Intrusion Detection and Prevention Systems

MITEL SOLUTIONS ENGINEERING GROUP

Technical Paper

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

Intrusion Detection and Prevention Systems
Mitel Solutions Engineering Group – Technical Paper
Version 1.0

List of Figures

List of Tables

Overview

This Mitel technical paper discusses Intrusion Detection and Intrusion Prevention systems (IDPS), what they are, how they operate, how to use these systems, and recommendations on selecting a solution.

The network designer and system administrator are provided with information on the following topics:

- Forms and types of IDPS solutions
- How do IDPS solutions detect attacks
- What are the various components that comprise an IDPS solution
- How IDPS solutions are used to protect networks
- Recommendations on how to choose an IDPS solution

This document is part of a suite of Mitel security documents that discuss topics related to Cloud based UC security, the documents included in this suite are:

- Securing Mitel Cloud Based UC Networks
- Network Intrusion Detection and Intrusion Prevention Systems

Introduction

IDPS products provide the network designer with powerful tools to help secure the network, but they are only one aspect of a total security solution. The network designer and administrator also need to be aware that overall network security is a responsibility that is shared between service providers, application providers, users and network administrators; this subject is discussed in the Mitel technical paper *Securing Mitel Cloud Based Unified Communications (UC) Networks.*

The principles and recommendations discussed in this document are informational in nature, for detailed information on how to secure a particular UC solution, contact Mitel Professional Services.

Who are the Parties that Should Use this Document

This document will be of interest to individuals that are involved with network design, system administration information technology and network security, and any individuals who wish to gain an understanding of IDPS technologies, how to deploy the technology and how to select an IDPS solution.

Intrusion Detection and Intrusion Prevention Systems

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are not exactly next generation security tools - the earliest research in this area dates from 1980. Quite often the IDS and IPS functions are combined into one product; these products are referred to as Intrusion Detection and Prevention Systems (IDPS). In recent years these systems have been evolving rapidly to meet industry demands and vendors have been integrating IDS, IPS or IDPS capabilities into other networking devices such as routers and L2 switches effectively creating next generation security tools.

Intrusion detection and intrusion prevention tools focus on network traffic and should not be confused with antivirus or antimalware technologies which focus on actual binary files. IDPS technologies have the ability to detect many different malicious activities at all levels of the network stack. Some IDPS technologies also perform protocol inspection which allows for the detection of malicious behaviour instigated by application protocols.

IDS and IDPS systems can be configured to generate alerts when suspicious activity is detected. Such alerts may be sent to the administrator by email or SMS, or the administrator may be notified of the alert via the IDS or IDPS user interface. Security solutions will often include a Security Information and Event Management system (SIEM), when a SIEM is present the IDS or IDPS systems can be configured to send alerts to the SIEM.

Security Information and Event Management (SIEM)

A Security Information and Event Management system (SIEM) is a product that combines the security information management system (SIM) and the security event management system (SEM) into one solution.

SIEMs are available as software products that run on a customer supplied industry standard server, as a turnkey appliance or as a managed service.

The SIEM provides the administrator with the ability to view data from all of the IDS and IDPS systems in a single place. This centralized view makes it easier to detect and analyze network trends and patterns that are out of the ordinary, and to recover from security events.

Most SIEMs will collect event data from the security devices using standards based logging protocols or SNMP. It is important that the network designer ensure that the security tools being considered for deployment employ a common communications protocol - standards based protocols are preferred over proprietary protocols.

IDS, IPS, and Firewalls - how do they differ?

Firewalls, Intrusion Detection, and Intrusion Prevention Systems all monitor network traffic for activity, but they differ in how they are deployed in the network, what types of traffic activity they look for, and in how they react should they detect a traffic anomaly.

The behaviour of Firewalls, Intrusion Detection and Intrusion Prevention Systems differs in the following ways:

- **A Traditional Firewall:** is designed to protect a network from threats and intrusions originating from outside the network being protected. These firewalls typically use IP addresses, port numbers and policies to allow or disallow traffic and they have very basic IPS functionality designed to protect against DoS attacks. Traditional Firewalls will not detect an intrusion or attack that originates from within the protected network.

- **A Stateful Firewall:** Allows/denies traffic based on IP, port and protocol, but also maintains a state table to ensure only legitimate traffic is accepted.
- **An Application Firewall:** Inspects incoming traffic , to ensure that only legitimate traffic is accepted (e.g. It will prevent the use of a DNS port for HTTP traffic)
- **An Intrusion Detection System:** is a passive system, like a firewall it analyzes traffic coming into the network and - this is where IDS differs from a firewall - it also analyzes internal network and out-going traffic. When suspicious or malicious traffic is detected, the system, if configured to do so will send a notification to the administrator and/or a Management Server. The onus is then on the administrator to evaluate the threat and if necessary block the traffic.
- **An Intrusion Prevention System:** is a reactive system, like an IDS it analyzes incoming out-going and internal network traffic looking for intrusions. When suspicious or malicious traffic is detected the IPS, if configured to do so, will send a notification to the system administrator and/or a Management Server. However, the IPS has the additional ability to take action to block the detected threat or intrusion. Depending on the IPS, data related to the attack may be sent to the vendor for further analysis. The IPS may also support the use of vendor provided signatures and regular signature updates protect against newly discovered threats.
- **An Intrusion Detection and Intrusion Prevention System:** is a system that combines IDS and IPS functionality into one product.

Notes:

1. Since Intrusion Detection capabilities are always an integral part of Intrusion Prevention Systems, Intrusion Prevention Systems are also referred to as **Intrusion Detection and Prevention Systems**, or **IDPS.**
2. This document uses **IPS** and **IDPS** interchangeably, **IDS** is used to refer to products that only perform the intrusion detection function.

IDS and IDPS, What do they do?

