

CounterSnipe Technologies

Intrusion Prevention Architectures

Introduction

Intrusion Prevention is a new technology that includes traditional Firewall technology as well as many aspects of Intrusion Detection technologies. It is designed to filter unauthorised traffic on your network and does this by not only Firewalling all connections, but by also evaluating all data streams with the Snort-inline intrusion prevention engine for signatures of unauthorised traffic.

The APD is a versatile device that can be used in many different configurations and this paper explores the design objectives for Intrusion Prevention Architecture.

Theoretical architecture

The ideal architecture will evaluate the different levels of the OSI for signatures of unauthorised traffic.

<i>OSI level</i>	<i>TCP model</i>	<i>Security technology</i>
Physical	Link	Physical isolation, access control, VLANs, Spanning tree controls, Man with gun
Data link		
Network	Network	Routing Firewalls
Transport	Transport	
Session	Application	Application filtering
Presentation		
Application		

To therefore have a complete security model implementation, you should consider physical and link layer security, routing firewalls and application filtering either by themselves or in combination or even with multiple overlapping solutions for defence in depth requirements.

Factors that might influence your architectural set-up

Security objectives

Confidentiality, integrity, authentication and non-repudiation are requirements that can be met with many different technological solutions.

Availability, reliability, serviceability, survivability, recoverability and continuity are also factors that will affect your choice of architecture.

Defence in depth

To ensure that failure of a single component does not lead to catastrophic failure in the case of critical dependencies, redundant designs might include different technologies possibly from different layers to minimise the risk of emergent vulnerabilities in individual products.

Performance

The load/performance requirements of the various different devices generally increase the higher you go in the OSI layers because of protocol complexity and technology maturity. There might therefore be increase requirement for larger devices to handle higher levels in the OSI.

Vulnerability of devices

The same devices that you use in your security architecture might themselves be vulnerable and therefore might be restricted where you place them in the architecture.

Disaster recovery

A single point of failure is in general a problem and a redundant design is required to ensure the functionality of your security architecture.

APD Security architectures

The APD product range is primarily an application-screening device (Layer 4-7) that includes powerful traditional firewall capabilities (Layer 3) and is designed to primarily function on a bridging level (Layer 2).

Since the APD is designed to function on a Layer 2 level, there is no requirement for any modifications to your routing environment, even if you want to make use of the Layer 3 capabilities of the device. The APD can be placed anywhere on an Ethernet segment, ranging from 10BaseT to 1000BaseT and 1000Base SX/SL, and it will allow forwarding of packets based on its evaluation of Layer 3-7 traffic.

Small environments

Architectural questions:

1. Use a single device for firewall and application filtering?
2. Should this device be connected directly to the Internet?

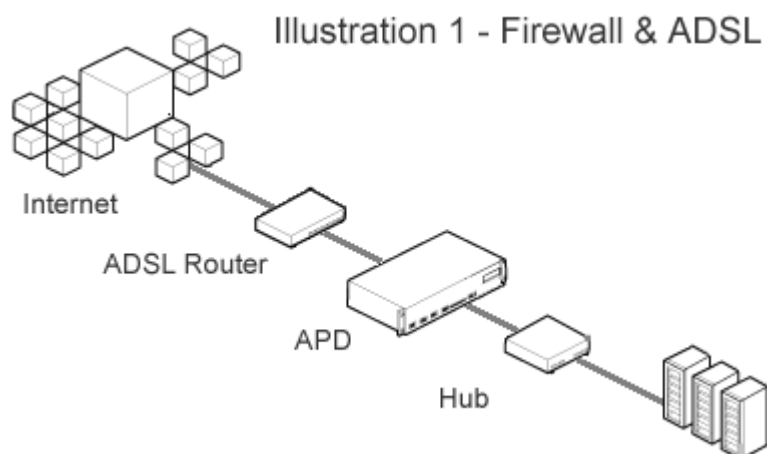
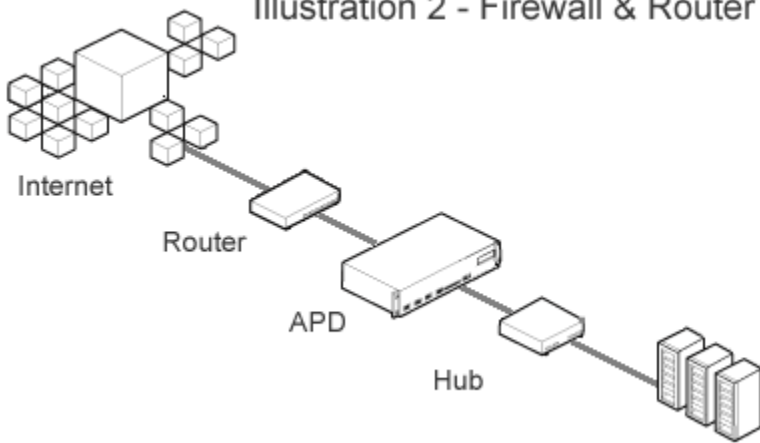


