
Threat **STOP**™

Internet.Security.Community

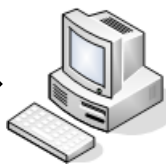
We're BACK!

Tom Byrnes
Founder & CEO
760.402.3999
tomb@threatstop.com

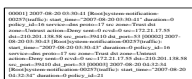
Manual Processes

ENFORCEMENT TOOLS

Host System Security



Auditing



Router Security



Firewalls



Intrusion Detection System



Incident Response System



Threat **STOP**TM
Adaptive Real-Time Security

ThreatSTOP Automates Process Like Anti-Virus Auto-Update, but in Real-Time

GOOD GUYS WITH THREAT INFO

Internet Storm Center - DShield

Shadowserver

SRI MTC

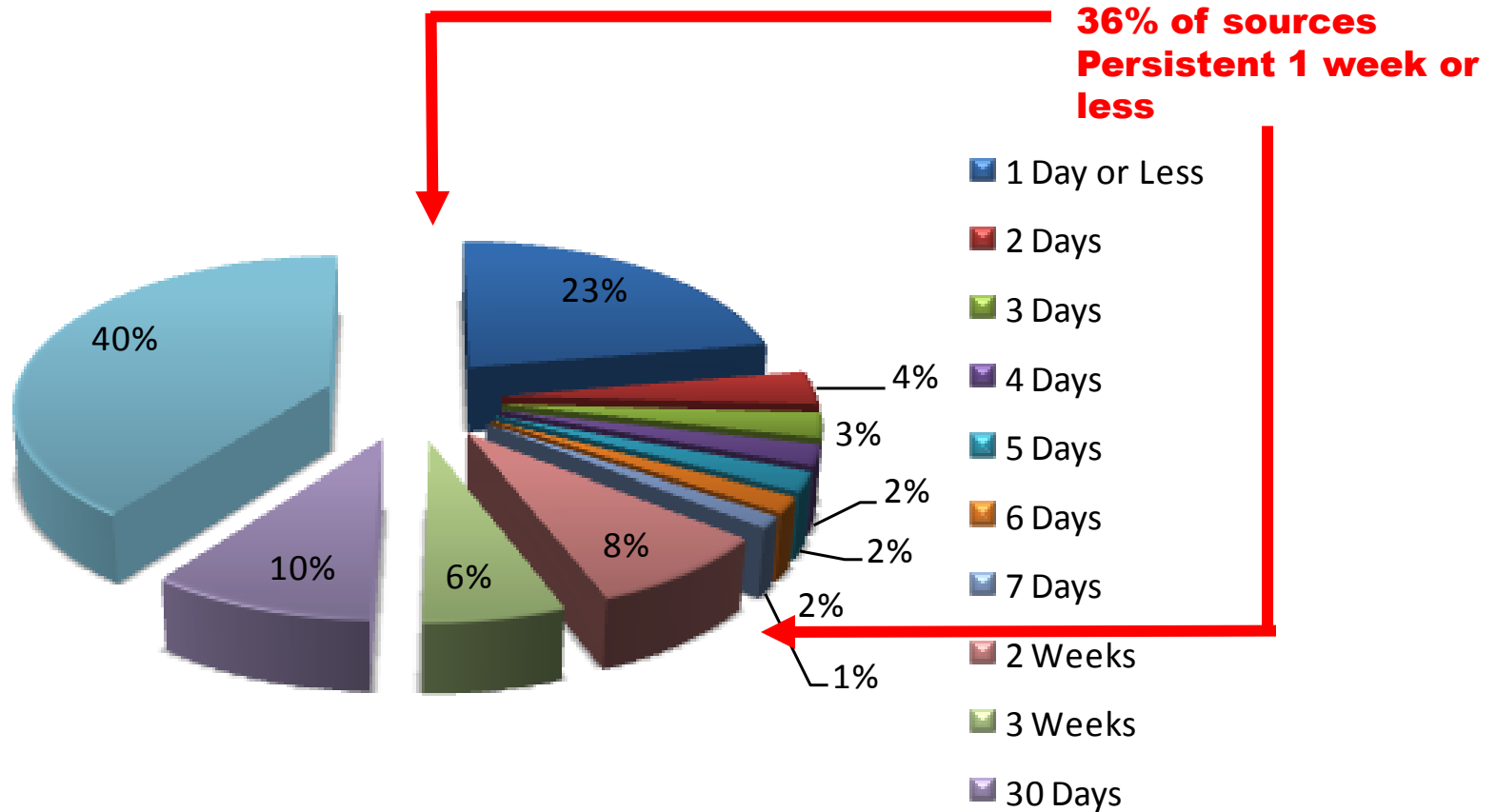
Cymru Bogons

PhishTank

DROP Advisory Null List

Malware Block List

Threats Change Rapidly

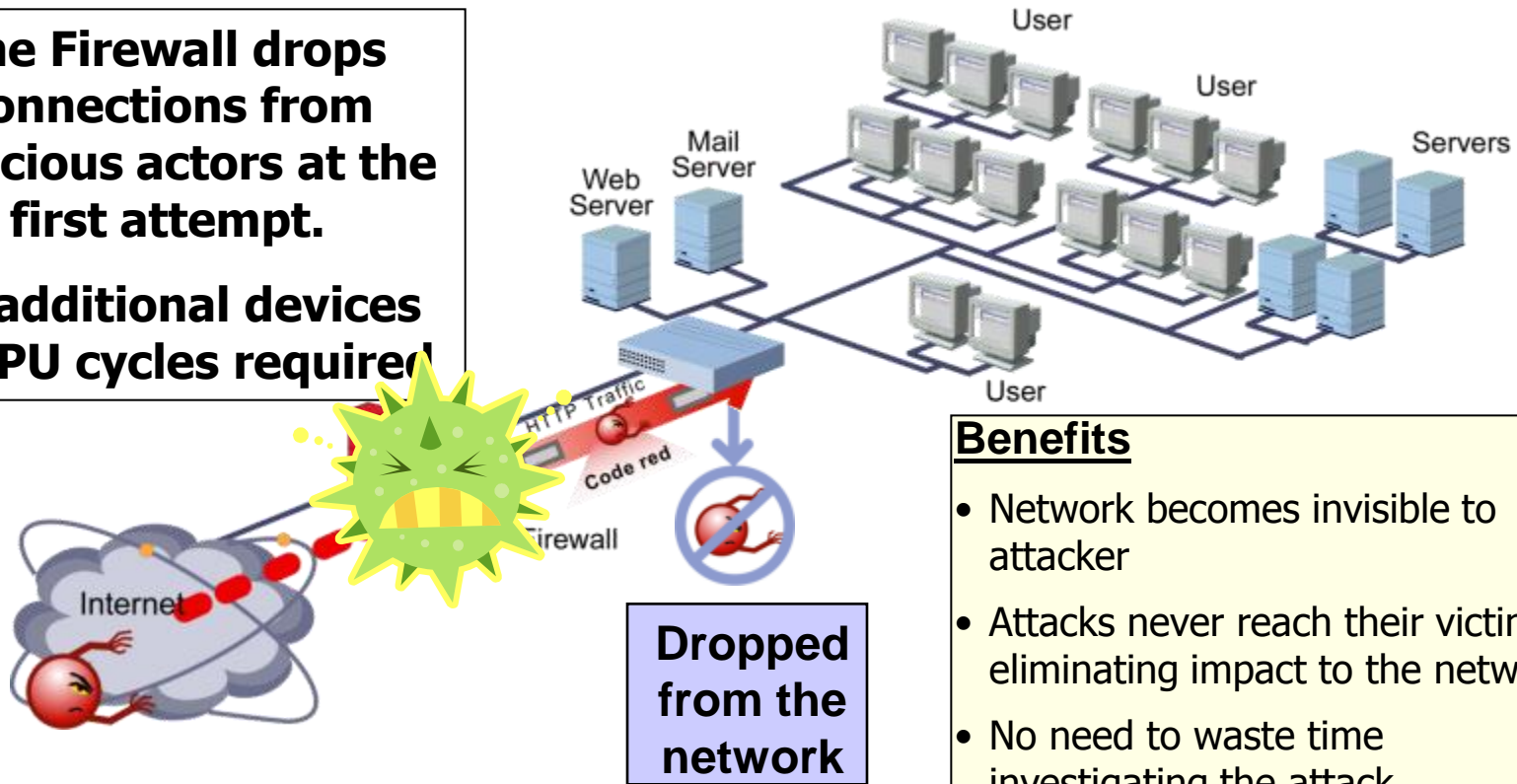


Source: SANS - Internet Storm Center, DShield top 10,000 sources, 9/17/2009

Drop At first SYN

The Firewall drops connections from malicious actors at the first attempt.

