# 12 things effective intrusion prevention systems should do

Making the right choice in selecting an intrusion prevention system

# Table of contents

# Introduction

The latest generation of exploits used to attack computer systems relies on extremely sophisticated evasion techniques to escape detection. The most serious of these attacks can provide the attacker with the ability to remotely initiate system-level commands. Cybercriminals often try to circumvent the intrusion prevention systems (IPS) by using complex algorithms to evade detection.

Next-generation firewalls (NGFWs) with integrated IPS with advanced anti-evasion provide the ability to identify and block malware before it can enter your network so that you can defeat these sophisticated evasion techniques. To be effective, your IPS should be able to perform each of the functions listed in the following pages.

**Failure to detect and block these exploits can leave an organization vulnerable to attackers.**

1st thing an effective IPS should do:

# Provide multiple methods of protection against server and client side attacks

Fundamentally, your IPS must include comprehensive signature coverage for attacks directed at both servers and clients.

All intrusion prevention systems should include application vulnerability protection, buffer overflow protection and protocol anomaly detection for a wide variety of known attack vectors.

Intrusion prevention systems are only as good as their ability to block attacks; make sure the one you select includes regular updates to always provide the best protection possible.

2nd thing an effective IPS should do:

## Scan all traffic, regardless of port or protocol

Traditional IPS only offered protection for only a limited range of ports and protocols, but modern attacks can target any application running on your network.

Your IPS needs to scan ALL traffic—not just a few select ports or protocols—to identify and protect against emerging and existing threats.


Intrusion prevention systems need to provide deep packet inspection of every packet crossing your network to effectively detect and block new sophisticated attacks.

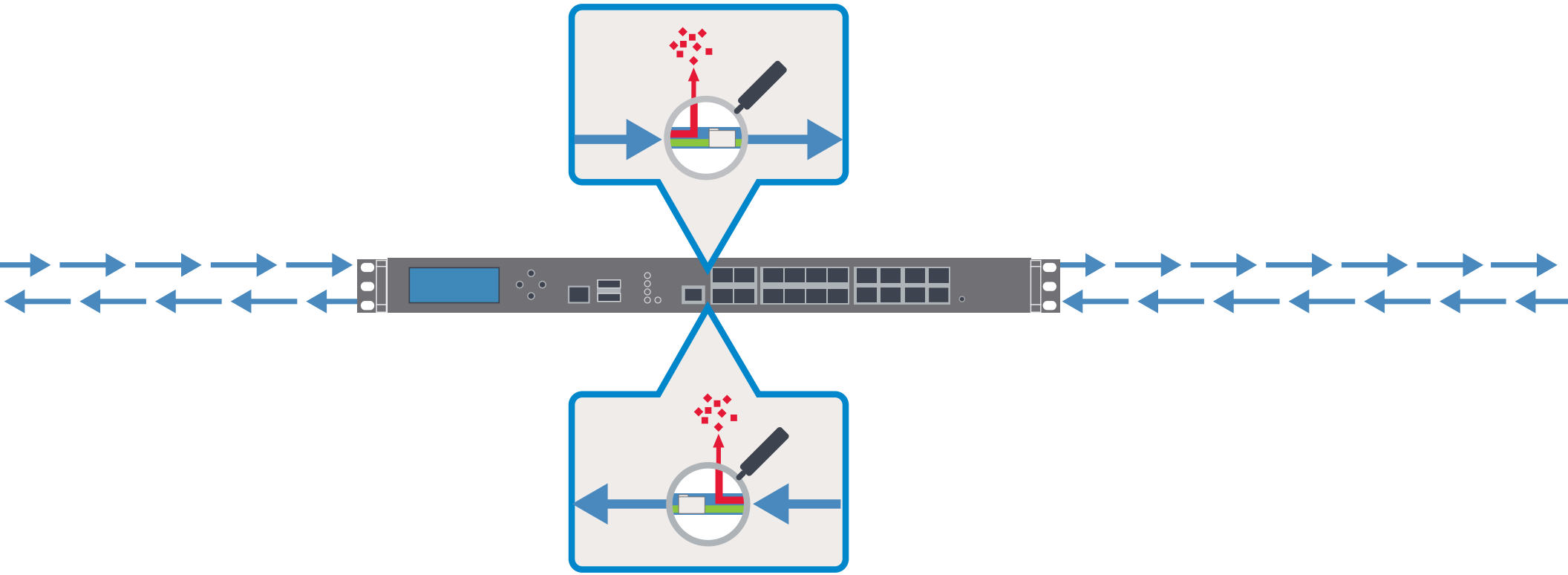
3rd thing an effective IPS should do:

# Scan all traffic, both inbound and outbound

Attackers can send confidential information from compromised systems inside your network, or worse, attackers can actually get inside your physical building and launch attacks. To counter this, as well as other internal attacks, your IPS needs to scan both ingress and egress traffic.

Most traditional IPS solutions only focus on inbound traffic. This leaves the organization vulnerable to attacks coming from other parts of the network.

Scanning ingress traffic is fine for keeping the bad guys from breaking into your network, but what about the ones that may already be inside?



4th thing an effective IPS should do:

# Normalize traffic to prevent evasion and obfuscation

Today's hackers use sophisticated encoding techniques in an attempt to evade detection, and can use these across all ports and network layers, in both inbound and outbound traffic.

Effective intrusion prevention systems need the ability to normalize traffic to a common format to detect and prevent advanced evasion and obfuscation techniques.

Sophisticated cyber criminals are aware of latest IPS techniques, and they work hard to prevent detections of their attacks. Your IPS needs to be able to defeat advanced evasion techniques in order to detect and prevent the actual attack.

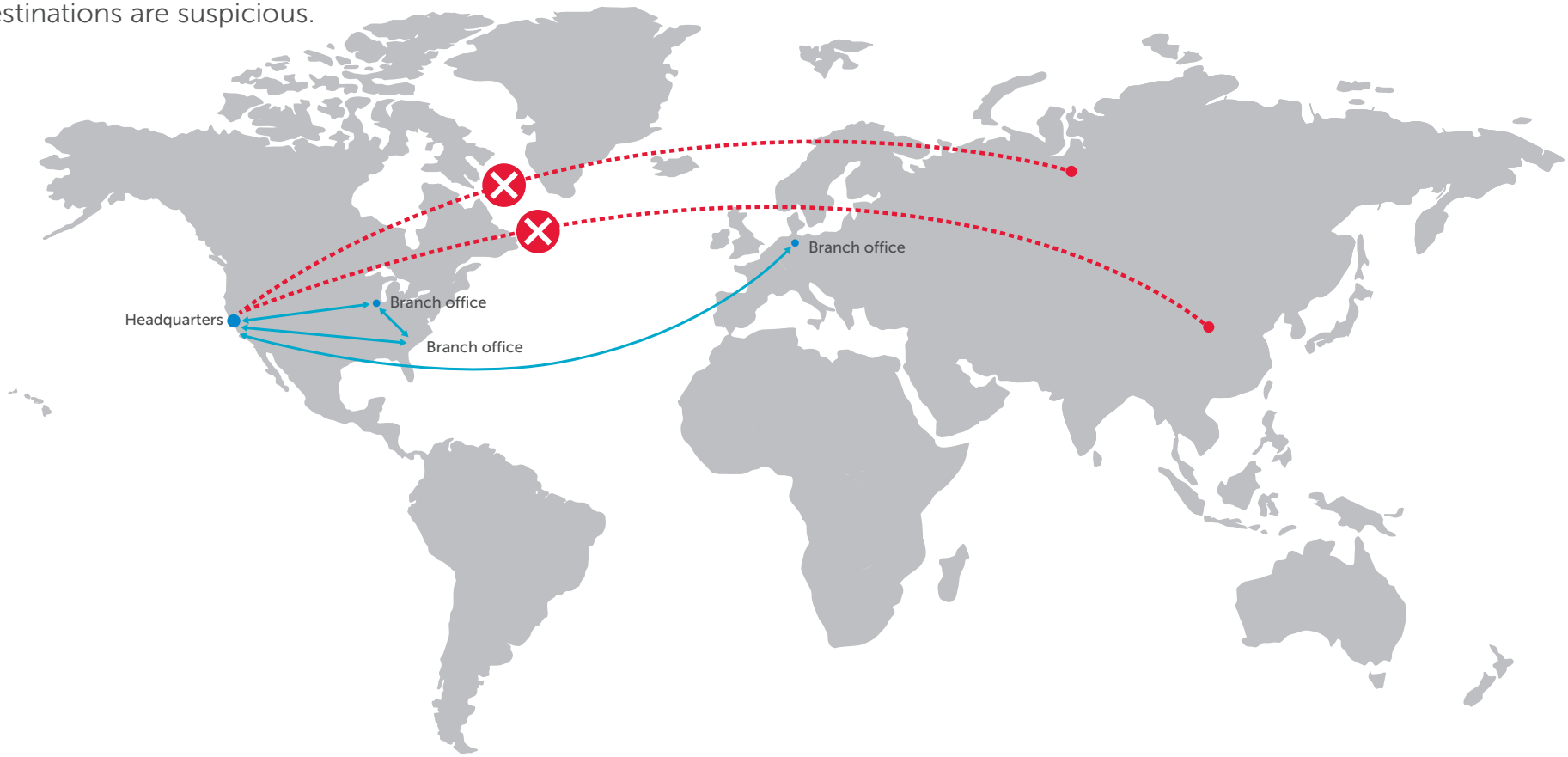
5th thing an effective IPS should do:

# Monitor and block traffic based on geographic origin

Sometimes where traffic comes from—or is being sent to—can be as much of a clue that there is something wrong as what it contains. Some locations are known hotbeds of criminal activity.

Intrusion prevention systems should have the ability to trace an IP address back to its geographical location to ascertain whether traffic sources or destinations are suspicious.

Your IPS should make it easy to identify and block anomalous behavior such as traffic coming or going to foreign countries.

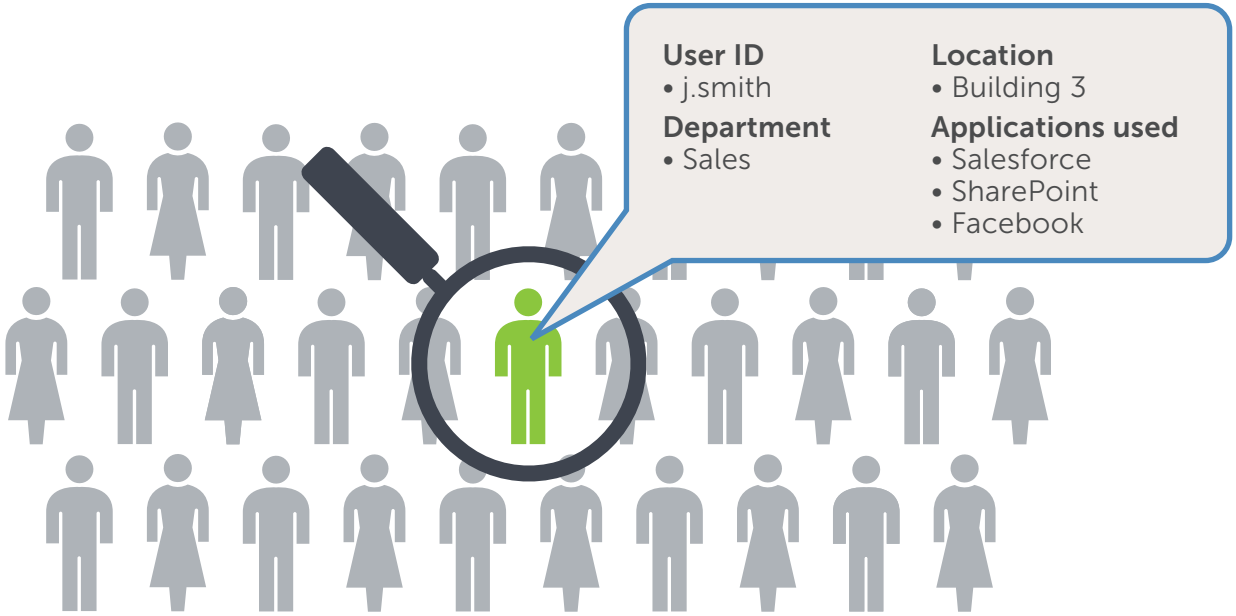


6th thing an effective IPS should do:

# Provide contextual awareness based on user

Some users are inherently more trusted than others; these roles should be reflected in their privileges. Effective intrusion prevention systems need to provide context of not just what applications are on the network, but also who is using them.

One piece of information alone can make it difficult to make the right decision. A good IPS should provide multiple data points in order for administrators to make an informed decision.




## Active directory can be integrated into the IPS to tie applications used on the network to specific user credentials.

7th thing an effective IPS should do:

# Allow custom signatures to be created and installed

IPS signatures must be updated frequently to meet emerging threats. But to deal with custom applications your IPS should enable you to create custom signatures for an added layer of protection against proprietary technology.

The signatures that are included with your IPS are extremely important, but sometimes that alone is not enough— what about that old CRM system that was built just for you? Effective IPS should allow you to create custom signatures to fill in the gaps.

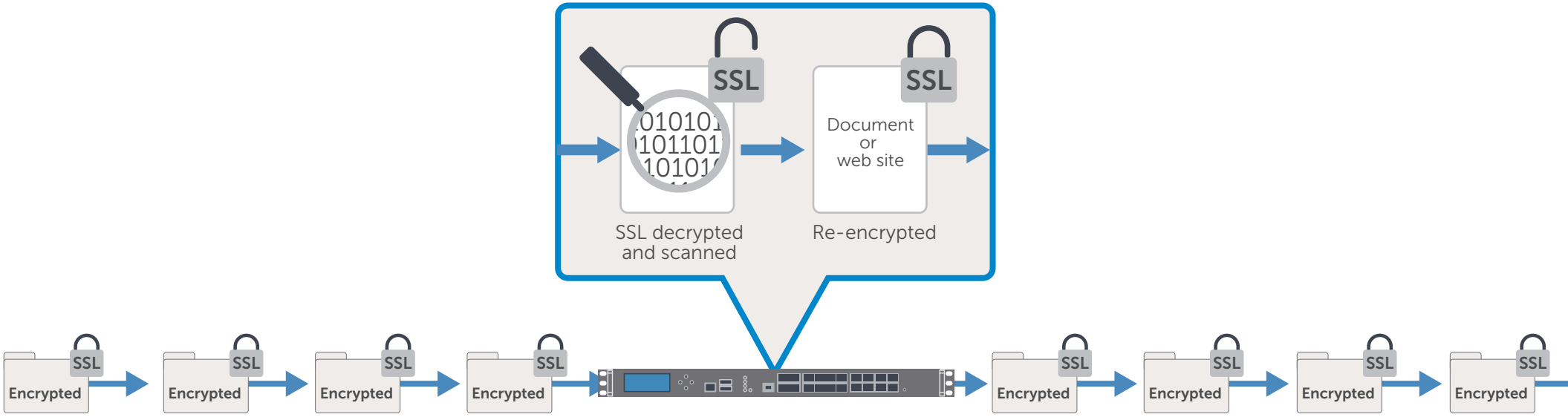
Custom signatures can be used to provide protection from an advanced attack that is tailored specifically to your environment.