Illustration 2 - Firewall & Router



In small environments the APD can function as both a firewall and an application-screening device. This allows you to connect the APD directly to the Internet or use it as a firewall device behind your router. If the APD is used as both an application screening device and a firewall, then the powerful features of the IP tables firewall can be used to do connection tracking (only allowing connections back into your environment that originated there),

rate limiting and many other IP tables components available.

Medium size environments

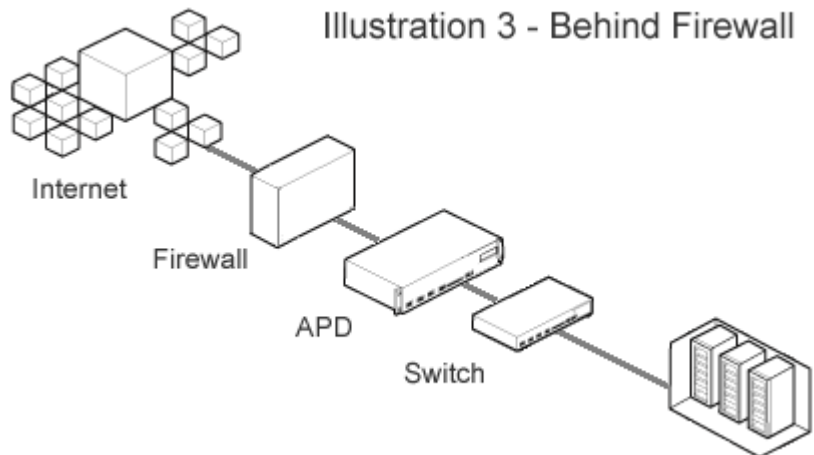
Architectural questions:

1. Use a single device for firewall and filtering?
2. Size and place the device to handle peak load.

In medium sized environments, the APD is implemented behind the firewall to provide defence in depth. It is possible to implement only the APD as both a firewall and an application-screening device.

The standard placement of the APD is behind the firewall, however, there might be specific requirements to reverse this set-up.

Illustration 3 - Behind Firewall



Large environments

Architectural questions

1. Load sharing to achieve capacities higher than what a single device can manage.
2. High availability configuration

The DMZ can be firewalled with the APD or individual machines in the DMZ can be placed behind an APD.

In large environments the number of configurations options are quite large. It can be seen from the diagrams that both load sharing and high availability configurations are supported.

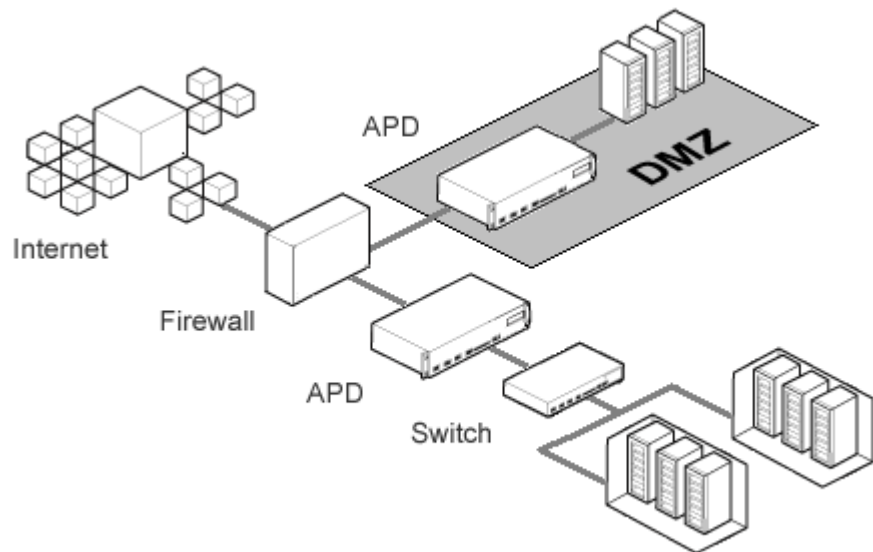


Illustration 6 - DMZ configuration

It is also possible to use the APD as an internal Firewall to do both Firewalling and application screening between internal campuses.