No additional devices or CPU cycles required

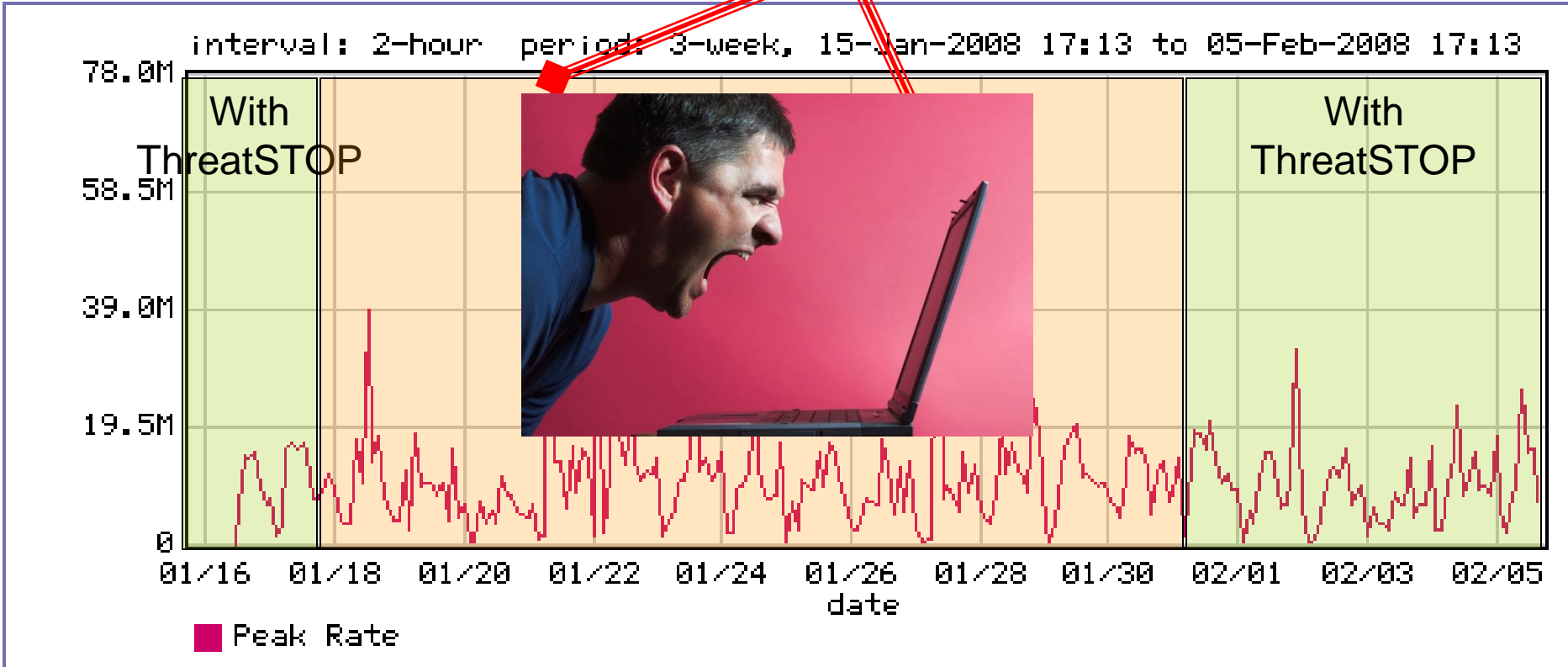


Benefits

- Network becomes invisible to attacker
- Attacks never reach their victim, eliminating impact to the network
- No need to waste time investigating the attack
- Works for all traffic (IP, TCP, UDP, etc.)
- Drops only traffic from known bad actors

SMTP Traffic Test

Bandwidth saturated by SMTP



ThreatSTOP Automation

Welcome Threat Stop (threatstop@threatstop.com) | [Sign Out](#)

[Home](#) | [Devices](#) | [User-Defined Lists](#) | [Log Submission](#) | [Reporting](#) | [My Account](#) | [Help](#)

My ThreatSTOP

My ThreatSTOP plan ThreatSTOP Enterprise - 30 Devices	Current Protection 3 devices 1 user allow list 1 user block list	Latest threat update 0 h 26 min ago on 08/24/2007 at 08:01AM PST
---	--	--

Devices

These are the devices that are currently configured.

Number	Nickname	Manufac	IP Address
1 of 30		iptables	214.28.94.1
2 of 30		Cisco	214.28.94.128
3 of 30		Netscre	214.28.95.100

[Manage Devices](#)

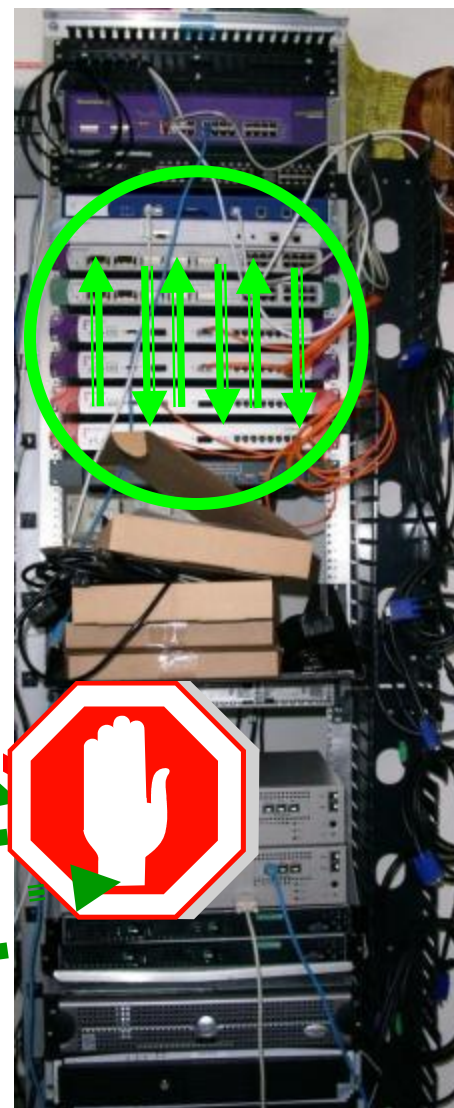
User-Defined Lists

Here are the custom lists that are configured.