8th thing an effective IPS should do:

# Scan SSL encrypted traffic

Today's web-based traffic frequently uses Secure Sockets Layer (SSL) to encrypt sensitive communications such as credit card transactions. However, cyber criminals also use SSL-encrypted traffic to hide threats.

The Internet is filled with drive-by download sites that use SSL to hide the delivery of malware. An effective IPS system should be able to decrypt SSL to stop these attacks.



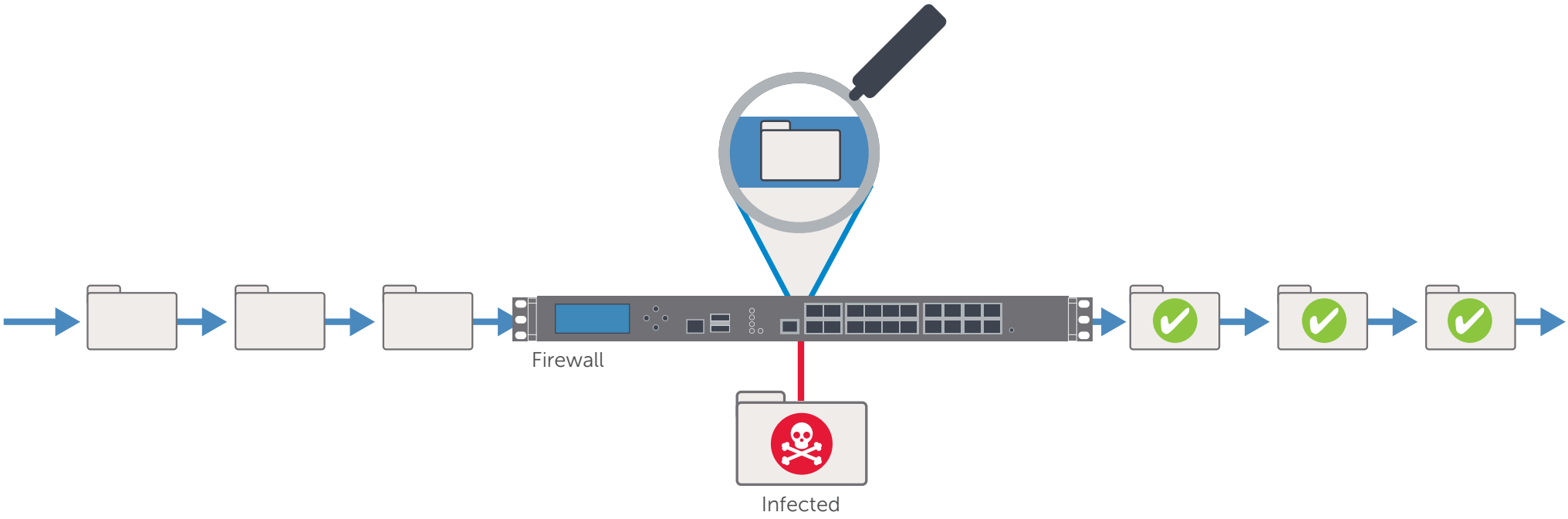

## Traditional IPS cannot detect or block attacks encrypted using SSL.

9th thing an effective IPS should do:

# Detect and block malware as it enters the network

Since malware has proliferated on the Internet it has become imperative that organizations add layers of protection at the gateway to secure their infrastructure.

Effective intrusion prevention systems need to be able to stop any kind of attack, including Trojans, viruses and worms that may be hidden in seemingly innocent traffic.




