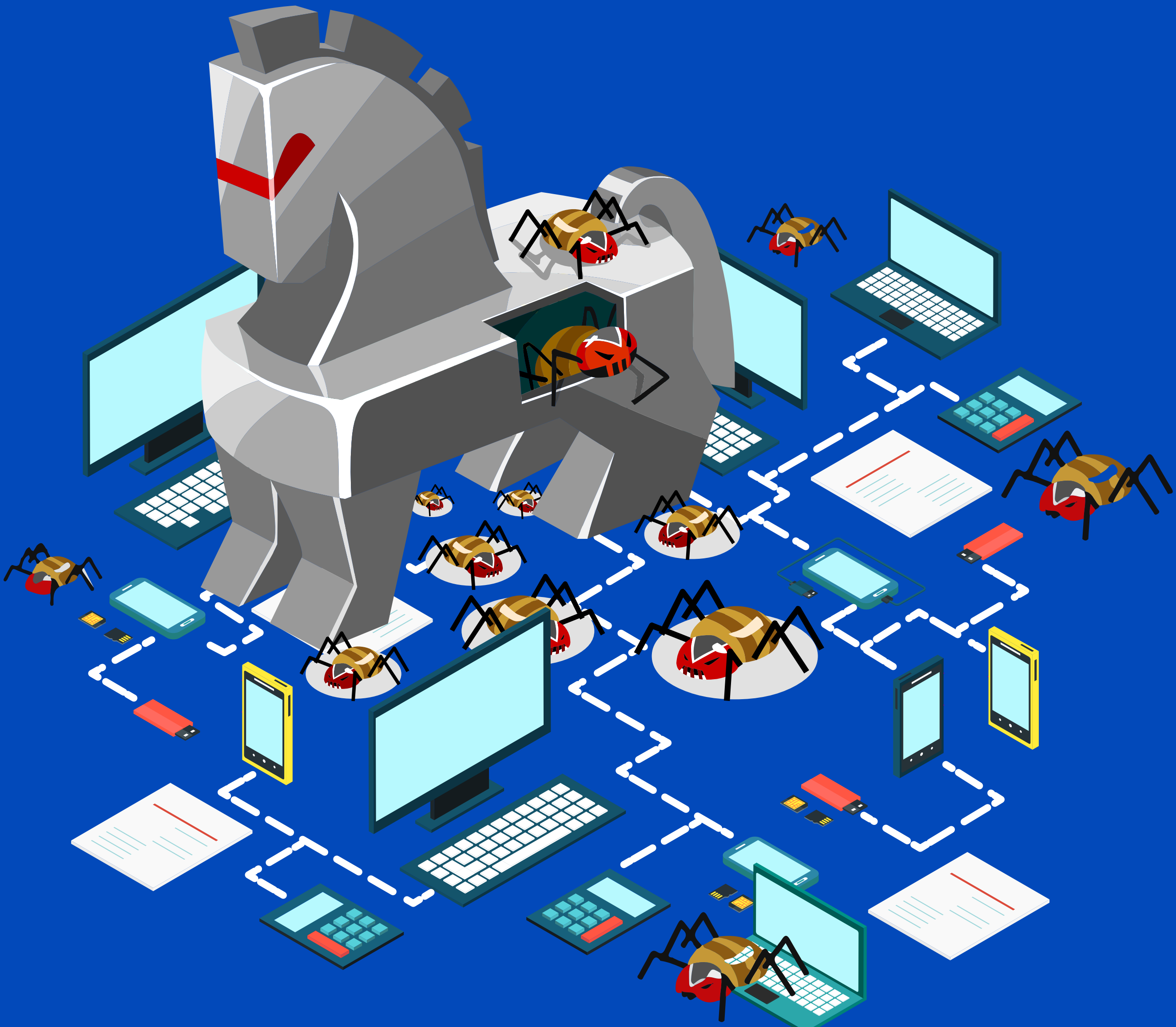
happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Botnet Filtering on ASA



Happiest People . Happiest Customers

Contents

Introduction

Implementing advance securities and following security improvement cycles on periodic basis have enabled industries, corporates offices and many organizations to avoid various kinds of attack that can harm them. Information trapping, attack on any server and a hacker tracking any particular PC’s activity inside an organization could lead to vital loss of information. . With increase in attacks like Virus, Man-in-Middle and hacker, it has become essential to have a precautionary security addition implemented.