User Allow Lists	# of IP Addr	Mem R
MyNet	256	0.1228 MB

User Block Lists	# of IP Addr	Mem R
	64	0.1185 MB

[Manage User-Defined Lists](#)



Firewall Report - Stopped Inbound Attacks for All devices

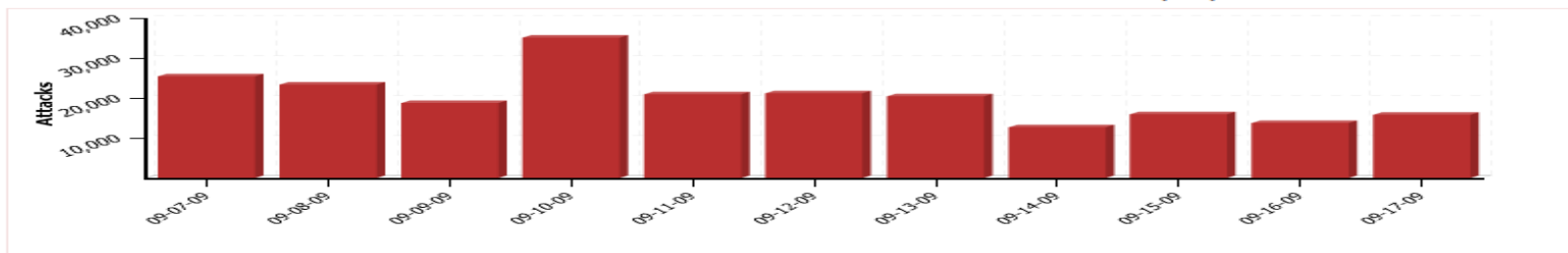
Please select the device and dates you would like to view. The report only shows connections to and from addresses that are in our block lists. We do not plan to process any logs submitted before 2008. If you would like the logs that were submitted before 2008 available, please contact us.

From:  To: 

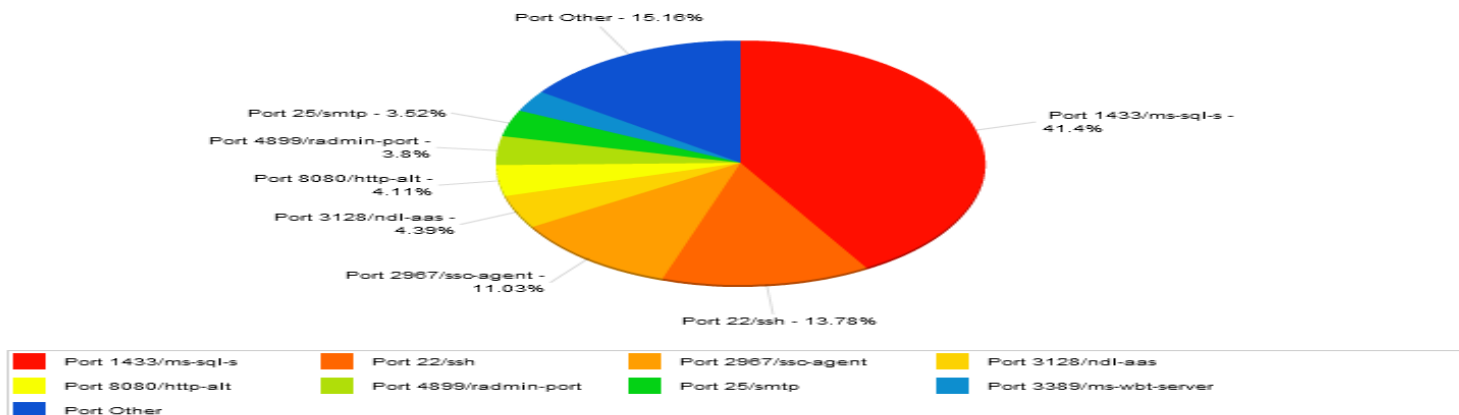
Devices: Report:

Number of attacks : 223526
Number of attackers : 424

Attack Frequency : 20321 per day
Last log file processed on:
09/18/2009



[Stopped Inbound Attacks >](#)
[Stopped Outbound Trojan Connections >](#)
[Attacked Services :](#)



[Stopped Inbound Attacks - Attacked Ports >](#)
[Stopped Outbound Trojan Connections - Destination Ports >](#)

