

# Netguard IPS

## ADVANCED INTRUSION PREVENTION SYSTEM WITH TOTAL INTERNET POLICY ENFORCEMENT

**Netbox Blue delivers the most advanced protection against known and unknown internet threats with its new Netguard IPS. The feature combines an advanced Intrusion Prevention System (IPS) with total internet policy alerting and enforcement control to give your company the surest means to protect vital data, preserve network integrity, manage office productivity and deliver your duty of care to staff and clients.**

### INTRUSION DETECTION PREVENTION

With the rise of internet use in businesses, companies are increasingly exposed to an avalanche of new threats. Traditional firewalls are not designed to block malware contained in web pages. With an increasing number of viruses now nested in internet sites and applications, traditional firewalls no longer provide the protection needed. By using everyday web applications and downloading information from internet sites, your staff members risk infecting your company with a virus or exposing your data to hacking attempts or phishing attacks. Internet use can also result in a company's network becoming a member of a botnet, being taken over by a spam network and being used to send out massive amounts of spam email without the knowledge of the company. This can severely damage a company's reputation and make it difficult to work with other organisations.

Even the most legitimate internet sites can be compromised by hackers. Staff members can then unknowingly download

Netguard IPS protects your company from the inside and the outside. It blocks malicious content from being downloaded onto your network and prevents your network from sending malicious content. The comprehensive policy setting features of Netguard IPS also provide total control over dynamic applications, such as peer to peer downloads and VoIP, that traditional firewalls are unable to block. Netguard IPS adds another layer of security and control to the Netbox's integrated suite of features, giving your company cost-effective protection against the ever changing digital threat landscape.

malicious content by simply just visiting the site. It's this 'unknowable' element to web browsing that Netguard IPS focuses on, using the HTTP anti-virus scanner to look for malicious code, in real-time. The system comes with all-port scanning abilities and is bi-directional. Many gateway Intrusion Prevention Systems focus only on traffic originating from the internet. Netguard IPS also looks at outbound traffic, delivering protection against brute force attacks and protecting the network from becoming a member of a botnet. If an infected PC or laptop is detected, the system automatically prevents it from sending out spam. It blocks the PC or laptop's access to the internet and alerts the IT administrator. In this way your company is protected against being hijacked by cyber criminals and prevents reputational damage.

Netguard IPS is seamlessly updated in real time, without any user intervention, to ensure your network is always protected from emerging internet threats.

*"We've had problems with PCs being infected by malware in the past, but since installing Netguard IPS we feel completely secure and protected. I also find the policy enforcement feature very useful for controlling certain applications. I particularly like the way we can choose which applications we want to block. It's a very handy feature."*

**Alex Wangsanata, BRITA Commercial Analyst**



### 15 Categories, with dynamic protection

There are 15 different categories, such as Chat/IM, P2P Protocols (BitTorrent), Online Games, and Email which can be selected depending on the specific requirements of the company.

The categories are updated on a continuous basis via a dynamic update service, therefore ensuring any emerging threats are blocked by the Netbox.



### Total content control

When combined with Category Web Filtering and email filtering, you can deliver total content control for your business.

The HTTP anti-virus scanning ensures that incoming traffic is scanned in real-time.



### Emailed alerts showing detected and blocked activity

The solution can be customised to send emailed alerts on detected or blocked activity. These alerts can be automatically emailed to you when the activity is detected.

## DYNAMIC APPLICATION CONTROL

Netguard IPS provides administrators with a vital tool for managing dynamic applications. Dynamic applications such as Skype, instant messaging and peer to peer applications can easily change the way they behave to bypass traditional firewalls, leaving the internet open to abuse. Uncontrolled internet use can have damaging consequences for productivity, disrupt internet performance, add to internet bills and bring down the entire network. Media and music streaming can have a particularly detrimental impact on a company's bandwidth and productivity and can also be illegal. If your staff members are spending time adding to their music collection, chances are, other crucial business applications will be affected as vital bandwidth is chewed up. Your company will also be paying higher internet charges. If staff members or even guests are using your systems to illegally stream media, your company can be liable.