From identity theft and fraud to corporate hacking attacks, few risks are as all-encompassing as ‘cyber threats’ nowadays. From being a matter of concern for the IT industry and security professionals it has reached the levels of a persistent business risk. Since the nature of these attacks and the impact is varied, it has become essential to invest in additional security measures.

This document explains one such new age attack that can have far reaching consequences and result in huge loss of data and henceforth the prevention steps.

Botnet Attack

A Botnet is a group of Internet-connected computers, each of which is maliciously taken over usually with the assistance of malware like Trojan Horses. Without the knowledge of the computers’ rightful owners, these machines are remotely controlled by an external source via standard network protocols, and often used for malicious purposes, most commonly for Distributed Denial-of-Service attack.

As with sophisticated cyber-attacks, there is no single defense that can protect an organization from a botnet attack. Bot infection includes downloading a program that is already virus infected, infecting systems via a worm or a drive-by infection is which an user can infect his or her system by just visiting a site.

The originator of a Botnet is commonly referred to as a "bot herder" or "bot master." This individual controls the Botnet remotely, often through an IRC server or a channel on a public IRC server – known as the command and control (C&C) server. Botnet servers mostly always communicate and cooperate with other Botnet servers, creating entire communities of Botnet’s, with individual or multiple bot masters. Botnet DDoS attacks are quickly becoming the most prevalent type of DDoS threats, growing rapidly in the past one year in both number and volume, according to a recent market research.

Threats involved from Botnet attacks

- **Distributed Denial-of-Service attack (DDoS)**
- **Adware**
- **Spyware**
- **E-Mail spam**
- **Click fraud**
- **Fast Flux**
- **Scareware**
- **Tracking victim's activity**

Prevention

Enterprises deploy multiple solutions based on their business and compliance requirements. Organizations over a period realized that deploying these solutions requires dedicated focus and deep expertise in the areas of Fault Monitoring tools, ITIL, ITSM tools, Cloud, Product Development, Solution Architecture, Integration, Application Development, and Support.

They have started outsourcing Network Monitoring to niche players like Happiest Minds who have rich expertise in building these solutions. Happiest Minds has been serving their clients using such a platform called iTaaS.

Cisco ASA

Adaptive Security Appliance is a Cisco proprietary firewall appliance device. ASA offers features like inspection, policing & prioritizing traffic, filters packet based on ACL's and Anti-X protection. The Anti-X features, enables us to configure botnet attack filter in Cisco ASA.

Botnet Filtering

Botnet attack filtering is termed as "Reputation based filtering". As preventive steps, Cisco has something called Security Intelligence Operation (SIO), where they have come up with a list of white and black listed IP/Domains across the world. These lists are stored in a database as per their reputations. Cisco ASA accesses the database, performing reputation based filtering to identify the hacker.

Cisco ASA Botnet filter components:

- **Dynamic and administrator blacklist data**
  The Botnet Traffic Filter uses a database of malicious domain names and IP addresses that is provided by Cisco Security Intelligence Operations. This database is maintained by Cisco Security Intelligence Operations and is downloaded dynamically from an update server. Administrators can also configure their own local blacklists and whitelists.
- **Traffic classification and reporting**
  Botnet Traffic Filter traffic classification is configured through the dynamic-filter. The dynamic filter compares the source and destination addresses of traffic against the IP addresses that have been reported for the various lists available (dynamic black, local white, local black) logs and reports the hits against the already maintained lists accordingly.
- **Domain Name System (DNS) snooping**
  In order to map IP addresses to domain names that are contained in the dynamic database or a local list, the Botnet Traffic Filter uses DNS snooping in conjunction with DNS inspection. Dynamic filter DNS snooping looks at User Datagram Protocol (UDP), DNS replies and builds a DNS reverse cache (DNSRC), which maps the IP addresses in those replies to the domain names they match. DNS snooping is configured via the Modular Policy Framework (MPF) policies

Traffic classifications:

Traffic that passes through the Botnet Traffic Filter is classified into four categories:

- **Blacklist:**
  This is traffic to or from an IP address that is considered to be malicious. This IP address can be either an IP address/network entry in the dynamic blacklist or administrator-configured blacklist or it can be a snooped IP address that was found in a DNS reply for a blacklisted domain.
- **Whitelist:**
  This is traffic to or from an IP address that is considered to be good. It is part of the administrator-configured lists.
- **Greylist:**
  A greylist IP address has been resolved to one or more blacklist entries as well as one or more unknown entries.

