



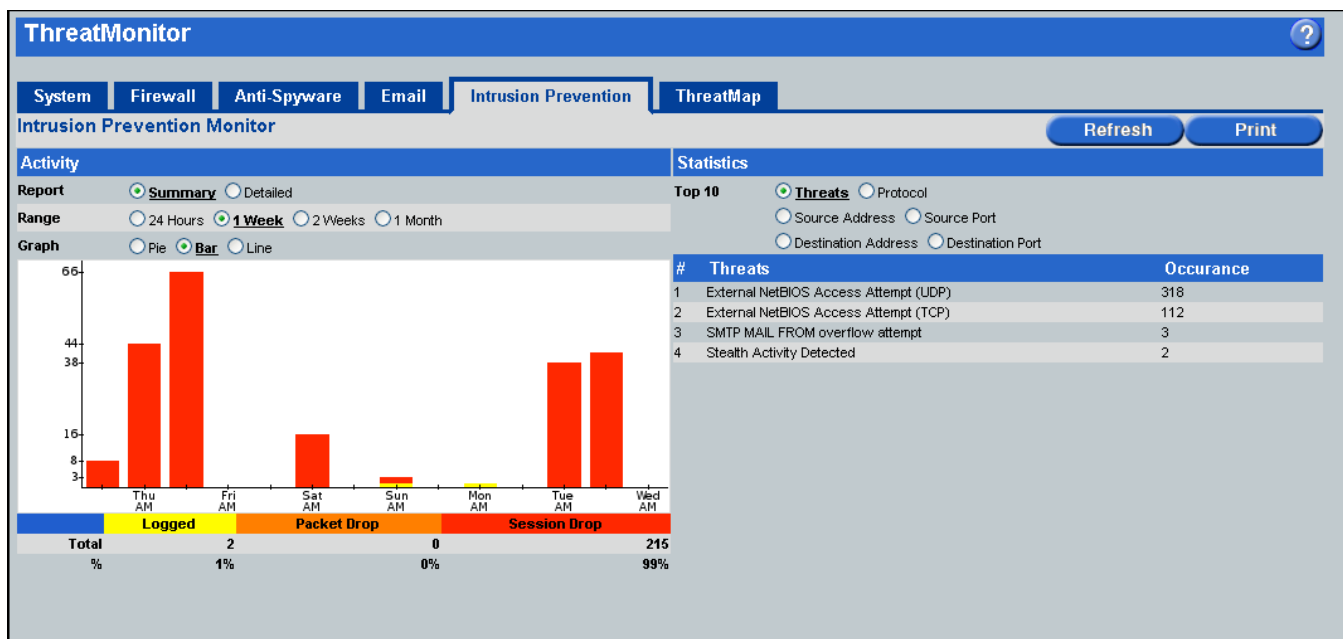
# **eSoft Intrusion Prevention SoftPak Training Guide**

**version 1.0 October 1, 2006**

# 1 INTRUSION PREVENTION SOFTPAK

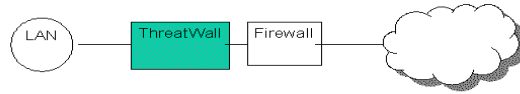
## 1.1 Intrusion Prevention SoftPak Overview

The Intrusion Prevention SoftPak Inspects all traffic passing through or past it for known exploits of many types. It is the “deep packet inspection” technology that allows the ThreatWall to stop malicious activity in traffic that is otherwise invisible to a traditional layer two firewall. This is accomplished by inspecting full packets in real time, not just the header information that a stateful inspection firewall does. IPS is a critical feature that allows the system to block and report on potentially damaging activity.



## 1.2 Intrusion Prevention SoftPak Configuration Options

When enabled, the IPS softPak will only “see” traffic that passes to or through its interfaces. The most common installation of the ThreatWall would be to place it immediately behind the existing firewall, but it could be placed at the edge of any network segment that you want to protect. It will inspect traffic for most frequently used Internet protocols such as HTTP, SMTP, and FTP for specific exploits. All blocking activity will be done by the ThreatWall itself, so there is no requirement for compatibility with an existing firewall product.



### 1.3 Intrusion Prevention Basic Settings

IPS will create a default setting of action profiles containing active rules based on the configuration settings found on this page

**Intrusion Prevention: Settings** Need More Help?

---

**Intrusion Prevention Settings**

Intrusion Prevention  Enabled

**Protected Networks**

Protected Networks  
*Enter the IP addresses and networks that are being protected in the form 192.168.100.0/24*

10.10.0.0/16  
 10.10.0.18/19

Protected Computers  
*Check a box for each operating system that is running on the network being protected.*

Microsoft  
 Apple Macintosh  
 Linux  
 Misc—Cisco, Sun, SCO, etc.

