatures to protect against previously unknown, zero-day malware as a result. The antivirus profile scans for a wide variety of malware within a broad range of file types, such as portable executables, Android™ APKs, HTML and JavaScript files, including support for scanning inside compressed files (.rar, .zip) and data encoding schemes.

Anti-Spyware Profiles

Anti-spyware profiles block spyware on compromised hosts from trying to communicate with external C2 servers. This prevents the spyware from downloading additional malware or participating in other botnet activities. It also allows you to detect malicious traffic that infected clients are attempting to send from the network. You can apply various levels of protection between zones. For example, you may want to have custom anti-spyware profiles that minimize inspection between trusted zones, while maximizing inspection on traffic sent to or from an untrusted zone, such as Internet-facing zones.

Tip: The Palo Alto Networks platform provides two categories of preset profile: default and strict. The default profile provides a mix of block and alert actions. The strict profile blocks medium-, high- and critical-severity vulnerabilities from being exploited.

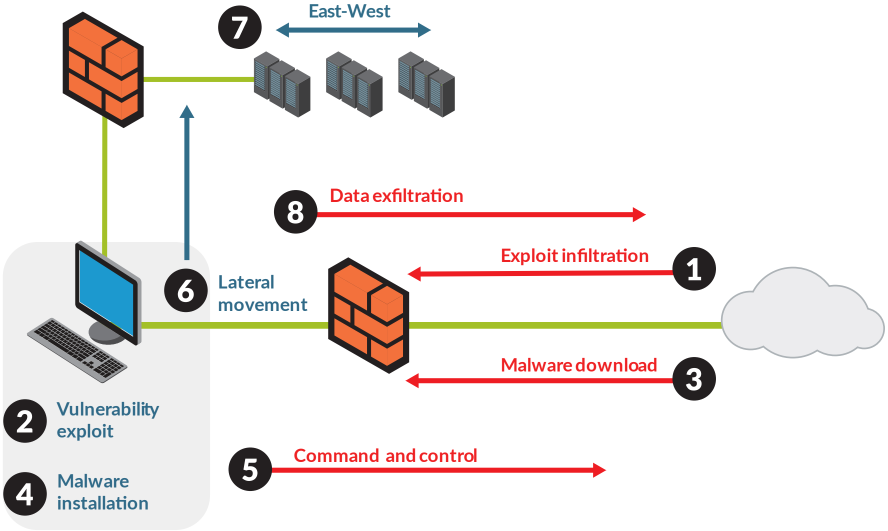


Figure 2: There are multiple stages within an attack. Vulnerability protection, antivirus, and anti-spyware security profiles protect the network against attack stages 1, 3, 5 and 8.

Tip: Consider configuring certain vulnerability signatures with a time threshold. For example, configure user login "brute force" signatures to match only after five unsuccessful login attempts in 30 seconds. This will help to cut down on alerts triggered by legitimate user mistakes while still alerting you to attempted attacks.

Policy Category and Default Settings

After setting up the profiles you need, attach the security profiles (antivirus, anti-spyware, and vulnerability protection) to a security rule.

Filter your logs to show your matches on critical- and high-severity threats first, then medium- and low-severity threats, and informational alerts last. Sorting this way sets you up to begin blocking those threats that pose the greatest risks to the organization first, where security is likely more important than any impact to application usability.

Palo Alto Networks professional services teams are available to review security logs and evaluate the impact of profile changes.

Administrator's Guide:

- Set Up Antivirus, Anti-Spyware, and Vulnerability Protection Profiles
- Antivirus Profiles
- Anti-Spyware Profiles
- Vulnerability Protection Profiles