- **Unknown/None:**
An IP address that does not map to a domain in either a blacklist or whitelist, and no syslog's will be generated for this traffic.

Training ASA for Botnet Filtering

Overview

Enabling Adaptive Security Appliance to use Botnet Filtering requires a certain set of processes. Please remember, this feature works only with a license. The Cisco ASA appliance with the Botnet Traffic Filter should be deployed at the edge of the enterprise, as the botnet database contains information only about external botnets. It is also best to address the external threat as close to the source as possible. This feature is restricted to IPv4 traffic.

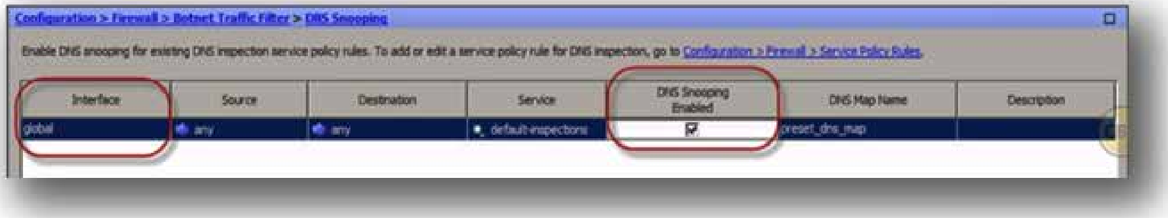
The Botnet Traffic Filter is supported in all firewall modes (single and multiple) and in routed and transparent modes.

Approach

- **Reachability:**
Cisco ASA Firewall must have valid Botnet Filtering license and have access to Cisco's Security Intelligence Operation (CSIO) dynamic database, which is in the internet. This is essential as Botnet Filtering features would communicate with CSIO dynamic database and verify with its White & Black listed database.

- **Enable DNS:**
DNS is required on ASA primarily for two reasons -
  - To make sure the ASA is capable of resolving the Cisco Security Intelligence Operations server IP
  - Allow to have a static whitelist site, even if the site is blacklisted

- **DNS Snooping:**
The Dynamic Filter DNS snooping feature looks at UDP DNS replies and builds a DNSRC that maps the IP addresses in those replies to the domain names they match.
  - DNS snooping should only be enabled for DNS traffic. Failure to do so will result in non-DNS traffic being dropped because it is not
  - adhering to the DNS protocol. DNS snooping should only be enabled for the interface that is facing the Internet, since the Botnet Traffic Filter database is aimed at addressing the external threat of botnets.



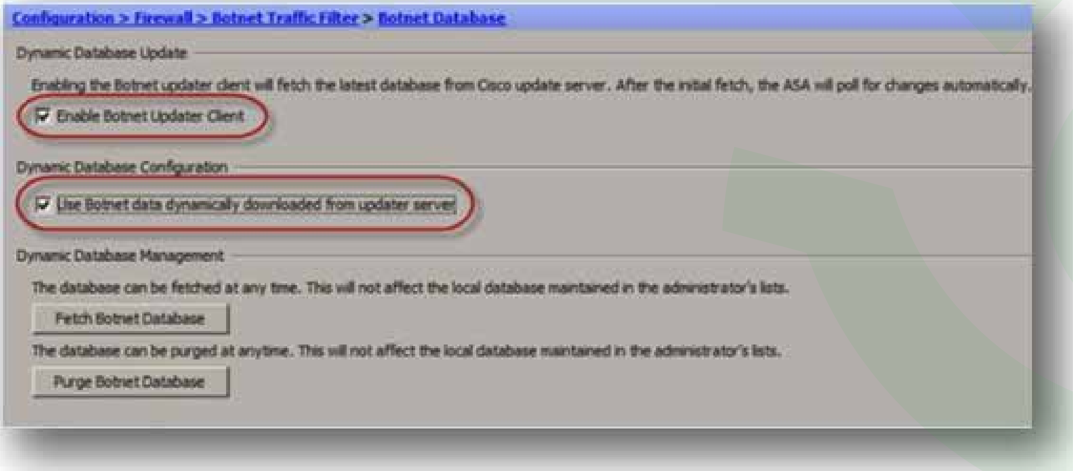
Configuration > Firewall > Botnet Traffic Filter > DNS Snooping

Enable DNS snooping for existing DNS inspection service policy rules. To add or edit a service policy rule for DNS inspection, go to Configuration > Firewall > Service Policy Rules.