**Web Servers**

Web Server Protection  Enabled

Public Web Server IP Addresses  
*Enter the IP address(es) of your local web servers. Note: if a server has a private IP address, that address should be used.*

10.10.54.117

Web Server Software  
 Mixed

**Mail Servers**

Mail Server Protection  Enabled

Public Mail Server IP Addresses  
*Enter the IP address(es) of your local mail servers. Note: if a server has a private IP address, that address should be used.*

10.10.54.117

**Network Policies**

Block Instant Messenger Traffic  Enabled  
*AIM, ICQ, MSN, IRC, Yahoo, and more*

Block Peer-To-Peer File Sharing Traffic  Enabled  
*GNUtella, Kazaa, Napster, BitTorrent, and more*

**Responsiveness**

Block Intruders  
*This determines the actions for the default set of Action Profiles.*

Aggressive — Log alerts and block all attacks  
 Normal — Log alerts and block some attacks  
 Passive — Only log alerts

**Apply** **Cancel**

#### 1.3.1 Protected Networks

Enter the IP or networks that are to be considered “trusted” by the ThreatWall- enter as many as are applicable. ThreatWall will use this information to determine what to scan and what not to scan based on where it is originating to and where it is going. Activity must be bound from an untrusted network to a trusted network to be acted upon; otherwise it has no way to determine what is untrusted.

Check all the types of computer operating systems are found on your trusted networks. Any system that is not specified will NOT be protected.

### **1.3.2 Web Servers**

Enable this option to protect against specific threats targeted at Web Servers that might exist on the protected networks. Specify location by IP address and Web server software that is running.

### **1.3.3 Mail Servers**

Enable this option to protect against specific threats targeted at Mail Servers that might exist on the protected networks. Specify location by IP address

### **1.3.4 Network Policies**

Enable this option to block Instant Messaging (IM) activity and or Peer to Peer (P2P) applications. ThreatWall will block all activity based on type without regard to the user. You do have an option to allow some types of IM or P2P if desired.

### **1.3.5 Responsiveness**

This setting determines how aggressive the system will be when it sees threats. The default setting is to log alerts and block some attacks. If set as aggressive, all attacks would be blocked.

## **1.4 Alert viewer**

---

This is the master console for viewing all of the current activity that has been seen by the system. It will report on all activity that has matched a rule in the active rule base. This event has already been acted on (or not) depending on the system settings. It also allows the administrator to mark an event as a false positive for feedback to the system- enough false positives (see action profiles) and the rule will be disabled. Events will be displayed as they are seen. If multiple occurrences of the same type of exploit are seen, it will be reported once, mentioning additional occurrences. A new event would be generated after a different exploit is seen.

Intrusion Prevention: Alert Viewer						
Time	Alert	Protocol	Source	Destination	FP?	
<i>If you are sure that a logged event was innocent and not something malicious, then it is a false positive. Put a checkmark next to any entry that is a false positive.</i>						
*Aug 15 08:56:30	SMTP MAIL FROM overflow attempt	TCP	192.168.5.126 Port: 1363	10.10.10.4 Port: smtp	<input type="checkbox"/>	
*Aug 15 10:54:23	SMTP MAIL FROM overflow attempt <i>Repeated 2 times</i>				<input type="checkbox"/>	
*Aug 15 10:54:23	External NetBIOS Access Attempt (TCP)	TCP	192.168.5.11 Port: 1028	10.10.100.1 Port: 445	<input type="checkbox"/>	
*Aug 15 10:54:26	External NetBIOS Access Attempt (UDP)	UDP	192.168.5.11 Port: netbios-ns	10.10.100.1 Port: netbios-ns	<input type="checkbox"/>	
*Aug 15 10:55:22	External NetBIOS Access Attempt (UDP) <i>Repeated 2 times</i>				<input type="checkbox"/>	
*Aug 15 10:55:22	External NetBIOS Access Attempt (TCP)	TCP	192.168.5.11 Port: 1042	10.10.100.1 Port: 445	<input type="checkbox"/>	
*Aug 15 10:55:24	External NetBIOS Access Attempt (UDP)	UDP	192.168.5.11 Port: netbios-ns	10.10.100.1 Port: netbios-ns	<input type="checkbox"/>	
*Aug 15 10:55:42	External NetBIOS Access Attempt (UDP) <i>Repeated 2 times</i>				<input type="checkbox"/>	
*Aug 15 10:55:42	External NetBIOS Access Attempt (TCP)	TCP	192.168.5.11 Port: 1044	10.10.100.1 Port: 445	<input type="checkbox"/>	
*Aug 15 10:55:44	External NetBIOS Access Attempt (UDP)	UDP	192.168.5.11 Port: netbios-ns	10.10.100.1 Port: netbios-ns	<input type="checkbox"/>	
*Aug 15 11:52:55	External NetBIOS Access Attempt (UDP) <i>Repeated 2 times</i>				<input type="checkbox"/>	
*Aug 15 11:52:55	External NetBIOS Access Attempt (TCP)	TCP	192.168.5.11 Port: 1271	10.10.100.1 Port: 445	<input type="checkbox"/>	
*Aug 15 11:52:57	External NetBIOS Access Attempt (UDP)	UDP	192.168.5.11 Port: netbios-ns	10.10.100.1 Port: netbios-ns	<input type="checkbox"/>	
*Aug 15 11:54:31	External NetBIOS Access Attempt (UDP) <i>Repeated 2 times</i>				<input type="checkbox"/>	
*Aug 15 11:54:31	External NetBIOS Access Attempt (TCP)	TCP	192.168.5.11 Port: 1281	10.10.100.1 Port: 445	<input type="checkbox"/>	
*Aug 15 11:54:34	External NetBIOS Access Attempt (UDP)	UDP	192.168.5.11 Port: netbios-ns	10.10.100.1 Port: netbios-ns	<input type="checkbox"/>	
*Aug 15 11:54:55	External NetBIOS Access Attempt (UDP) <i>Repeated 2 times</i>				<input type="checkbox"/>	
*Aug 15 11:54:55	External NetBIOS Access Attempt (TCP)	TCP	192.168.5.11 Port: 1283	10.10.100.1 Port: 445	<input type="checkbox"/>	
*Aug 15 11:54:57	External NetBIOS Access Attempt (UDP)	UDP	192.168.5.11 Port: netbios-ns	10.10.100.1 Port: netbios-ns	<input type="checkbox"/>	

