

# THREATSTOP IP REPUTATION SERVICE BLOCKS BOTNETS AND PREVENTS DATA THEFT/MALWARE INFESTATION

## SRX Series Uses ThreatSTOP’s Blocklist to Prevent Traffic to and from Botnet and Malware Sites

### Challenge

Botnets and criminal malware steal valuable data, control your machines, and perpetrate active exploits that cause great damage to organizations. Current signature-based products do not stop this major threat cost-effectively or in a timely enough manner.

### Solution

ThreatSTOP delivers a blocklist of IP addresses for known criminal sites to Juniper Networks SRX Series Services Gateways to block all traffic to and from those sites.

### Benefits

- Blocks inbound spam, malware, and botnets in a way that can increase network performance and reduce hardware upgrade costs
- Prevents data theft and many zero-day attacks
- Reduces attack surface of your network by making it disappear from the criminal’s radar
- Easy to use, eliminating manual updates and lowering total cost of ownership

ThreatSTOP is a cloud service that delivers IP addresses for known criminal sites to Juniper Networks® SRX Series Services Gateways so that they can block all traffic to and from those sites. This blocklist is updated continually, and it is distributed to the SRX Series via a Domain Name System (DNS) lookup. The service can be enabled on an SRX Series device within an hour via a two-command install. No software, network reconfiguration, or user training is needed.

Botnets, spear-phishing, and related criminal malware are among the greatest network security risks today. Designed to steal valuable data and control your machines, these threats can cause great financial, competitive, productivity, and reputational damage. Industry surveys show botnet infection rates are near 100% for organizations of all sizes and types. No one is immune from this exponentially growing and pervasive problem.

Most of today’s security products rely on signature detection to spot threats. Used exclusively, this approach leads to low catch rates, slow detection, and high false positives. Equally important, these solutions do not stop malware from “calling home” to command and control hosts to pilfer your valuable financial, corporate, and customer data.

### The Challenge

Almost all security products in use today are based on some form of signature analysis, where an attempt is made to detect the signature of an exploit, write a patch for it, and have the customer implement it. While this has worked well in the past, this 20 year old approach is ineffective against modern day botnets and criminal malware for three key reasons:

- 1) It is impossible to keep up with the infinite combinations of possible exploits given their sheer volume and constantly changing nature.
- 2) The signature detection/patching cycle is always late and resource intensive for both vendor and customer.
- 3) Most outbound traffic is not inspected. Worse, encrypted SSL traffic can’t be inspected without breaking the SSL security model—creating still more opportunities for data exfiltration. Botnets depend on an outbound communications channel to “call home” for instructions from command and control hosts. Failing to inspect outbound traffic is an open invitation to data theft.

“By the time the malware is discovered and security companies have created a signature to protect users from it, the signature is already useless because that version of the malware is generally never used a second time.”

Forrester Research





**“You delayed my need to upgrade my email servers by 2 years. That’s \$200,000 I put in classrooms instead of hardware”**

Steve Gorham,

CIO, Hillsborough Community College, Tampa, FL

### 3. Prevent zero-day attacks

Zero-day attacks are often launched from IP addresses that already have a poor reputation because criminals usually use computers that are already under their control. Because ThreatSTOP-enabled SRX Series Services Gateways already know about these addresses, the network is proactively protected against many zero-day attacks. By comparison, signature-based products, because they rely on characterizing the signature or behavior of an attack, must wait for expert attack analysis and signature distribution before protection is enabled.

### 4. Reduce attack surface of network

When the ThreatSTOP/SRX Series solution rejects traffic from a bad IP address, the criminal’s host receives no acknowledgement that the probed computer exists. After a few attempts, the criminals’ attention will move elsewhere and your network effectively disappears from their view. This reduces your network’s attack surface, reduces spam, and decreases overall vulnerability.

### 5. Geo-blocking and sub-lists

ThreatSTOP supports specialized IP address sub-lists for expert users, including custom white and black lists, lists for inbound or outbound blocking, or specialized lists focused on geographical regions or malware types. The ability to block traffic from specific countries where malware origination is more prevalent is particularly useful for government agencies and organizations which have no reason to communicate with certain high threat countries.

### 6. Easy to use, eliminates manual updates, lowest TCO

ThreatSTOP is easy to set up and use with the lowest TCO. The service can be enabled on an SRX Series device within an hour via a two-command install. No software, network reconfiguration, or user training is needed. Once installed, the update process is automated via DNS, which eliminates the drudgery of manual updates and administration of block lists.

## Solution Components

ThreatSTOP’s IP reputation service is provisioned entirely via the website <https://threatstop.com/>. Subscribers can sign up, choose what threats they wish to protect against, and register their firewalls. The service is then installed on an SRX Series device by running simple scripts downloaded from the website. The initial setup can be done within an hour. Once installed, the SRX Series automatically updates its block policies via periodic contact with the ThreatSTOP DNS servers.

## Summary—Prevent Data Loss and Reduce Risk from Cyber Attack

The ThreatSTOP/SRX Series Services Gateways security solution prevents data loss, reduces network attack surface, and improves network performance by blocking traffic to and from known botnet and criminal malware sites. It is also easy to set up and use, eliminates manual work with automated updates via DNS, and lowering total cost of ownership.

## Next Steps

Would you like to stop botnets stealing from you, reduce your risk from malware infestation, and ensure compliance on information security?

For more information about ThreatSTOP, visit [www.threatstop.com](http://www.threatstop.com), or contact sales at [sales@threatstop.com](mailto:sales@threatstop.com), (telephone in North America and Asia Pacific, 760-542-1550; in EMEA, +44-1223-970-150). For more information about SRX Series Services Gateways, visit [www.juniper.net](http://www.juniper.net), or contact Juniper Networks at 888-JUNIPER (888-586-4737) or 408-745-2000.

## About ThreatSTOP

ThreatSTOP is the leading provider of real-time IP reputation service to protect networks against botnets and malicious malware. ThreatSTOP enables firewalls to block both incoming botnet attacks as well as outbound “call homes” to command and control hosts. Updated in real-time and automatically distributed via DNS to firewalls, ThreatSTOP delivers actionable threat intelligence to enable proactive defense against the most criminal malware sites. ThreatSTOP can be activated within an hour without an expensive forklift upgrade, network reconfigurations, or requiring manual updates. For more information, visit [www.threatstop.com](http://www.threatstop.com).

## About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at [www.juniper.net](http://www.juniper.net).

---

### Corporate and Sales Headquarters

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100  
[www.juniper.net](http://www.juniper.net)

### APAC Headquarters

Juniper Networks (Hong Kong)  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

### EMEA Headquarters

Juniper Networks Ireland  
Airside Business Park  
Swords, County Dublin, Ireland  
Phone: 35.31.8903.600  
EMEA Sales: 00800.4586.4737  
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2011 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.