IDS and IDPS products differ widely with respect to the types of events that they can detect and the methods that they use to detect events, but most IDS and IDPS products perform the following functions when they detect an intrusion.

- **Packet Capture:** Capture of TCP and UDP packets that being sent over the monitored network segment.
- **Event Logging:** Information about the event that was detected will be logged by the IDS or IPS, either locally or to a remote management Server. The information may also be sent to a central logging server or a Security Information and Event Management (SIEM) system.
- **Administrator Notification: :** An alert - which is a configurable action taken based on a defined trigger and event - is sent to the administrator by email, the SIEM, IDS or IPS user interface, SNMP traps, SMS, or a screen pop-up.
- **Report Generation:** Depending on the solution and configuration, the IDS or IPS captures audit data and provide export or reporting facilities to allow for more thorough review and analysis.

Unlike the simpler IDS products, IDPS products take action against an intrusion or threat and attempt to thwart the attack, the most common actions are:

Stopping the attack: The IDPS may close down the network connection where the attack is originating, or it may close down the user that is causing the attack. The IDPS might also respond by blocking all network access to the target, or it may protect the target by blocking/isolating the source of the attack.

- **Modify the Security Environment:** The IDPS might change the configuration of other security controls such as routers and network switches or a firewall integral to a host to block the suspicious activity.
- **Alter the Attack's Content:** Very advanced IDPS products can delete or replace malicious portions of a suspected attack to neutralize the attack. This might involve removing or quarantining a suspicious email attachment, or it could be a more complex operation such as when an IDPS acts as a proxy and repackages incoming payloads that are wrapped with potentially suspect headers with new normalized headers before allowing the packet into the network.

Are IDS and IDPS Products Failsafe?

Those responsible for securing a network or applications must keep in mind that IDS and IDPS technologies are fallible. IDS and IDPS technologies can mistakenly raise an alarm based on a legitimate activity, when this happens it is referred to as a false positive. When IDS or IDPS technologies fail to detect malicious activity and fail to raise an alarm, it is referred to as a false negative.

It is not possible for IDS and IDPS products to eliminate all false positives and false negatives, often trying to eliminate one causes the other to increase, it is a balancing act. The administrator will typically err on the side of caution and attempt to decrease the occurrence of false negatives; however this will cause false positives to increase. With an increased volume of false positives the administrator will need to invest more time trying to determine if the false positive is in fact a false positive or if it is actually a malicious event.

Reconfiguring IDS or IDPS products to rebalance false positives against false negatives is referred to as tuning, and IDS and IDPS tuning will need to be conducted on an ongoing basis.

It should be noted that while increasingly detailed signatures may help reduce false positives, they may also increase network latency while the data in transit is checked.

Forms and Types of Intrusion Detection and Protection Systems

IDPS solutions are available in a number of different forms, and there are also several different types of IDPS solutions. IDPS technologies run the gamut from open source freeware offerings, to very costly software or hardware based offerings, this section discusses forms and types of IDPS technologies, specific product offering are discussed in the section called, *Choosing an IDPS Product.*

Some of the available forms and types of IDPS solutions are described in the following sections.

Different Forms of IDPS

Intrusion Detection and Prevention Systems are available in several different forms:

- **Dedicated IDPS:** this form performs Intrusion Detection and Intrusion Prevention, dedicated IDPS is available as:

  - **A hardware based device:** these devices are available with different interfaces speeds, different processing capabilities, and some vendors offer redundant hardware options.
  - **A virtual appliance:** this software appliance is deployed on a server that will be dedicated to act as an IDPS.

- **Integrated IDPS:** an IDPS software appliance is integrated into another networking device to provide additional security capabilities, such as Next Generation Firewalls (NGFW) and Unified Threat Management (UTM) solutions.
- **Host based IDPS:** is another form of Integrated IDPS, the IDPS appliance is installed on a server to protect an application or applications that are hosted on the server.

Different Types of IDPS

There are a number of different types of Intrusion Detection and Prevention Systems, each type is optimized for a specific purpose and for deployment in a specific place in a network:

- **Network-based IDPS:** these systems are designed to be deployed at strategic points in the network. A Network-based IDPS will monitor and analyze the network traffic and application protocol activity; it compares its analysis to a library of known attacks. If an attack is detected, the system notifies the administrator and takes remedial action to thwart the attack. (There is also an alternate type of Network-based IDPS called Off-line Network-based IDPS that is used to analyze stored data; these systems would typically be deployed within a SAN).
- **Host-based IDPS:** these systems are designed to protect a single host computer. The IDPS is installed on the host to be protected and the system will typically monitor network traffic associated with this host, system logs, application activity, file access, file modification and system configuration changes. Some Host-based IDPS solutions offer prevention capabilities, they will block ingress or egress traffic if necessary. Some host IDPS solutions will prevent access to system files, or may self-correct changes to files, along with generating a notification of the detected activity.

  Typically a Host-based IDPS solution will not be able to protect against things that have already happened, such as file modifications or file access modifications, with these types of events the IDPS will transmit a notification.
- **Application-based IDPS:** these systems are usually Host-based IDPS products, but they are focused on protecting a single application rather than the host itself.
- **Network Behaviour Analysis IDPS:** these systems are usually deployed where traffic flows between two networks or subnets, or they may be deployed in a location where they can monitor traffic on critical network backbones. The system monitors network traffic looking for unusual traffic flows such as would be seen if a DDoS attack were underway or if network policy violations were detected, such as a system providing network services to systems that are restricted from obtaining services.

  Specialized network behaviour analysis IDPS solutions are available for addressing the security needs of specific network functions such as, storage area networks, e-mail servers and web servers.
- **Wireless IDPS:** these systems monitor and examine the wireless networking protocols and analyze the data for rogue Wi-Fi Access Points, unauthorized devices, unexpected behaviour and network attacks. These systems do not analyze activity related to the application layer or higher layer network protocols such as TCP or UDP.