Current Product

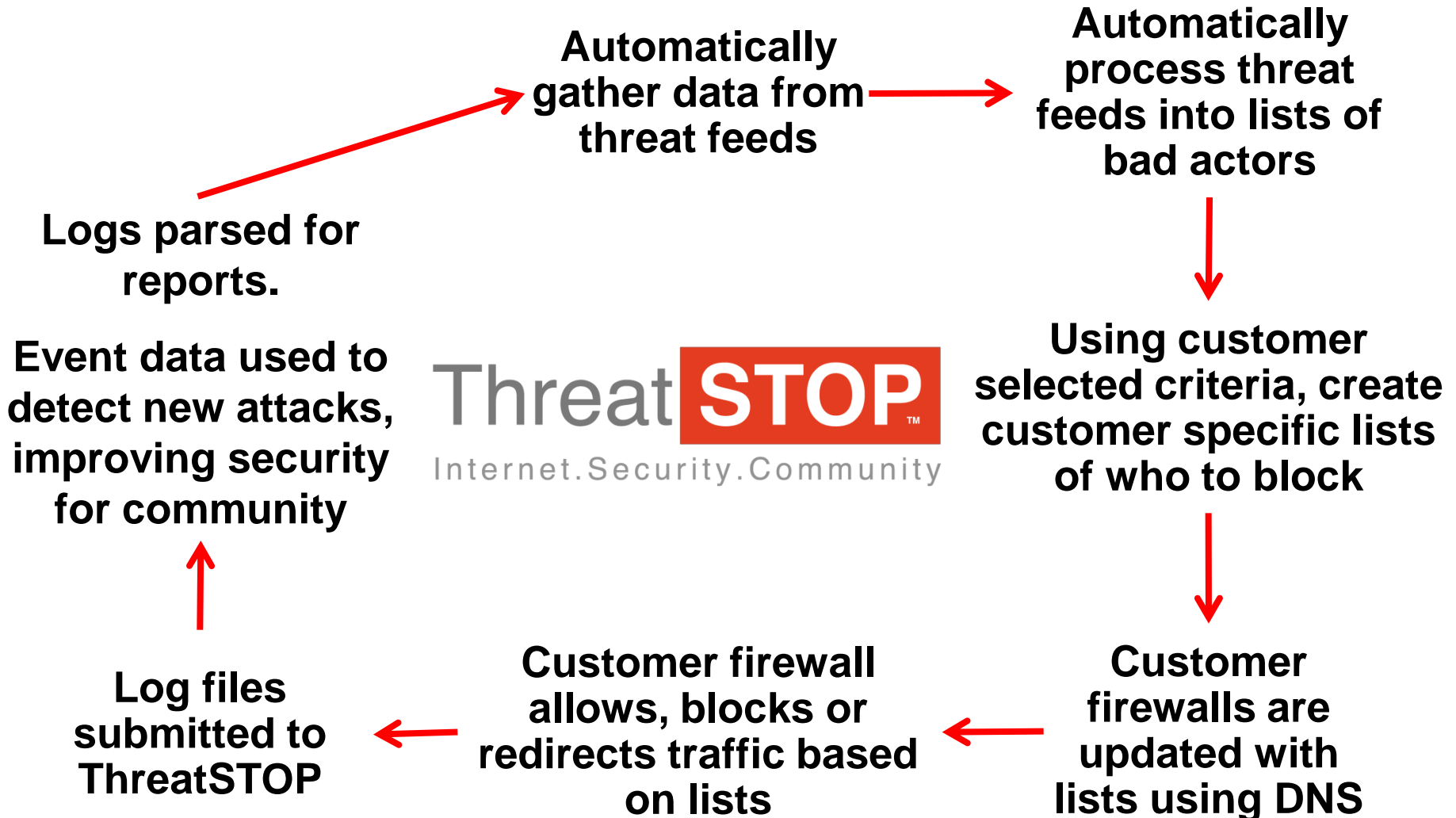
Supported Firewalls

- BSD/Solaris/SYSVR4/pf
- Checkpoint
- IPTables
- JunOS w Enhanced Services
- Netscreen ScreenOS 5 & 6
- PIX/ASA
- ZoneAlarm

Data Sources

Feed	Threat Profile
DShield	Network based attacks, worms, botnets
Emergency	Latest detected threat:iFrames, Worms, Malware hosts
SSH Crackers	Password brute forcers/cracking
Shadowserver	Botnet C&C hosts
PhishTank	Active phishing sites
Cyber-TA	Malware droppers, C&Cs, Fast-Flux botnets
Bogons	DOS (Inc self-DOS, by blocking ranges that used to be bogon, but are now assigned)
Malware Hosts	Site that have been detected as hosting malware
Spyware, browser hijackers	Spyware and browser hijacking hosts
SpamHAUS DROP	Worst networks as identified by SpamHAUS, hijacked CIDRs, netblocks of crime syndicates
Geographic	Netblocks by country. About 98% accurate

Community ↑ Security



Who Are We?

- **Tom Byrnes - Founder & CEO**
- Security experience spans 25+ years of civilian & military
 - Radware, iPivot, Zero Gravity, ADN, Datatech, U.S. Army
- **VP Engineering – Boris Veksler (Betria Consulting)**
 - 15+ years experience in project management & engineering
 - Tradebeam, Struxicon, Johnson Controls, Neiman Marcus, Tyco
 - MBA from Anderson School at UCLA; MS in Structural Analysis & Mathematics/Computer Science from St. Petersburg Technical Univ.
- **VP Customer Experience (QA & Operations) – David Daugherty**
 - Operations in e-commerce platforms: Virtual Dreams, ArtistDirect
 - Test and QA: iPivot, Intel and ADN
- **Paul Mockapetris – Advisor**
 - Inventor of the Domain Name System (DNS)
 - Currently the Chief Scientist and Chairman of Nominum, Inc.
- **Marcus H. Sachs, P.E. – Advisor**
 - Verizon Exec. Dir. of Gov. Affairs for National Security Policy
 - First head of Cybersecurity @ DHS
 - Director of the SANS Internet Storm Center
- **Johannes Ullrich - Advisor**
 - Chief Research Officer for the SANS Institute
 - Founded DShield.org

Summary

- Internet Service - ThreatSTOP is everywhere.
- Works with any traffic management system that has a DNS resolver.
- Makes existing systems work better
- Increases capacity/reclaims lost bandwidth
- Virtuous Cycle: All Users contribute to the Community enhancing Security for everyone
- Pull, not push: Non Intrusive / Secure
- Web Based Management and reporting
- Easy to Implement and Use
- Cost effective: Saves hardware/software and staff time