## Traditional IPS cannot detect or block malware as it enters the network.

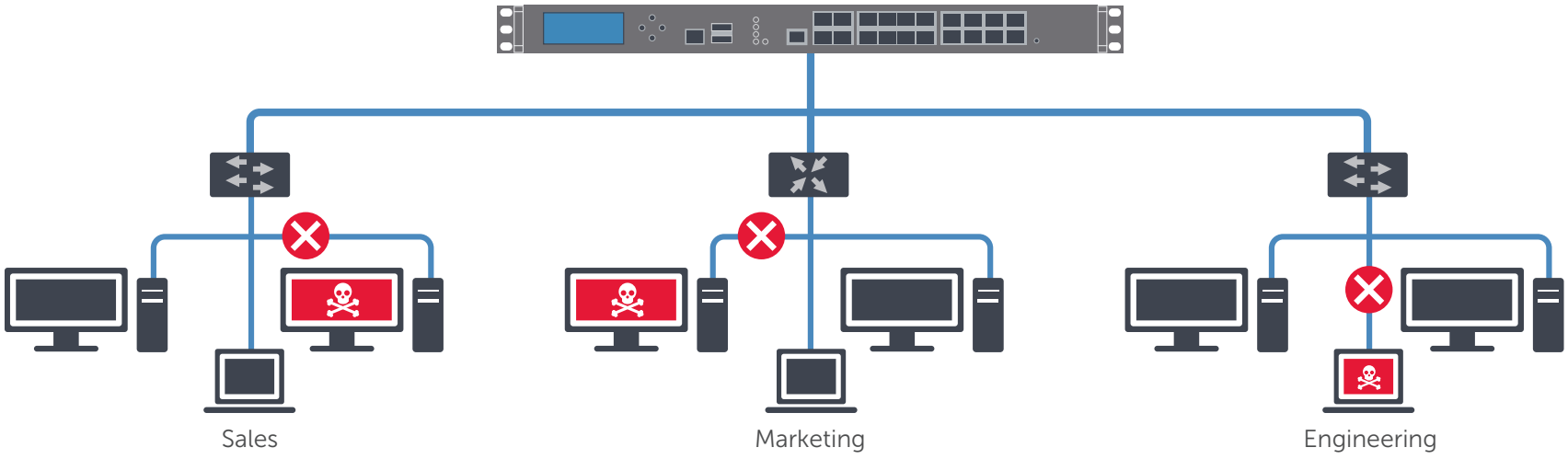
10th thing an effective IPS should do:

# Detect and block communication from systems that are already compromised

Botnets and staged attacks often use common ports and protocols in an attempt to hide command and control traffic sent by systems that have already been compromised.

Sophisticated attackers often try to hide communications by abusing protocols to tunnel traffic out of the network. Botnets often communicate with known compromised servers using similar methods.

Effective IPS should support anomaly detection and IP reputation to block communication from compromised systems and botnets.