How do IDPS Solutions Detect Attacks?

Intrusion Detection and Prevention Systems have several different methods of detecting threats, but the primary mechanisms used are Signature Based Detection, Statistical Anomaly Based Detection and Stateful Protocol Analysis. Some implementations will only use one method to detect attacks, and some implementations will use multiple methods to provide for broader attack detection.

Signature Based IDS: This method monitors network traffic and compares the traffic to a database of signatures or attributes associated with known threats. Should the IDS detect traffic that possesses an attribute or signature of a known threat, then action is taken. The signature database is populated with uniquely identifiable signatures found in the code of each threat.

As new threats are discovered, the signatures are stored in the vendor's constantly growing database of signatures. Database updates are either sent out to IDS systems on an automatic basis from the vendor, or the administrator is responsible for manually updating the database.

One weakness of Signature Based IDS is that there will be a time lag between the time that a new threat is identified, or a variant of a known threat, and the time it takes to update the IDS database with a signature representing the new threat or the new variant. During this time lag the IDS will be unable to detect the new threat. An additional weakness of Signature Based IDS is that it does not perform stateful protocol analysis; therefore it is unable to detect attacks that are orchestrated with multiple events.

Statistical Anomaly Based IDS: This method monitors normal network traffic and creates baseline profiles that represent what normal behaviour is for users, hosts, applications and network connections. Behavioural data might be based on the number of emails a user typically sends or receives the number of failed log in attempts on a host and/or the level of processor or memory usage on a host. The baseline profiles may also be created based on network bandwidth usage, typical protocols in use, the IP addresses of devices communicating with each other and the particular ports that were used. Should the IDS detect traffic or behaviour that does not match the baseline profiles, then action is taken. Anomaly based IDS relies on comparing network, host or user behaviour to established profiles, it is very effective at detecting unknown threats.

The initial profiles are created during a training period, the length of the training period however will vary based on what the administrator decides; the training period could be days or weeks.

There are static profiles that do not change once they are created, and will eventually become outdated and ineffective as the network and its behaviour will evolve over time.

There are also dynamic profiles that get updated when the IDS detects new events or behaviours. Dynamic profiles can be tricked by hackers who intrude into the network incrementally over an extended period of time, causing the IDS to update profiles since it has decided that this is normal behaviour. Creating dynamic profiles can also be an error prone process. An event that occurs infrequently may not be scheduled to happen during the training period; on the other hand there could be malicious activity occurring on the network during the training period and this activity will be included in the profile.

Anomaly Based IDS often generates false positive detections due to legitimate activity that falls outside of an established profile, to address this, the administrator will need to frequently update a static profile or tune a dynamic profile.

Stateful Protocol Analysis IDS: this method of intrusion detection relies on using predetermined profiles that define how and how not a given protocol should be used. The protocol profiles are models based on protocol standards published by software vendors and standards bodies.

Based on these profiles the IDS is capable of understanding and following stateful network, transport and application protocols.

A key part of this detection method is its ability to match requests with responses. For instance when a user attempts to log into a system or service, the user will be in an unauthenticated state, and as a result there will be a limited number of legal commands that the user can transmit, such as username and password. The IDS can also examine the system's response to the user's login request to determine if the login was successful or not.

Once the user has been authenticated by the system, the user will be in an authenticated state and the user will have the ability to issue several additional legal commands. While the user is in an authenticated state the IDS will not be suspicious of the use of these additional commands, however if these additional commands were issued when the user was in an unauthenticated state, the IDS would deem this to be intrusive activity.

Protecting Networks with IDS & IPS Solutions

In reality it is next to impossible to secure every system on a network, providing that the network needs to remain reasonably operational. Many times security controls impede network or application performance and user accessibility. Also, security controls that are deployed without careful consideration may introduce network failure points or worse, single points of failure in the network, thereby reducing network availability ratings.

The network designer will need to try to strike a balance between security requirements, network and application performance and network reliability. This can be achieved by using a hierarchal network design, by segregating the network into Trust Zones, and employing a distributed IDPS solution.

Hierarchal Networks

A properly designed hierarchal network will place the most important computing assets at the core, lesser assets at the distribution layer and the least significant assets at the access layer.

This will allow appropriately sized security measures to be assigned to each of the layers and network resiliency mechanisms to be effectively employed. This topic is covered in the Mitel technical paper called *Securing Mitel Cloud Based UC Networks.*

Trust Zones

It is far more practical to secure a network that has been segregated into trust zones, than a network that has not been segregated into trust zones.

To segregate a network into trust zones, the network designer takes an inventory of the assets and data that require protection, and then applies a rank to these assets and data based on how sensitive the assets and data are. All the assets and data of a particular sensitivity rank are then segregated into their own trust zone; the trust zone may or may not correspond to a subnet. Each trust zone will have different security policies based on the sensitivity rank. This network structure allows for a reasonable balance between security and network or application performance. This topic is covered in the Mitel technical paper called *Securing Mitel Cloud Based UC Networks.*

Distributed IDPS Solutions

Up until this point, IDS and IPS have been described as standalone systems, or as functions that are integrated into devices such as firewalls or embedded into host computers.

What has not yet been discussed is that to provide optimum network coverage, multiple IDS and IPS solutions may need to be deployed in several places in the network to provide an overall distributed IDPS solution.

IDPS components and how these components are deployed are discussed in the following sections.

IDPS Components

When designing security measures into a network, unless cost is no object it will quickly become apparent that it is impractical to deploy fully integrated IDPS products at every network connection to a host or router.

Recognizing this, many vendors offer IDPS systems that are comprised of separate components. This allows the network designer to only deploy the necessary security sub-function at a particular place in the network.