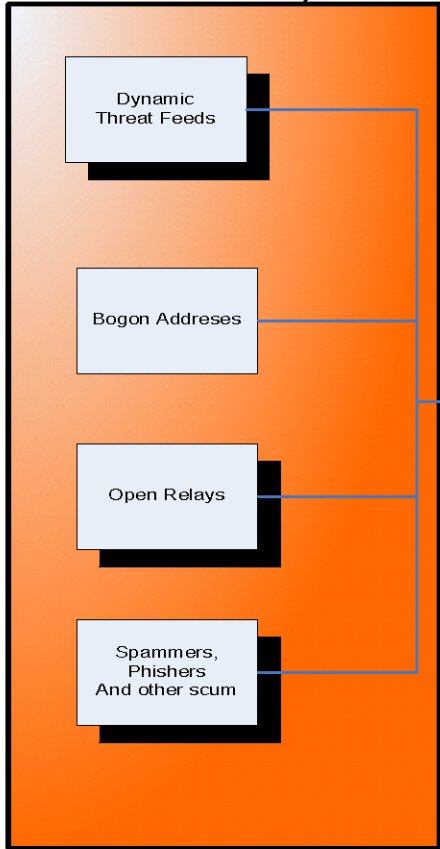
Subscribe/Contact

- www.threatstop.com
- info@threatstop.com
- +1-858-412-7334
- Tom Byrnes: tomb@threatstop.com