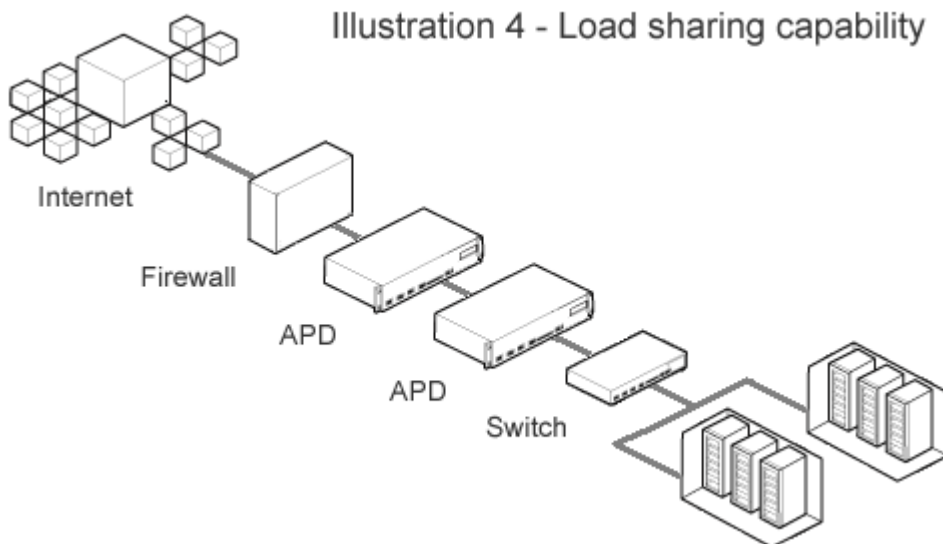
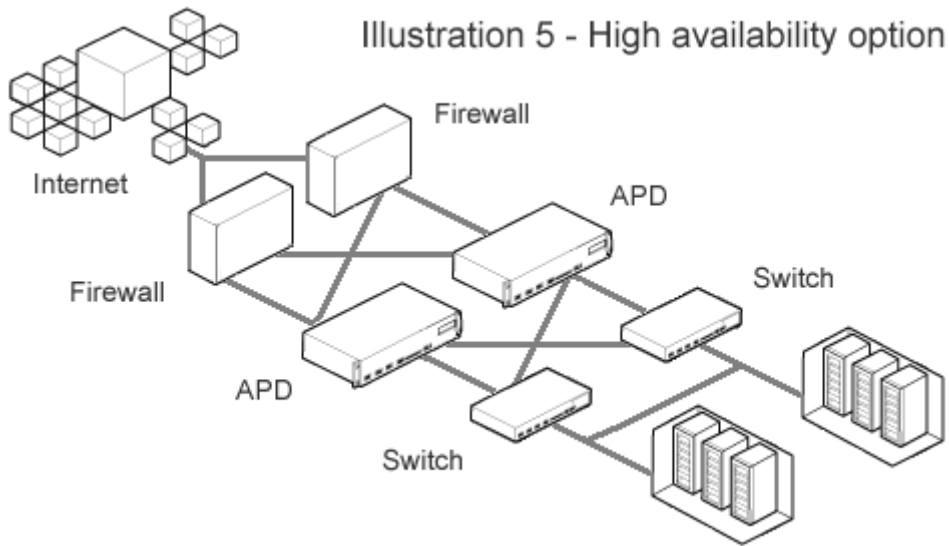


Illustration 4 - Load sharing capability

The APD can also have more than just 2 Ethernet interfaces bridging in your environment so it is possible connect a number of Ethernet segments together in a secure manner.



Summary

CounterSnipe APD can be confidently deployed with a high degree of flexibility into diverse network scenarios to provide powerful, accurate high speed detection and defence against known bad traffic and zero day exploits, whilst maintaining complete network integrity.

About CounterSnipe Technologies

Countersnipe Technologies is dedicated to the provision of IT security products with a focus on maximum Active Protection of corporate infrastructures.

The team at CounterSnipe have been working together since early 2002 to develop our flagship product the Active Protection Device for in-line protection of corporate assets. The emphasis on ensuring a precision delivery of engineering elements in all of the products we build, ensures world-class solutions for our customers.

Countersnipe is a privately held company Headquartered in Atlanta, Georgia with an ever-increasing presence in the International markets.

CounterSnipe Technologies
1230 Peachtree Tower
Suite 1800
Atlanta
Georgia 30309
USA