The sub-components that are used to build an overall or distributed IDPS solution are:

- **Sensors:** Sensor is another name for the IDPS sub-components that perform the Intrusion Detection (ID) and/or the Intrusion Prevention (IP) functions. ID and IP sensors are used to monitor and analyze network activity; ID and IP sensors are used by Network-Based, Network Behaviour Analysis and Wireless-Based IDPS solutions. There are two types of ID and IP sensors; appliance-based sensors and software-based sensors.
    - Appliance-based ID and IP sensors use NICs and NIC drivers that are optimized for packet capture, appliances may also use hardware accelerators that assist with the analysis of traffic.
    - Software-based ID and IP sensors are installed onto hosts that meet the sensor's performance criteria; some are installed onto standard operating systems, while others may use custom operating systems.
- **Agents:** Agents are ID and IP sensors that are used to monitor and analyze activity for Host-based and Application-Based IDPS solutions. Agents are installed onto the host computer.
- **Management Server:** The management server manages sensors and agents, and also receives network information from the sensors and agents. The management server may also perform event analysis and correlate events that have been detected by multiple sensors and agents.
- **Database Server:** The database server is an optional component that serves as a repository for event information.
- **Administration Console:** The administration console provides a user interface to access the IDPS sensors and agents so that the administrator can configure and monitor sensors and agents.

Network IDPS Sensor Behaviour

This section discusses how network Intrusion Detection (ID) and Intrusion Prevention (IP) sensors behave, and based on this behaviour where the sensors should be located on the network being monitored.

Network ID and IP sensors can be deployed in two basic modes; inline mode or passive mode.

- **Inline Mode:** Inline sensors are deployed in series with the data flow, meaning the traffic that the sensor is monitoring passes through the sensor just like how a firewall works. Many Next Generation Firewalls have an integrated IDPS operating in inline mode sensor.
- Inline sensors are most often deployed in series with firewalls or routers - on the secure side, where there is a connection between a WAN and a LAN, or between two different trust zones. This configuration allows the firewall to alleviate some of the processing demands on the inline sensor. Needless to say, Inline sensors must have enough traffic processing capabilities so that they do not become a network bottle neck, and in a network that does not have a resilient path, a failed Inline sensor has the potential to kill a network connection.

  An IDPS that has been deployed as an inline sensor has the ability to stop an attack by blocking the offending traffic. An IDS that has been deployed as an inline sensor can only alert the administrator and/or a Management Server if it detects suspicious traffic.

  Next Generation Firewalls and IDPSs are examples of network sensors that would typically be deployed as inline mode sensors.
- **Passive Mode:** passive sensors are like wire taps, or network packet sniffers. They passively collect all packets from a network segment, but no traffic passes through them. Passive sensors are usually deployed in places where they can monitor critical network locations such as within a DMZ.

  Passive sensors can obtain access to the traffic stream in several ways, for instance:

  - **L2 Switch Port Mirroring:** This method is easy to implement, but if the L2 switch configuration gets intentionally or mistakenly altered it is possible that the port may not mirror the traffic or all of the traffic. Also, some L2 switches may not replicate all traffic or protocols out the mirror port, or under heavy traffic load the L2 switch may limit mirroring.
  - **Networks Taps:** A network tap will provide the sensor with the ability to monitor exactly what is on the network. There are several types of network taps available for both copper and fibre optic media. Generally copper network taps should be avoided as they introduce a point of failure. Fibre optic taps are available that are strictly passive - they operate using prisms to divert a copy of the traffic to the tap, these devices do not introduce points of failure.
  - **Network Load Balancer:** A Network Load Balancer can be used to aggregate traffic from multiple streams, and based on routing rules established by the administrator, send the traffic to various sensors.

Network Intrusion Detection and Intrusion Prevention - A Comparison

The primary differences between IDS and IDPS solutions are:

- IDS products only perform intrusion detection; they cannot block an attack they can only raise an alarm or generate a notification that an event has been detected. These products are deployed as passive or out-of-band sensors.
- IDPS products perform intrusion detection and intrusion prevention, these products will detect an intrusion, raise an alarm and block the intrusion. These products are deployed as in-line or in-band sensors.

Even though IDS and IDPS products are different solutions they do share some common requirements. However, due to how these two different solutions are deployed and how they function, the solutions place a different level of importance on these requirements.

The requirements for an IDPS solution, in order of importance are:

- The product must be operationally stable.
- The product's network performance must be well defined
- The product should generate no false positives
- The product should generate a minimum number of false negatives

With an IDPS, product stability is paramount; an IDPS that fails could potentially block all network traffic at the network junction where it is deployed, and an IDPS that cannot keep up with processing incoming traffic will cause transmission delays and possibly introduce packet loss.

When an IDPS makes a false positive determination, it may needlessly block incoming traffic.

The requirements for an IDS solution, in order of importance are:

- The product should generate a minimum number of false negatives
- The product should generate no false positives
- The product's network performance must be well defined
- The product must be operationally stable

With an IDS solution, the primary concern is ensuring that IT personnel are kept informed of any network anomalies; this is achieved by keeping false negatives to a minimum and eliminating false positives. While network performance is important - the solution should be able to keep in step with incoming packets - maintaining close to zero packet processing latency is not important. Even though product stability is important, should the IDS solution fail, it will not interrupt network operations.

The key differences between IDS and IDPS solutions are summarized in Table 1.