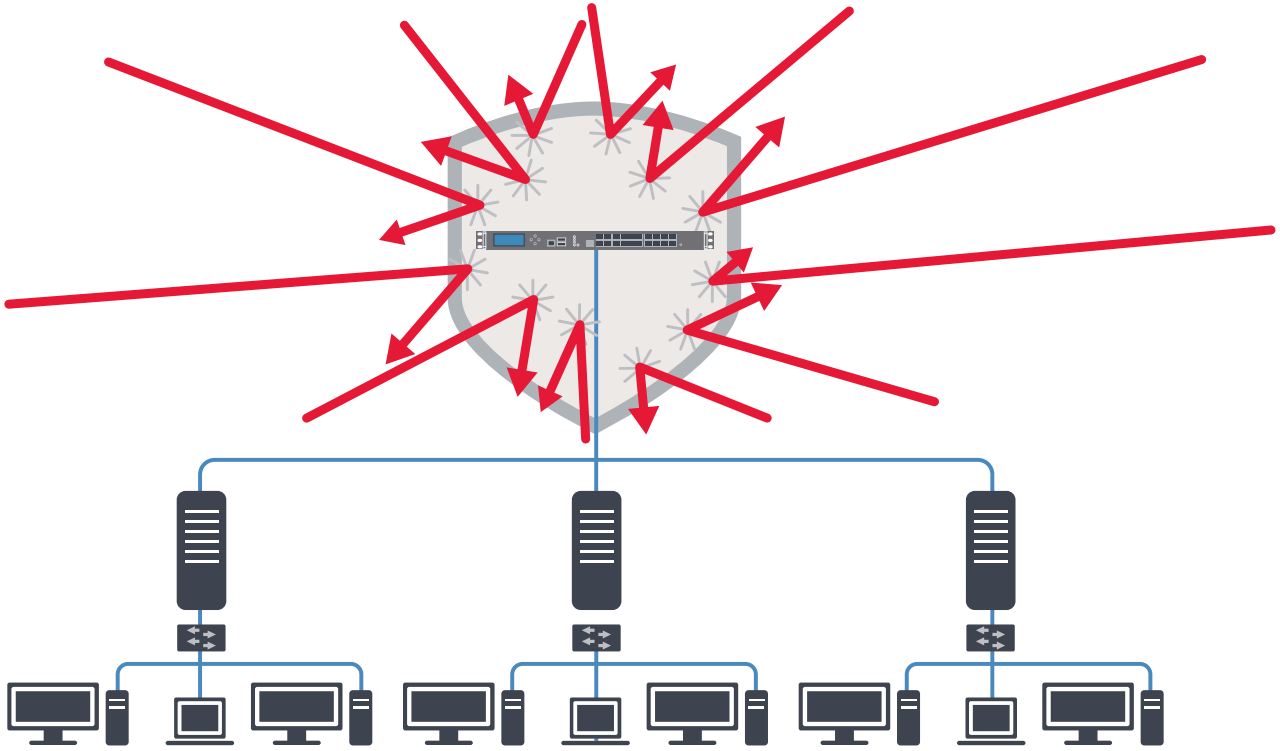
11th thing an effective IPS should do:

# Protect the network from denial of service and flood attacks

Attackers will sometimes attempt to block all Internet communication coming into or out of an organization by using denial of service and flooding techniques.

Part of a well-rounded intrusion prevention system includes the ability to protect an organization from attacks that may impair business operations.

In today's world, stopping an organization from conducting business over the Internet can sometimes be an effective attack method. Your intrusion prevention system should be able to block any type of attack, regardless of how it's initiated.



12th thing an effective IPS should do:

# Provide traffic analytics and integrate with other analytics engines

Trends such as social media and the consumerization of IT have resulted in application chaos over business networks. To make sense of it all, your IPS should enable off-box reporting to flow-based protocols such as NetFlow and IPFIX.

Exporting traffic flow analytics from the IPS enables valuable insight and greater visibility into network traffic.

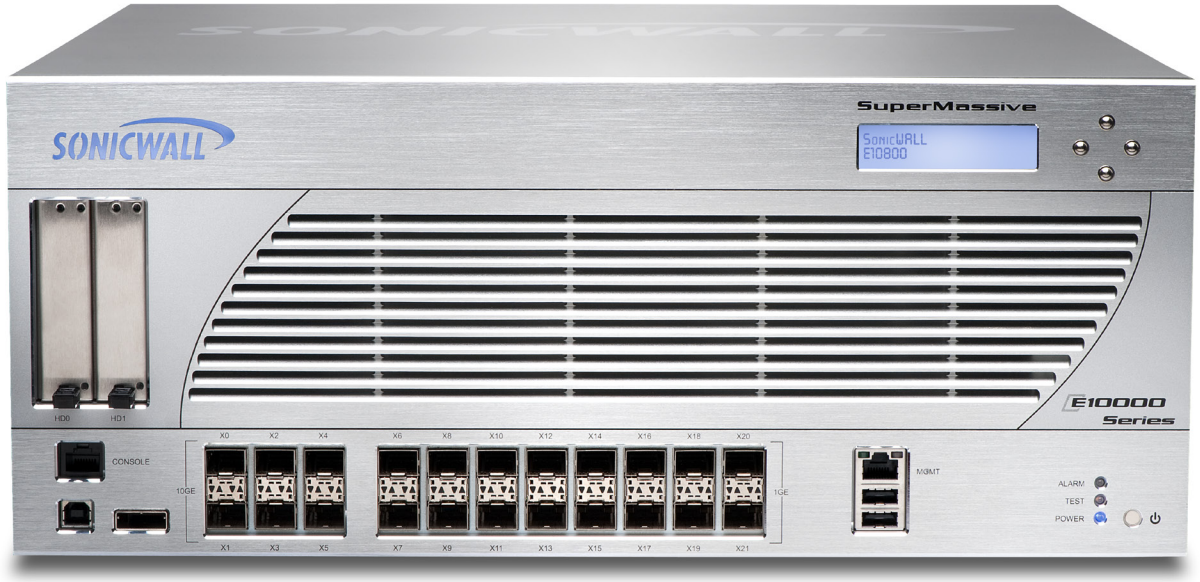
Sometimes information from two weeks or two months ago can help you understand what is happening today. By exporting traffic analytics to an off-box collector, organizations can store historical information such as hidden communications, client/server attacks, VPN usage, VoIP traffic or Internet application activity by user for as long as desired.