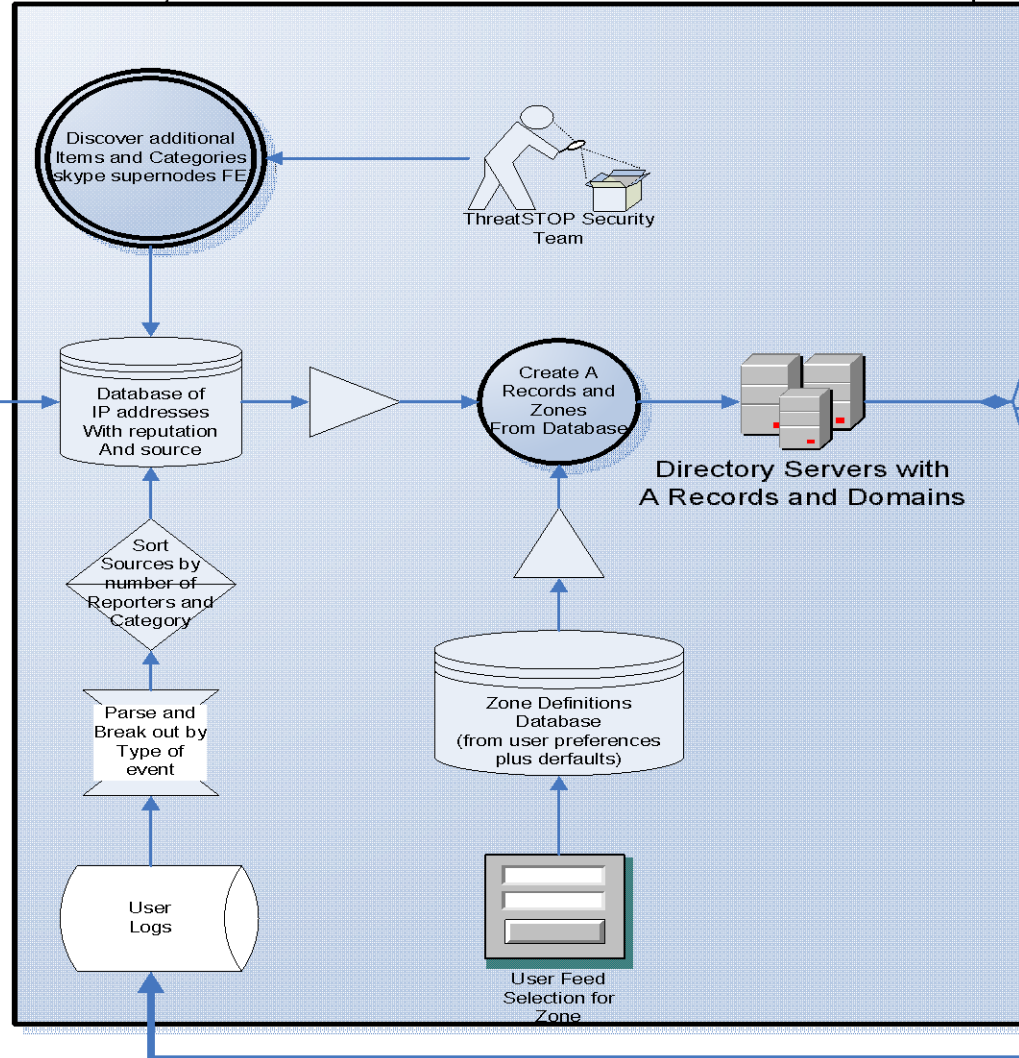
Backup Slides

Service Architecture

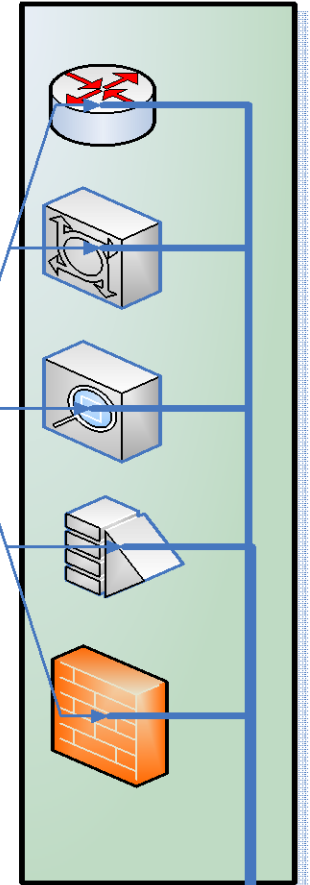
External Data Sources Threat and Vulnerability Feeds



Threatstop Processes and Data Sources Collate, sort and filter Feeds to Produce Generic and custom Lookups



Customers use DNS Queries in Rules



DESCRIPTION	ThreatSTOP Basic System Design
DRAWN BY	TOM BYRNES
DATE	6/17/2006

Configure your lists

[Home](#) | [Devices](#) | [User-Defined Lists](#) | [Log Submission](#) | [Reporting](#) | [My Account](#) | [Help](#)

User-Defined Lists

Here you can configure your own lists. You can use these to create white lists for use on your firewalls. It can be used to either implement a "Deny all except..." security policy, or "No matter what, I need to talk to..." one. Other applications of this are an IP based Closed User Group (poor mans VPN) or special traffic handling such as IP wiretapping.

User Allow Lists	# of IP Address	RAM Requirements	Actions
MyNet	256	0.1228 MB	Edit Delete
			Add List
User Block Lists	# of IP Address	RAM Requirements	Actions
AttackMe	64	0.1185 MB	Edit Delete
			Add List

[Privacy Policy](#) | [Terms of Service](#) | [Contact Us](#)

Copyright © 2007 ThreatSTOP/DISS, Inc. All rights reserved.

Configure your Devices

[Home](#) | [Devices](#) | [User-Defined Lists](#) | [Log Submission](#) | [Reporting](#) | [My Account](#) | [Help](#)

Device Configuration

Here you would configure your device and select the lists that you want to use. Enter a nickname to give the device so it is easy for you to recognize. The nickname is limited to 10 characters. The IP address must be the public or outside IP address of the device. Our DNS servers will not answer queries coming from a different address than the one you enter.

If your firewall or model is not listed, please use the "Other" option and fill in the text box with some detail about which firewall you are using.

(Please note all fields marked with * are required)

#	Nickname *	Manufacturer *	Model *	IP Address *
1 of 30	<input type="text"/>	<input type="text" value="iptables"/>	<input type="text" value="Linux"/>	<input type="text" value="214.28.94.1"/>
	Location of Device <input type="text" value="United States"/>			Postal Code <input type="text" value="92620"/>

Configure ThreatSTOP Protection For This Device

ThreatSTOP Block Lists

Select the lists you want to assign to this device.

	# of IPs	Device RAM Requirements
<input type="checkbox"/> Bot Blocker - Top Ten This blocker is an aggregation of DShield Top 10 and proprietary ThreatSTOP bot lists	20	0.0003 MB
<input type="checkbox"/> Bot Blocker - Top 4000 This blocker is an aggregation of DShield Top 4000 and proprietary ThreatSTOP bot lists	4000	0.0076 MB
<input type="checkbox"/> Bot Blocker - Full This blocker is an aggregation of DShield Top 10, DShield Block, TQM Top 10, and proprietary ThreatSTOP bot lists	5140	0.0125 MB
<input type="checkbox"/> Spam Blocker - Top Ten This blocker is an aggregation of TQM Dirty Dozen and proprietary ThreatSTOP aggregate lists	2560	0.0151 MB
<input type="checkbox"/> Spam Blocker - Full This blocker is an aggregation of TQM Dirty Dozen and proprietary ThreatSTOP aggregate lists expanded to cover last 24 hours of spam activity	2560	0.0151 MB
<input type="checkbox"/> Fraud Blocker - Top Ten This blocker is an aggregation of TQM Dirty Dozen over last week and proprietary ThreatSTOP phishing lists	2560	0.0151 MB
<input type="checkbox"/> Fraud Blocker - Full This blocker is an aggregation of Hijacked IPs and proprietary ThreatSTOP phishing lists	4096	0.0102 MB

User-Defined Block Lists Available

If you have any custom lists you want to include, select them here. Block lists will have a "b" in the name - device-001b.account.threatstop.local.