	IDPS (IPS)	IDS	Comments
Able to Detect an Intrusion	✓	✓	
Able to Notify Administrator of Intrusion	✓	✓	
Able to Prevent Intrusion	✓	×	
Deployed out-of-band	×	✓	
Deployed in-band	✓	×	
Operational Stability	# 1 Priority	# 4 Priority	An IDPS failure is catastrophic. An IDS failure is a nuisance and a temporary security hole.
Network Performance	# 2 Priority	# 3 Priority	IDPS processing capability must match peak network load, and latency must be minimal: In the core, Latency ≤ 200 μs At the edge, Latency ≤ 10 ms. IDS processing capacity must match average network load, processing latency can be from seconds to minutes depending on the administrator's requirements
Zero False Positives	# 3 Priority	# 2 Priority	A false positive is never wanted: With an IDS: The administrator will be needlessly interrupted. With an IDPS: Network traffic will be needlessly interrupted.
Minimal False Negatives	# 4 Priority	# 1 Priority	A false negative means that the IDS or IDPS solution lacks accuracy. In the case of the IDS accuracy should be job one.

Table 1 Comparison of Key IDPS & IDS Characteristics

Determining How Many ID and IP Sensors are required

The network designer should consider locating ID and IP Sensors on any network segment where there is a possibility of malicious activity or data is considered to be highly sensitive and warrants protection.

The network designer will need to evaluate the network design, and if not already done, the designer will need to:

- Take an inventory all assets that require securing
- Rank the assets by sensitivity to attacks
- Partition the network into trust zones

Once these steps have been taken the designer can start to determine how many ID and IP sensors are required, if the sensors should be inline or passive, how the passive sensors will be connected and what performance capabilities are required from both the inline and passive sensors.

Where to deploy Network-based IDSs?

A Network-based IDS solution is only able to monitor traffic and cannot directly thwart an attack, as a result Network-based IDS solutions are typically used as passive mode sensors, they are placed out-of-band, and they are not placed in the traffic path.

When deployed as a passive mode sensor, should the packet processing capabilities of the IDS be exceeded, it will not affect network traffic in anyway, but the IDS may not be able to monitor all traffic.

Because it is located out-of-band a Network-based IDS will not impact network connectivity should the device fail.

Since Network-based IDS products cannot take direct action to prevent a detected exploit from taking over the system, Network-based IDS solutions should never be deployed where a prevention device is required.

Network-based IDS solutions might be deployed in the following locations:

- The boundary between two similar trust zones.
- Key network segments, such as trunks or uplink segments.
- Within an external access DMZ, or a DMZ being utilized to protect a critical host.
- To monitor traffic stream that is being generated by a load balancer

Figure 1 shows an IDS solution deployment. The IDS is monitoring (but not protecting) the traffic flows - in both directions - between Network 1 and Network 2. The IDS connection to the Security Management network is used to report an intrusion to the administrator and to communicate with other security tools.

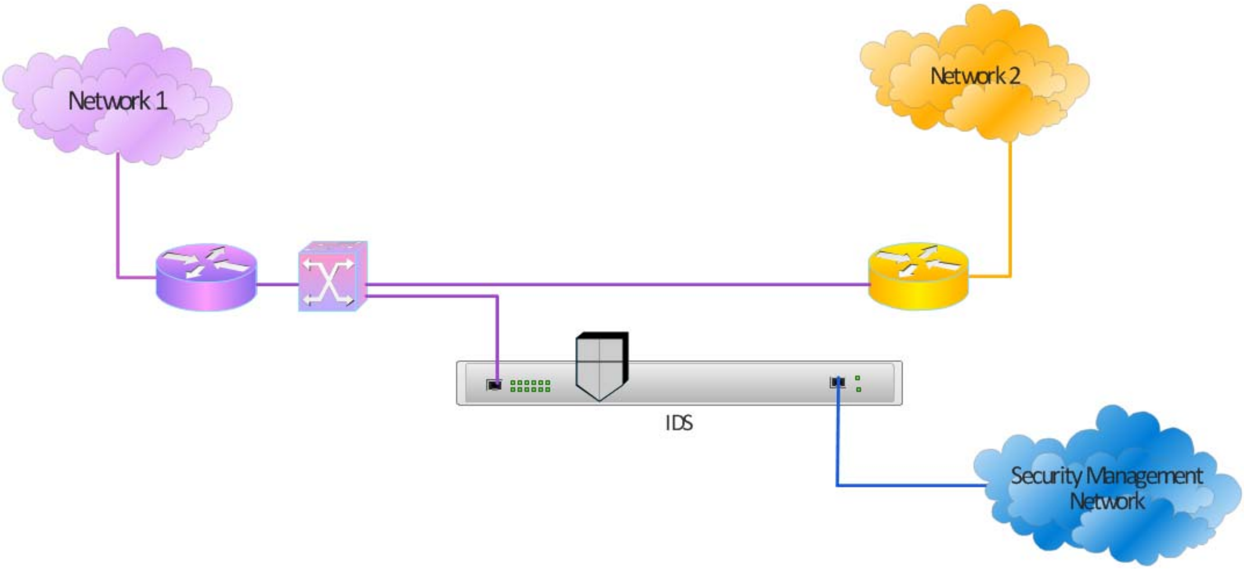

Figure 1 Deploying Network Based IDS

Where to deploy Network-based IDPSs?

A Network-based IDPS is able to take direct action when a threat is detected, but to be able to act upon the threat the sensor must be placed in-band with the traffic flow, as an inline sensor.

A Network-based IDPS must be chosen with enough packet processing capabilities so that it will not introduce a network bottle neck. The network designer must also consider what will happen to network connectivity in the event that the Network-based IDPS fails.

Quite often Network-based IDPS solutions are placed directly behind a network firewall or router; with this configuration the Network-based IDPS provides a complementary layer of traffic analysis. The inline sensor will also be in the right location to drop malicious packets or block traffic from a particular source thereby stopping the threat before it enters the network.

Sometimes a Network-based IDPS will be located so that it can protect a very sensitive host or trust zone, or possibly a SAN that contains highly sensitive data. When used to protect sensitive hosts sometimes the host will be deployed in a DMZ and the Network-based IDPS will be used in conjunction with a router to guard the DMZ where the host is located.

