Bpappas

12-02-2016 05:23 P

Summary of BlackNurse

On Thursday, Nov. 10, 2016, TDC Security Operations Center in Denmark published a report stating they had noticed several low-volume ICMP attacks in their customers' networks. TDC named this type of attack BlackNurse.

The security of our customers is our top priority. We have conducted an investigation into this issue and to date have found that Palo Alto Networks Next-Generation Firewall customers may be affected in a specific scenario that contravenes best practices by exceeding the platform's maximum Connections Per Seconds (CPS) limits and no protections have been enabled on the device.

Attack details

A traditional ICMP flood attack sends ICMP requests to the target in a large volume. BlackNurse, on the other hand, is an ICMP attack that sends a low volume of ICMP Type 3 (Destination Unreachable) Code 3 (Port Unreachable) requests to the target. BlackNurse is a form of Denial-of-Service (DoS) attack and the TDC report claims that it has the potential to disrupt the target organization's operations.

Impact

Palo Alto Networks Next-Generation Firewalls may be impacted by the BlackNurse attack if the attack rate approaches the platform's maximum Connections Per Seconds (CPS) limits and no protections are enabled on the device.

Recommendations

For protection against BlackNurse, we recommend that customers implement ICMP Flood Protection, which is part of Zone Protection. Customers may also implement DoS Protection in cases where the attack is from a single source IP.

Note: All BlackNurse attacks larger than the platform's maximum Connections Per Seconds (CPS) limits, may result in unexpected performance issues. In such cases, "rate limiting" of the involved ICMP traffic has to take place before reaching our firewall.

Zone Protection

A Zone Protection profile is enforced before security policy checks. This helps throttle packets once the threshold is reached and protects the firewall resources as well as resources being protected by the firewall.

Please follow the steps below from the page Zone Protection section in the PAN-OS 7.1; PAN-OS 7.0; PAN-OS 6.1; PAN-OS 6.0 Administrator's Guides:

- Enable ***Zone Protection***with ICMP Flood Protection.
- Apply the ***maximum threshold*** (Connections/second) values per the table below.

Firewall	Maximum Threshold
PA-7050	16,000
PA-5060	7,500
PA-5050	7,500
PA-5020	8,000
PA-3060	8,000
PA-3050	8,000
PA-3020	8,000
PA-500	2,000
PA-200	1,000

Note: Based on our testing, keeping a threshold value above what is recommended may result in sluggish and/or unexpected performance. Testing was performed on PAN-OS 7.1.5 and the above values will work similarly with previous versions.

- If no ICMP error messages are expected in your environment: Enable Zone Protection's "**Discard ICMP embedded with error message**" can be used. This option is configured under the Zone Protection Profile -> Packet Based Protection -> ICMP Drop -> Discard ICMP embedded with error message.

Note : This setting will drop ALL ICMP packets with an error message under ALL conditions. If your environment uses ICMP error messages for legitimate purposes, you should not enable this option on the ingress zone

- Commit the configuration.

DoS Protection

A DoS Protection profile may help mitigate against the attack more efficiently in cases where the attack is from a single source IP. The thresholds for DoS policy are typically lower since these thresholds are on a 'per IP' basis whereas the Zone Protection configuration threshold is an aggregate of all ingress traffic for the zone.

Note: Please do not use a DoS Protection profile on interfaces facing a high number of sources, such as the internet-facing interfaces.

To implement DoS Protection measures, please follow the below steps from the page Configure DoS Protection Against Flooding of New Sessions in the PAN-OS 7.1 Administrator’s Guide:

- Configure a DoS Protection profile for flood protection. Because flood attacks can occur over multiple protocols, the recommended best practice is to activate protection for all flood types in the DoS Protection profile. However, to protect against BlackNurse, the following types of flood protection are required:
  - ICMP Flood
  - ICMPv6 Flood
- Commit the configuration.

For more, please refer to the step-by-step instructions listed on the Configure DoS Protection Against Flooding of New Sessions page in the PAN-OS 7.1 Administrator’s Guide.

For customers using a version of PAN-OS prior to 6.1, please see the PAN-OS Administrator’s Guide for your organization’s software version listed on our Technical Documentation page and refer to the steps listed under the section ‘Threat Prevention’ > About Security Profiles > DoS Protection.

Note: DoS and Zone protection is included as part of PAN-OS and does not require any software subscriptions.

Should you have any questions or need assistance with implementing these recommendations, please don’t hesitate to contact our support team at support.paloaltonetworks.com.

☆☆☆☆☆

▸ Custom Tag

594 Views