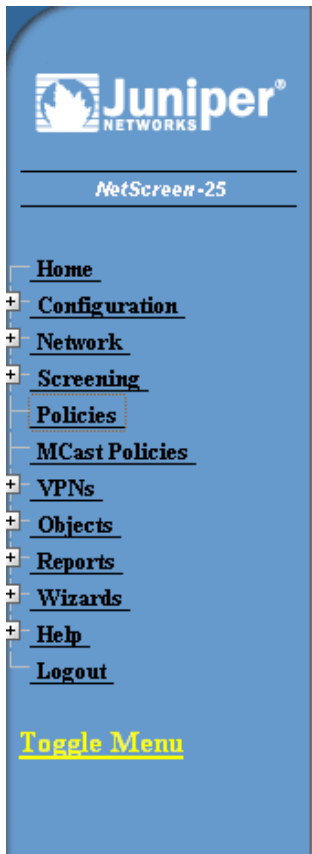
	# of IPs	Device RAM Requirements
<input type="checkbox"/> AttackMe	64	0.1185 MB

User-Defined Allow Lists Available

Allow lists will have an "a" in the name - device-001a.account.threatstop.local.

Easy to Use & Configure

➤ Just add two simple rules to existing firewalls






Juniper NETWORKS
NetScreen-25




- Home
- Configuration
- Network
- Screening
- Policies**
- MCast Policies
- VPNs
- Objects
- Reports
- Wizards
- Help
- Logout

[Toggle Menu](#)

From Untrust To Trust, total policy: 6

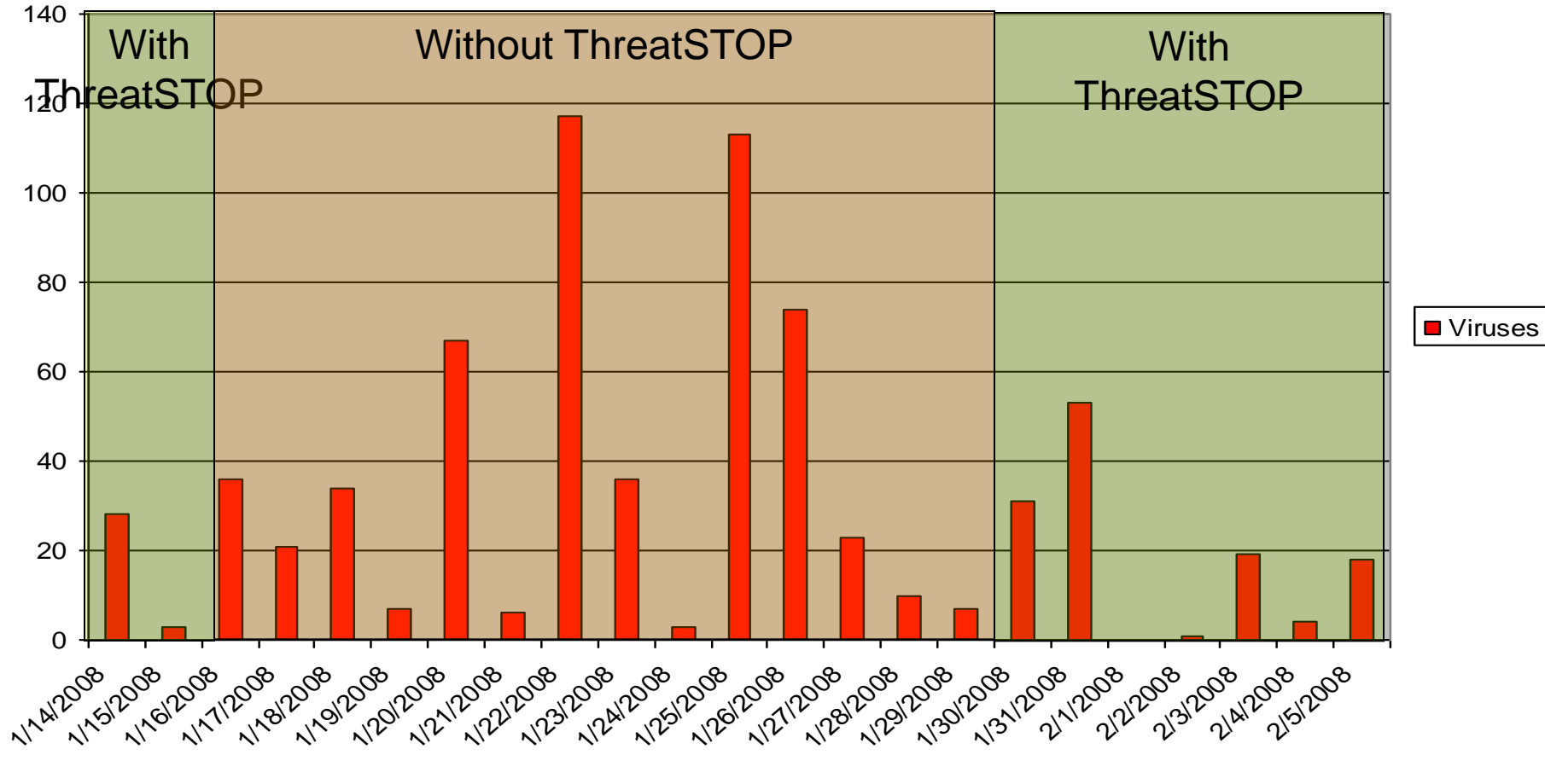
ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
19	Block	Any	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	

From Trust To Untrust, total policy: 3

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
16	Any	Block	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	

Viruses (detected by Sophos)

Viruses



Blocked Traffic