Figure 2 shows how an IDPS solution deployment. The IDPS is monitoring the traffic flows - in both directions - between Network 1 and Network 2. Should the IDPS detect suspicious traffic, it will block the traffic. The IDPS connection to the Security Management network is used to report an intrusion to the administrator and to communicate with other security tools.

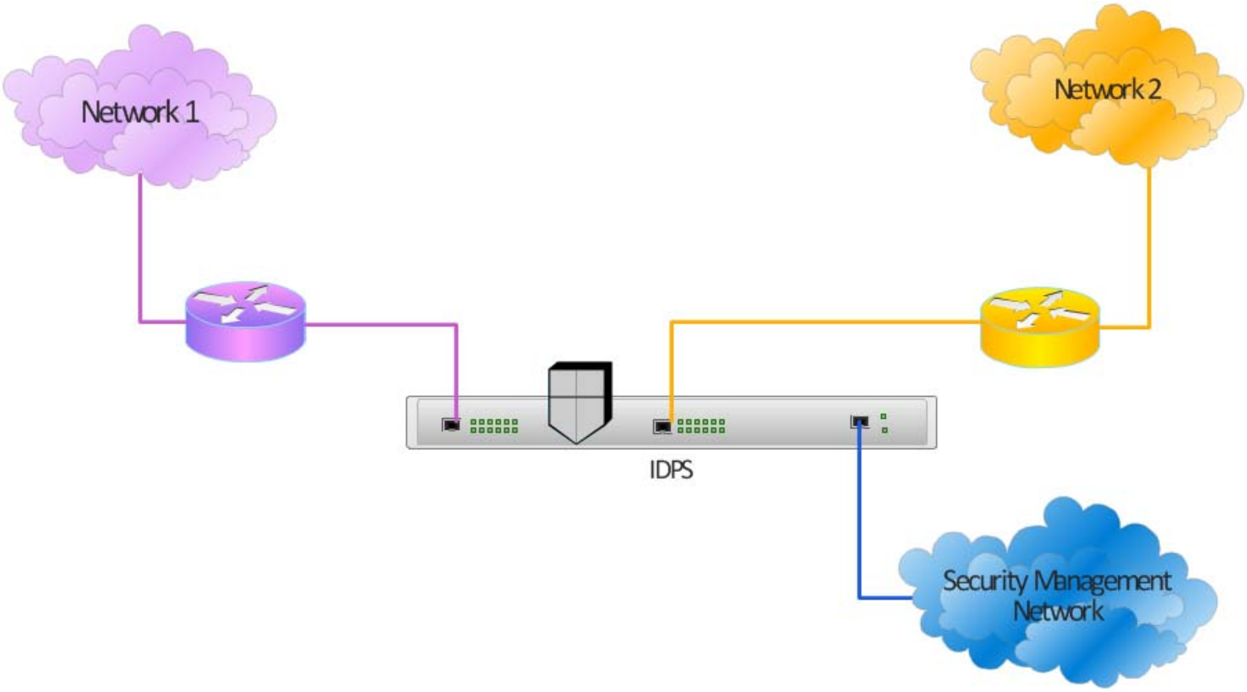

Figure 2 Deploying Network Based IDPS

Where Host-based IDPSs should be deployed?

Host-based IDPSs are intended for deployment on critical hosts. The IDPS monitors all of the inbound and outbound traffic related to the host, and it will raise an alarm should suspicious activity be detected. Some Host-based IDPSs will block ingress or egress traffic when it is warranted.

Host-based IDPSs may be deployed on critical servers and if necessary, client desktops.

Some Host-based IDPSs are appliance based and are located between the host being protected and the network similar to how a Network-based IDPS is deployed. However, the sensors usually monitor network activity for only one specific type of traffic, such as Web server access or database server access, so they are more specialized than a standard Network-based IDPS.

Where Should Network Behaviour Analysis IDPS be Deployed?

Network Behaviour Analysis (NBA) IDPS solutions are often used to monitor traffic flow behaviour between two internal networks, between two trust zones, or on the network backbones since the backbones carry an aggregation of traffic between several internal networks. NBA IDPSs are also deployed where they can monitor traffic flow behaviour between an organization’s internal network and an external network, such as the internet or possibly a business partner's network.

Wireless IDPS Solutions

With the exception of sensors, wireless IDPS solutions use the same types of components as Network-based IDPS solutions. Wireless IDPS sensors fulfill the same role as Network-based sensors, but they function differently and they are often integrated into components that are specific to wireless LANs.

Unlike Network-based sensors, wireless sensors do not analyze application layer data or network protocols; instead they are optimized for analyzing wireless protocol activity looking for suspicious activity.

Securing the IDPS Solutions

The network designer must give careful consideration to securing access to the IDPS solutions. This is very important because IDPSs are often the target of attackers. If an attacker can compromise an IDPS, the IDPS can be rendered useless in detecting subsequent attacks against the network.

IDPSs quite often contain information about host configuration that could be useful in planning additional attacks. The administrator should ensure that all IDPS solutions are kept fully up to date with the latest signature information and any relevant operational patches from the IDPS vendors.

Administrators should create separate accounts for each user and administrator of the IDPS, and assign each account only the necessary privileges.

Network devices such as firewalls, routers, and switches should be configured so as to limit direct access to all IDPS components to only those hosts that require access. If remote access to IDPS solutions is allowed, then strong authentication mechanisms should be in place.

The network designer is advised to use a dedicated management network for managing all of the IDPS solutions. If an IDPS solution is deployed without the use of a separate management network, then the network designer should consider the use of a VLAN to segregate the IDPS management plane.

The Security Management Network

Organizations should consider using a dedicated security management network for connecting security devices to each other, the SIEM and if required a management application.