Interface	Source	Destination	Service	DNS Snooping Enabled	DNS Map Name	Description
global	any	any	default-inspections	☑	preset_dns_map	

Enabling DNS Snooping

- **Enable ASA Client:**
Enabling ASA for being a client, this will download all dynamic databases from SIO and then make decision based on the downloaded dynamic database. Failing this setting, ASA will not have an updated database to verify with.



Configuration > Firewall > Botnet Traffic Filter > Botnet Database

Dynamic Database Update

Enabling the Botnet updater client will fetch the latest database from Cisco update server. After the initial fetch, the ASA will poll for changes automatically.

☑ Enable Botnet Updater Client

Dynamic Database Configuration

☑ Use Botnet data dynamically downloaded from updater server

Dynamic Database Management

The database can be fetched at any time. This will not affect the local database maintained in the administrator's lists.

The database can be purged at anytime. This will not affect the local database maintained in the administrator's lists.

Impact of Botnet Filtering

Post implementing the entire process of Botnet Filtering, there is a high chance that, Botnet Filtering can drop some websites which are most commonly used for business needs. Thus it is mandatory for us to get an analysis done post the implementation.

- Infrastructure analysis
- Scheduling a downtime
- Run a pilot test
- Recovery action

Infrastructure Analysis

Prior to considering implementing Botnet filtering on ASA devices, it is critical to analyze the execution process. One must consider executing this change in a set of batches, in case of multiple sites. The most essential part is to have the list ready before moving to the executing phase.

Scheduling a downtime

The whole idea of having a step by step execution is to mitigate the errors and large scale impact on users. The implementation must be followed on a priorly discussed scheduled date, keeping the end user updated about the change and its expected affect. Failing this would lead to loss of business activity.

Run a pilot test

The idea of having a pilot test is to know the problems you might encounter when Botnet filtering is enabled on the ASA and how to prevent and solve them. Therefore, you should expect and even welcome problems during the pilot run. A pilot must be large enough to capture a representative sample of the issues that can be expected. It should check if the attack prevents its implementation on multiple branch offices.

Recovery Action

Cisco Security Intelligent Operations (CSIO) has the list of updated botnet hackers collected across the globe. It includes websites of various risk levels – low to medium to high. There is a possibility that some websites which one may need for business is also in the list of CSIO database hence get blocked. It is the administrator’s responsibility to analyze the risk factor of any given website with their respective infrastructure security team. This will enable one to decide if the website can be added under static whitelist if it is important for a business.

Summary

The Cisco ASA Botnet Traffic Filter is an effective tool that enterprises can use to gain insights in one of today's leading threats. In conjunction with accurate threat data provided by Cisco Security Intelligence Operations and Cisco Global Correlation for IPS, the Botnet Traffic Filter offers an industry-leading solution to combat modern botnet threats in a dynamic business environment.

About the Author

Mohan Alagar

6.1 years of IT experience, Including 4years of Networking Security technologies and 3 years of Novell Technologies. Skill set are Juniper Firewalls, Cisco ASA, Cisco Routers and Switches, Cloud Websense Proxy, Novell eDirectory, Novell ZENworks, iPrint, Identity Manager, and SuSE Linux. Roles that I have worked includes Juniper TAC, Novell Technical Support, Technical Solution Rep II and Senior Engineer. Past Key projects include - Managing, Troubleshooting and fixing issue on Production Environment to Global Customers of Juniper and Novell Technologies. I have published several Techincal Information Document (TID) for Novell. I am Certified - Juniper Networks Certified Intenet Specialist (JNCIS-FWV), Cisco Certified Network Associate - SecurityCCNA-Security), Cisco Certified Network Associate - Routing and Switching (CCNA R&S).

Happiest Minds