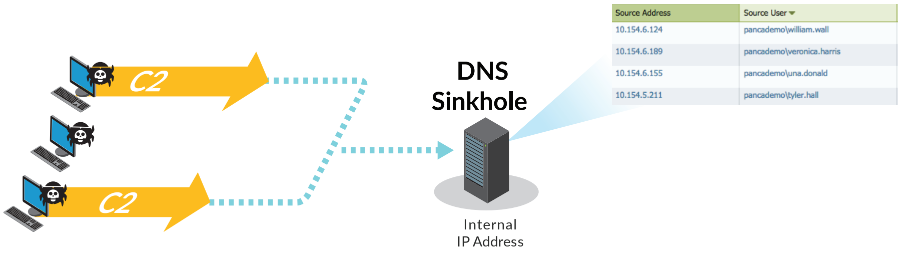
Tip: Use the external dynamic lists (labeled "Dynamic Block Lists" in PAN-OS® versions 7.0 and earlier) to block the IP addresses, URLs and domains from your threat logs and/or from AutoFocus™ contextual threat intelligence service that are hosting and delivering threats.

PHASE 3: REFINEMENT, MONITORING AND ACTIVE PREVENTION

Use the web interface to monitor the system log files for known vulnerabilities that have been detected. This will help to inform you about the nature and volume of threats targeting application vulnerabilities in your environment.

If you initially configured your system using alert-only security profiles, consider actively blocking threats. You can start blocking critical- and high-severity exploits, malware, and command-and-control channels as you gain a better understanding of the Threat Prevention profiles and any impact they may have on your users. Over time, you can then move to actively blocking a greater number of medium- and low-severity threats.

To combat malicious C2 activity, consider implementing a DNS sinkhole when configuring your anti-spyware profile. DNS sinkholing reroutes DNS-request traffic sent by users to malicious domains to an internal IP address of your choosing. This feature provides two benefits. First, it prevents the spyware module from contacting a C2 server, preventing the spyware from downloading additional malware or participating in a botnet. Second, DNS sinkhole traffic is logged, which enables you to identify and decontaminate the infected machine. Note that no changes to internal DNS servers are required to implement a DNS sinkhole.



Source Address	Source User ▾
10.154.6.124	pancademo\william.wall
10.154.6.189	pancademo\veronica.harris
10.154.6.155	pancademo\una.donald
10.154.5.211	pancademo\tyler.hall

Figure 3: **The sinkhole action within the anti-spyware profile reroutes command-and-control traffic to an internal IP address to both prevent C2 communication and identify infected user devices.**

Use a security policy to block applications that are not business-critical and contain too many threats, as evidenced by your threat logs. This especially includes unknown applications/traffic. Unknown traffic can be a non-compliant application or protocol that is anomalous or abnormal and may contain threats. Until you verify what the application is, which ports it is using, and whether the traffic it generates is legitimate, the prudent thing to do is block it.

From an ongoing management perspective, perhaps the most important thing you can do is to continue to keep signatures up to date. Configure your NGFW to download signature updates daily or, if you also have a WildFire subscription, configure updates every five minutes. The number of signatures does not impact performance and throughput because of the single-pass scanning architecture that the Palo Alto Networks NGFW uses, and your ability to prevent new exploits, malware families and command-and-control channels will always be up to date.

Administrator's Guide:

- DNS Sinkholing
- Use an External Dynamic List in Policy

Palo Alto Networks Commitment to Support Customers

Palo Alto Networks is committed to ensuring a successful deployment and provides comprehensive support through our Global Customer Services organization. We understand fully that failure is not an option. Our support offerings and training programs are designed to mitigate any deployment concerns you may have.

- Palo Alto Networks Solution Assurance Services
- Palo Alto Networks Customer Support Plans
- Palo Alto Networks Consulting Services
- Palo Alto Networks Educational Services

Join Palo Alto Networks LIVE Community for user discussions, tutorials and knowledge-base articles.

fuel
PALO ALTO NETWORKS
USER GROUP

Join Palo Alto Networks Fuel User Group community to connect with like-minded professionals around the globe who are ready to discuss their hard-won best practices and trade insights. You can also get exclusive access to subject matter experts to answer your most challenging, security-related questions through in-person events as well as online events, such as webinars and Q&A sessions.

paloalto
NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054

Main:	+1.408.753.4000
Sales:	+1.866.320.4788
Support:	+1.866.898.9087

www.paloaltonetworks.com