The benefits of having a dedicated security management network for interconnecting security tools and the SIEM are:

- A dedicated security management network allows very strict access controls to be imposed on management interfaces and makes it very difficult for general users that are connected to the production network to gain access.
- If the production network is subjected to a DoS attack, or if some kind of a storm or flood is in play on the production network:
  - The administrator will still be able to access the management interfaces of the security tools and restore order.
  - Security tools will be able to communicate with each other and the SIEM so that attack information may be shared, alarms can be sent to the administrator and preventative measures can be communicated to other devices.
- If a networking device has failed on the production network, or a network connection has been severed - the administrator will still be able to reach the management interfaces of the security tools.

Dedicated security management networks are covered in more detail in the Mitel technical paper *Securing Mitel Cloud Based UC Networks.*

Choosing an IDPS Product

The process of selecting an IDPS product can be broken down into some basic steps; the steps involved are as follows:

1. Gain an understanding of available IDPS technologies.

2. Evaluate the network, identify the assets and then create an inventory of where the security weaknesses are and what exactly the weaknesses are.

3. Determine the type of IDPS solution that is required to eliminate each of the network security weaknesses that have been identified.

4. Conduct a survey of IDPS vendors, and currently available IDPS solutions that they are offering.

5. Evaluate the available IDPS products.

The preceding sections of this Chapter address Step 1 - Gaining an understanding of IDPS technologies.

Steps 2 and 3 are addressed in the Mitel technical paper *Securing Mitel Cloud Based UC Networks*, which discusses identifying the UC solution assets, securing the UC solution network, and provides recommendations as to where various security tools should be deployed.

The following sections are intended to provide the reader with guidance on how to address Steps 4 and 5 - conducting a survey of available IDPS solutions and what to consider when evaluating IDPS products.

Surveying IDPS Solutions & Vendors

Network designers may conduct their own surveys of available IDPS solutions, or they can rely on surveys that have already been conducted by third parties.

Third Party Surveys

Various organizations have conducted surveys which are available for free, however these surveys will many times have been sponsored by a particular vendor and reflect a vendor bias or a design methodology bias. Other organizations have conducted surveys and published reports which are available for a cost, these surveys will be of a better quality than free surveys.

In general, the old adage holds true, you get what you pay for.

If the network designer is relying on third party reports, another consideration to be aware of is the date of publication. In the world of security devices and tools, product life cycles are relatively short and corporate mergers and acquisitions are a way of life. If a survey/report is much older than 12 months, the network designer needs to be aware that much of the data will likely be stale and the value of the survey will decrease on a weekly basis.

Conducting Your Own Survey

Obviously the first step to conducting an IDPS product survey involves identifying a number of vendors of interest.

During this phase of the investigation the network designer should focus on vendors that are able to offer a complete suite of security solutions. A full suite of solutions should cover network, host, application and wireless IDPS solutions, as well as NGFW, NAC, WAF and SIEM solutions that all work together to provide an overall security solution. The vendors of interest should support on-going security updates via subscription services and the vendors should also have a strategy in place for threat intelligence sharing.

The network designer should also try to determine if the vendor's suite of offerings are based on products that they developed themselves or if the suite of offerings was cobbled together as a result of corporate mergers and acquisitions. Solutions that are put together through corporate mergers and acquisitions should be carefully evaluated since they typically lack cohesiveness and could be more difficult for the vendor to support should field issues arise.

Alternately, if a vendor does not offer a complete suite of security solutions, then the vendor should be offering products that have been proven to be interoperable with other vendor's security devices via an independent test lab, otherwise the onus will be on the network designer to verify interoperability prior to deploying the security solution into a live network.

Above all, the network designer should be aiming to deploy a fully unified security solution, rather than a solution that is based on a variety of products that may or may not be able to work together cohesively.

Balancing the Security Requirements against the Security Budget

Before starting the IDPS product evaluation process, the designer and IT personnel involved will need to understand their company's security requirements and they will need to know the extent of the company's budget for implementing security measures.

Once the security requirements and the amount of available funds have been determined, it will usually be necessary to balance the security requirements against the available funds in the IT/security budget.

For some organizations security will be paramount and the cost of security will not be an issue, other organizations will not have endowed their IT groups with a book of blank cheques, and the available funds for security measures will be limited.

Before engaging a security vendor and discussing a potential solution, the organization will have to determine if their security needs are high, medium or low and if they are prepared to spend money accordingly. The cost of security tools ranges from freeware solutions such as Snort, to unified commercial solutions costing well over a million dollars.

In trying to determine if the security needs are high, medium or low, the individuals involved need to keep in mind that the real objective is not about securing the network or devices on the network, the real objective is how to ensure the security of the organization's data and the security of the services provided over the network.

It is a lot easier to quantify the cost/benefit ratio of data theft, data loss or the costs should employees or customers be denied access to their UC services for an extended period of time, than it is to quantify the cost/benefit ratio of securing a network that by itself offers no tangible services.

Evaluating IDPS Products

This section discusses a number of IDPS parameters and operational capabilities that the network designer should take into consideration when evaluating and selecting an IDPS solution.

- What kinds of network events can the IDPS solution detect?
- DDoS
- Buffer overflow attacks
- Network scans
- Botnet communications
- Advanced malware detection
- Others

Interoperability

- Will all of the required IDPS solutions - network based IDPS, host based IDPS and Wi-Fi based IDPS - support integration/interoperability with each other and the SIEM to form a unified management system?
- Can the IDPS solutions integrate with open source security controls such as Snort?

- Do the IDPS products support IETF RFC4765, the Intrusion Detection Message Exchange Format (IDEMF), or are the message exchange protocols used by the product proprietary?

Event Correlation

- Do the IDPS solutions support event correlation capabilities to assist the administrator with troubleshooting efforts - so that response times are kept to a minimum?

Attack Signature Updates

- Are updates for attack signatures applied automatically from the vendor's site or manually installed by the customer? How frequent are attack signature updates?
- How often does the vendor update their own attack signature data base?
- Does the vendor have a solution to address zero day attacks?
- Are the IDPS solutions able to obtain threat information from multiple sources?