## 1.5 Rule Manager

---

Rule Manager allows you to view all of the rules available in the system categorized by their action profile. Clicking on the category will allow you to see all of the individual rules and more detailed information regarding each one. Links exist for more research on each.

## 1.6 Action Profiles

---

Action Profiles define the action (or inaction) taken on each rule once matched. There are several default action profiles that have been created by eSoft and rules associated with those profiles- they include High Priority attacks, Web server attacks, Attempted denial of service, etc.

Each Action Profile uses various criteria to define the action. For example-

**High Priority Attacks-** This Action profile includes rules which are considered to be of the highest priority, are classified as an Attack and can be targeted for any defined operating system. The default action will be to log the event and drop the connection.

**Attempted Intrusion-** This action profile uses the category criteria which defines specific behaviors- attempted administrator privilege gain and attempted user privilege gain. It's considered an attack, against all defined operating systems and will be logged with connection dropped.

Both Action profiles above result in the same action, but one is much more specific to the type of attack.

Action Profile	Action	Move
<i>The Action Profiles are ordered by importance so that a rule that satisfies two Action Profiles is only associated with one of them. The higher priority Action Profile takes precedence.</i>		
<input checked="" type="radio"/> High Priority Attacks	Log + Drop Connection	↓
<input type="radio"/> Possible Breach	Log	↑ ↓
<input type="radio"/> Attempted Intrusion	Log + Drop Connection	↑ ↓
<input type="radio"/> Attempted Denial of Service	Log + Drop Packet	↑ ↓
<input type="radio"/> Policy: Peer To Peer Traffic	Log + Drop Connection	↑ ↓
<input type="radio"/> Unusual Traffic	Log	↑ ↓
<input type="radio"/> Reconnaissance	Log	↑
<input type="radio"/> Disabled Rules	Ignore	—

## 1.7 Tips & Traps

---

eSoft Intrusion Prevention Softpak is meant to add an additional layer of protection to an existing layer two firewall, offering an ability to inspect packets that are passing. It is designed to work in tandem with other eSoft Softpaks that provide

other areas of inspection- Network and Email ThreatPaks for viruses, worms and Trojans, Anti-spyware for spyware related items. IPS watches for many other types of activities that are not specific to viruses, worms, Trojans or spyware.

eSoft has carefully built a rule base that covers the majority of threats that will be seen by the majority of networks, but is not all. By keeping the rule base relatively small and writing signatures that often cover multiple more specific signatures; we are able to cover the most dangerous activity without sacrificing performance and creating a high level of false positives and the associated attention required by the local admin.

Altering the action profiles or default settings should be done with a specific goal. You should consider consulting with eSoft support to insure the correct result- i.e.; a profile needs to be altered to prevent acting on a specific type of browser

If a specific rule is desired that doesn't exist in our IPS rule base, a request can be submitted to the eSoft Threat Prevention team through eSoft support.

IPS will only see activity that originates from an "untrusted" network bound for a trusted one. This will limit its ability to see internal attacks to local servers, or outbound activity originating from the local network.

ThreatWall is not a firewall itself, so should generally be placed behind an existing firewall.