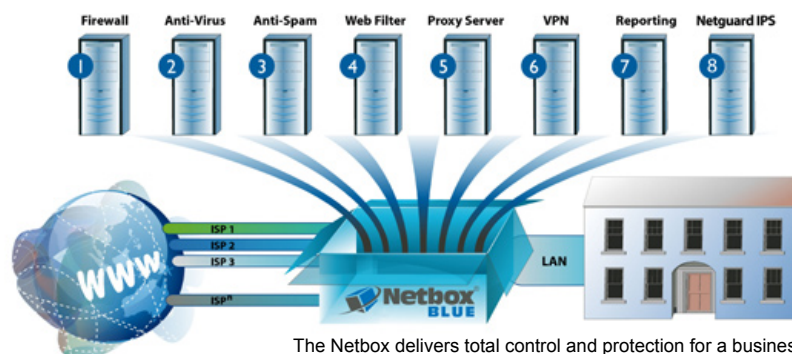
Netguard IPS uses Deep Packet Inspection (DPI) to effectively open up a file and inspect its contents to determine if it fits within the company's policy. In this way it is able to identify and block applications, such as peer to peer downloads, that would bypass a traditional firewall. The system can be used to block or alert managers when a company policy is being breached. This allows managers to take swift action if needed. The granular policy setting offered by Netguard IPS also gives managers unprecedented flexibility in controlling applications. If a company needs to use an instant messaging application, for instance, it can do so and block all others. This would not be possible with a port-blocking firewall. Netguard IPS combined with Netbox Blue's Category Web Filtering and email filtering engines delivers total content control to businesses of all sizes.

**Signature Categories**

Category	Signature Info	Alert LAN	Alert Internet	Drop	Internet Blacklist Time	LAN Blacklist Time	Current Blocks
<b>Current Threats</b> [edit] [A regularly updated list of current network security threats]	Enabled: 71 Total: 74	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1d	1h	None
<b>Spyware and Malware</b> [edit] [Traffic signatures identifying outgoing connections originating from spyware and malware applications]	Enabled: 881 Total: 1943	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1d	1h	None
<b>Attack Reconnaissance</b> [edit] [Common pre-attack reconnaissance behaviour observed prior to network infiltration]	Enabled: 76 Total: 101	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1d	1h	None
<b>Windows Networking Exploits</b> [edit] [Windows file sharing and RPC exploits]	Enabled: 1732 Total: 2822	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
<b>Denial of Service</b> [edit] [Standard and distributed DOS attacks]	Enabled: 2 Total: 69	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
<b>ActiveX Exploits</b> [edit] [Common malicious ActiveX components]	Enabled: 587 Total: 587	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
<b>General Exploits</b> [edit] [General network exploit signatures, for example exploit shellcode and remote admin applications such as Backoffice]	Enabled: 748 Total: 920	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
<b>Service Exploits</b> [edit] [Exploit signatures for common network services such as DNS, Telnet, FTP, TFTP and NNTP]	Enabled: 81 Total: 146	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
<b>Chat/IM</b> [edit] [Traffic signatures for chat and instant messaging protocols such as ICQ, IRC, Jabber, MSN, Yahoo]	Enabled: 7 Total: 40	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
<b>P2P Protocols</b> [edit] [Skype and common peer to peer filesharing protocols, such as BitTorrent, eDonkey and Gnutella]	Enabled: 8 Total: 94	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
<b>Online Games</b> [edit] [Online multiplayer games and services including Steam and World of Warcraft]	Enabled: 1 Total: 40	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
<b>Email</b> [edit] [Signatures for exploits that affect common network mail services such as IMAP, POP3 and SMTP]	Enabled: 93 Total: 150	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
<b>Databases</b> [edit] [Signatures for exploits that affect common database such as MySQL and Oracle]	Enabled: 304 Total: 322	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
<b>VoIP</b> [edit] [Exploits signatures for common VoIP software]	Enabled: 14 Total: 52	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
<b>Miscellaneous</b> [edit] [Miscellaneous policy traffic signatures]	Enabled: 0 Total: 249	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			None
	<b>Enabled: 4605 Total: 7609</b>						

[Update]

Netguard IPS is available as a premium upgrade to the Netbox and can be included in all new installations.



The Netbox delivers total control and protection for a business