# THE POWER OF 2

Using

## NSFOCUS Threat Feeds

in PA's Firewall to Better Protect Against Attacks From APAC

## OVERVIEW

Every day organisations are facing a significant increase in attack traffic originating from all around the globe. To help counter this, Palo Alto has built dynamic threat prevention into their Next Generation PA Firewall family. This threat prevention technology relies on feeds from several sources including:

- ✓ The Palo Alto Wildfire Service
- ✓ The PAN-DB URL Filtering Service
- ✓ Integration into the Mindmeld application which allows for the aggregation and correlation of third-party threat intelligence feeds.

While valuable, these default threat feeds only capture around

**60%**

of the active global threats.

INTRODUCING

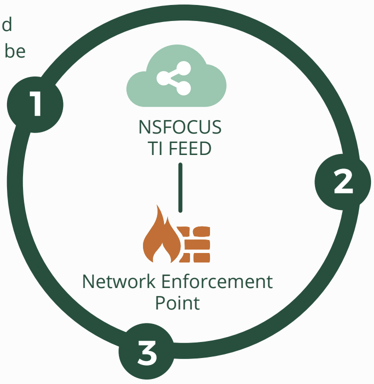
NSFOCUS

# Threat Intelligence Feeds

Most available threat feeds have poor visibility into Northern Asia where up to 40% of all malicious Internet traffic comes from.

The **NSFOCUS Threat Intelligence (NTI) Feed** subscriptions will help close this enormous cyber-threat hole by augmenting the default Palo Alto feeds with threat intelligence covering APAC and especially North Asia in depth.

## How it works?



1 NSFOCUS integrates with Palo Alto Mindmeld using an API Connector allowing NTI data to be intelligently combined with the Palo Alto Networks AutoFocus™ contextual threat intelligence service.

2 AutoFocus identifies the most virulent threats that you are exposed to by adding context around the attack, including malicious actor, malware family and campaign.

3 As a result of this integration, Palo Alto firewalls can now actively understand and block threats originating from China. Organizations with this integration are now having greater visibility into these threats hence allowing them to take remediation actions when needed. This integration results in a 40% improvement in coverage versus the default set of feeds.

## Why NSFOCUS Threat Intelligence is important to Palo Alto Customers

Ignoring threat intel about China and other dangerous countries in Northern Asia leaves you exposed to the vast amount of attack traffic that comes from that region.

Without NTI, your Palo Alto investment's return is not fully realized. You are missing a huge swath of malicious activities and IP addresses that are already identified by NSFOCUS database. Having the **NSFOCUS TI Perspective** allows your Palo Alto firewall to better defend against Chinese attack traffic, providing significant value to your investment in Palo Alto.

# NSFOCUS TI Data

immediately actionable on combating Chinese threats. Subscribing to NSFOCUS TI subscriptions instantly adds these capabilities to your Palo Alto Firewall:

- ✓ Verify known malicious addresses from Chinese Actors.
- ✓ Detect unknown or suspicious activities emanating from China.
- ✓ Ability to detect when internal protected assets are contacting Chinese Command and Control servers.

## Added value of the NTI Feeds

Synthesis of over **700GB per day** of known malicious Chinese activity from our vast sensor network composed of firewalls, anti-DDoS, endpoints, honeypots, Intrusion Detection Systems, and Web Application Firewalls fed to your firewall every few hours.

Updating dynamic lists throughout the day to prevent malicious connections to or from protected assets.

Access to the NTI portal to conduct forensic analysis of events and exposed asset analysis of IPs on the internet.

Palo Alto customers are now protected against otherwise unknown malicious IPs and URLs coming from China. The **Palo Alto Firewall** will be intelligently tuned to cover the Chinese “blind spot”, providing clarity and minimizing impacts from questionable traffic.

This means the protections offered by Palo Alto firewalls are greatly enhanced at minimal additional expense, providing a significant improvement to your organisations security posture.

## NSFOCUS - Complete Threat Intelligence

40% Threat intel from China + 60% Threat intel from Rest of World = Worldwide Threat Visibility

NSFOCUS

NSFOCUSGLOBAL.COM