IDPS Operating System Updates

- How are IDPS solution operating system updates automatic or manual?
- How much IDPS downtime is required to perform an OS update?
- How are the IDPS operating systems protected from attacks?

Product Reliability/Availability

Anytime an IDPS is being deployed on a critical network segment, the network designer should consider the reliability of the product.

The IDPS manufacturer should make reliability/availability data available on the product data sheet, reliability is typically stated as Mean Time Before Failure (MTBF). When protecting critical network segments with an IDPS, the designer may want to consider a solution that supports resilient or redundant operation. Some points to consider are:

- When selecting any IDPS solution it is important to ensure that the when the IDPS solution fails, it fails in such a way that network connectivity is maintained.
- Do the network locations where in-line sensors are being deployed require high availability solutions, if so does the sensor meet the network availability requirements?
- If the vendor states that their product supports high availability, does the product offer true high availability, is there an automatic fail over to a secondary device should the primary device fail, does fail over occur fast enough for the particular application?

SIEM Considerations

- Will the SIEM or management system be able to handle the number, types of sensors being deployed, and the volume of data generated?
- Will the SIEM or management system be able to detect a sensor failure?
- How sophisticated is the SIEM, does the SIEM support automated event data correlation and analysis or is the system administrator burdened with performing event correlation and analysis?

- If sensor data is being correlated and analyzed by a third party managed Security as a Service provider, does the provider have access to the data flowing through the IDPS sensor? Is any network data routed through the managed security provider's network or equipment other than the IDPS solutions?

IDPS - Performance Considerations

When selecting an IDS or IDPS solution the network designer must consider the throughput and packet processing capabilities of the product. IDS and IDPS products are built for specific network speeds and applications; there are IDS and IDPS solutions on the market to meet the requirements of most businesses and also the most common network interface speeds.

The IDPS solution needs to be able to process packets at wire speed - the same speed as the network segment that it is protecting. When an IDPS solution is introduced into a network segment, the product's behaviour must be as close to transparent as possible. The IDPS solution must not cause network congestion and any network latency introduced by the solution should be kept as low as possible, especially on network segments carrying real time traffic such as VoIP telephony and video conferencing.

An IDS device should selected so that its packet processing capabilities closely match the wire speed of the network segment being monitored, but since the data flow is not through the IDS, IDS processing speed is not as critical a consideration as when selecting an IDPS solution.

The following table provides some examples of IDPS product families and available interface speeds.

Product	Available Interface Speeds
Cisco IPS 4200 Sensor	1 Gb/s, 600 Mb/s, 250 Mb/s & 80 Mb/s
IBM Proventia IPS	2 Gb/s, 1.2 Gb/s, 400 Mb/s, 200 Mb/s
Juniper Networks IDP	1 Gb/s, 500 Mb/s, 250 Mb/s & 50 Mb/s
McAfee IntruSheild Network IPS	2 Gb/s, 1 Gb/s, 600 Mb/s, 200 Mb/s & 100 Mb/s
Tipping Point	5 Gb/s, 2 Gb/s, 1.2 Gb/s, 600 Mb/s, 200 Mb/s & 50 Mb/s

Table 2 IDPS Product Interface Speeds

IDPS Product - Legal Considerations

The network designer should consider if the organization needs to comply with any legal requirements, and if these legal requirements have any bearing on IDPS selection. Law enforcement agencies may need to have access to IDPS logs during the course of an investigation into an attack, and the logs may need to be preserved as evidence if the instigator is brought before the courts.

Some organizations need to meet accreditation by certain authorities; these authorities may have requirements that are specific to IDPS products.

IDPS Product - Personnel Considerations

The network designer needs to determine if IT staff will be available 24/7 to monitor the IDPS solution. Some IDPS solutions require constant manual monitoring and maintenance, if 24/7 IT support personnel are not available or this burden is not feasible, then the designer needs to consider IDPS solutions that can function unattended.

When surveying IDPS solution vendors, the network designer and administrator need to ensure that the vendor can provide IT employees with the necessary training at a reasonable price.

Prior to deciding on a particular IDPS solution, the system administrator should consider what level of ongoing technical support the vendor can provide to IT personnel, what the response times are and what the ongoing support costs will be.

Conclusions

There are several organizations that publish reports comparing the capabilities of IDPS solutions, and these reports provide product selection recommendations; the network designer should make use of these resources.

Many IDPS and SIEM vendors often make their products available on a short term evaluation basis. The network designer may want to consider distilling down the survey results into a short list of potential vendors and then have the various IDPS offerings brought into their own labs for evaluation purposes.

At this time there are no standardized evaluation test methodologies for evaluating IDPS solutions and the obstacles involved in creating a comprehensive test suite are likely insurmountable.

However, some level of testing can offer the network administrator insight into how much effort is required to deploy, tune and maintain a particular IDPS solution.

The administrator may also be able to run the IDPS solutions through a small suite of tests with attack stimulus that includes benign threats and real threats, so that the security detection capabilities can be compared.

The tests that are probably the easiest and most straight forward for the administrator to conduct are network performance tests. Network performance tests need to be performed so that the administrator can determine if the IDPS solutions can keep up with the expected volume of network traffic.

Network throughput and latency tests will be of extreme importance to the network administrator of a UC solution since real-time applications such as VoIP telephony and video conferencing have very stringent network transmission requirements.

Further information on selecting an IDPS solution and vendor can be found in the following documents:

- The NIST Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS).
- The SANS Institute InfoSec Reading Room document called - Selecting an Intrusion Detection System.
- The ITsecurity document called, IDS IPS Buyer's Guide
- The ITsecurity document called, Intrusion Detection Systems Comparison Table

Powering connections