# Your choice: Point solutions vs. consolidated solutions

In the past, enterprise organizations needed separate best-of-breed firewalls and best-in-class intrusion prevention systems to protect their enterprise. Today, organizations can attain best-in-class firewall and intrusion prevention without the complexity of managing separate appliances, GUIs, and deployments.

Next-generation firewalls that consolidate advanced IPS capabilities—such as the Dell™ SonicWALL™ SuperMassive™ E10800—can deliver resistance to evasion, powerful context and content protection capabilities, comprehensive threat protection and application control in a single integrated device.

Consolidated solutions offer higher security, easier management (fewer consoles and consolidated security data), lower total cost of ownership (TCO) and more flexible deployment options.



# Dell SonicWALL Intrusion Prevention System

Dell SonicWALL next-generation firewalls provide a deeper level of network security first, by using a patented[1] Reassembly-Free Deep Packet Inspection® (RFDPI) engine to deliver full inspection of every byte of inbound and outbound traffic at all layers of the network stack, regardless of protocol or SSL encryption.

All Dell SonicWALL NGFWs feature a tightly integrated intrusion prevention system with sophisticated anti-evasion capabilities, in order to provide this deeper level of security to organizations of any size.

Additionally, Dell SonicWALL network security goes deeper than other firewalls by providing an intrusion prevention system that features sophisticated anti-evasion technology, high-performance SSL decryption and inspection,  and network-based malware protection that leverages the power of the cloud.

**Advanced context awareness features of Dell SonicWALL IPS include:**

- Geolocation
- User and application identification
- Inspection and identification of documents and content
- Ability to scan for administrator-specified custom content such as text strings and credit card numbers

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361

# 2012 NSS Labs Security Value Map for IPS

In the 2012 NSS Labs Security Value Map™ (SVM) for IPS, the Dell SonicWALL SuperMassive E10800 Next-Generation Firewall with integrated intrusion prevention not only garnered the highly coveted "Recommend" rating but also outperformed many dedicated IPS vendors.


"Resistance to known evasion techniques was perfect, with the Dell SonicWALL SuperMassive SonicOS 6.0 achieving a 100% score across the board in all related tests."—NSS Labs

"For high-end multi-gigabit environments looking to upgrade defenses from their current IPS, the advanced architecture of the Dell SonicWALL SuperMassive running SonicOS 6.0 provides an extremely high level of protection and performance."—NSS Labs

## How can I learn more?

- Download the 2012 NSS Labs Security Value Map for IPS
- Download the whitepaper, Anti-Evasion: Why It's a Critical Component of Intrusion Prevention Systems

For feedback on this e-book or other Dell SonicWALL e-books or whitepapers, please send an email to feedback@sonicwall.com.


**For more information**

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124

www.sonicwall.com
T +1 408.745.9600
F +1 408.745.9300




About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results.

If you have any questions regarding your potential use of this material, contact:


Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.



09/13 DS 0558