# Market Central®

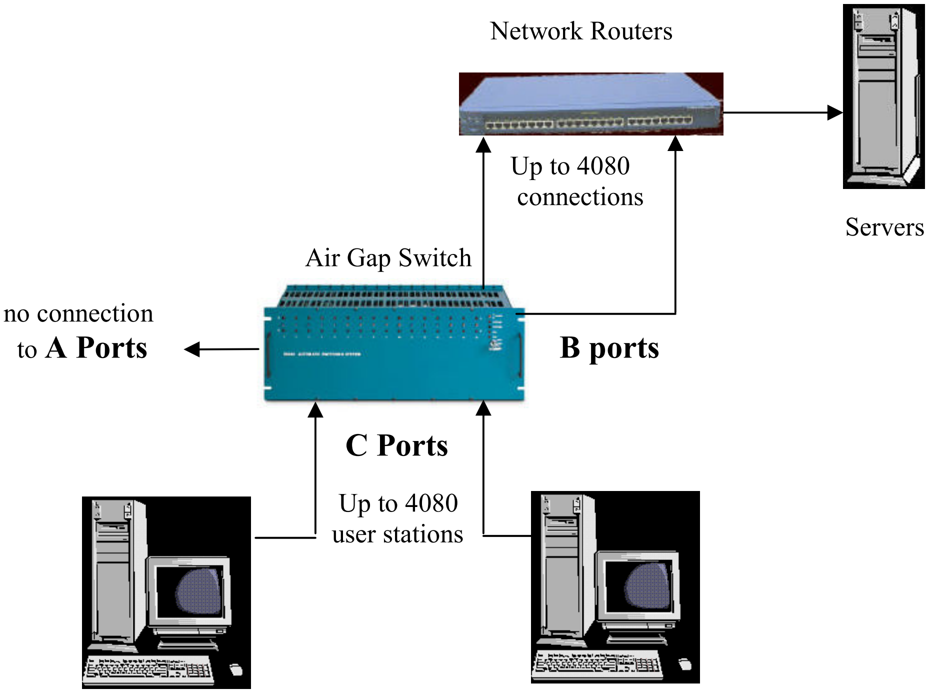
**www.secureswitch.com**

## Air Gap Isolation and Network Access Control are Vital to a Comprehensive IT Risk-Management Strategy

Some network security experts would like you to believe that air-gap isolation is fundamentally flawed, bad practice, and an unachievable myth. Their argument often focuses on the need to perform S/W updates to devices on the network or periodically refreshing stored data files using external sources. If you do any of these things then they claim that your air gap isolated network isn't isolated at all and anyone using this approach, is at best, a fool.

The truth is that the above reasoning is one dimensional – air gap isolation has an important, and in many cases, a critical role to play in protecting your network & IP assets. But as these experts point out, you also need to incorporate additional measures into your overall security paradigm to address other threat modes.

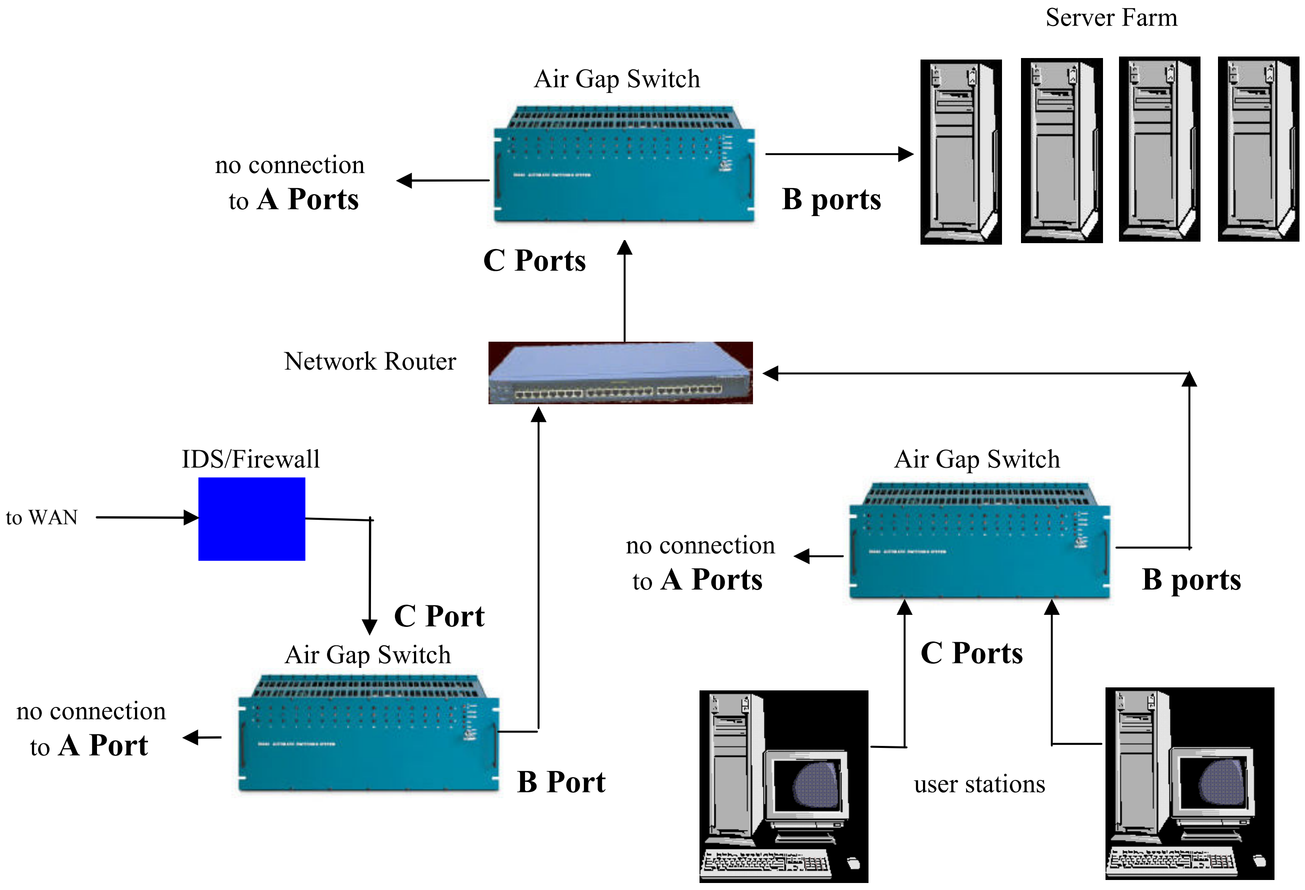
When an air-gap switch is used to isolate a device or a network, the wired connection is physically broken and data transfer using this path is 100% disabled – no ifs, ands or buts. When is this useful? If you want to minimize the risk of unauthorized data transfers via authorized devices, air-gap switches can sever the physical connections between these known access points and your data storage. Many data breaches are perpetrated by trusted individuals using authorized resources after normal working hours to transfer information when network security staff is often significantly reduced and scrutiny is lessened and/or responses are delayed. An air gap switch that disconnects authorized resources after hours reduces the probability of a data breach by shrinking the window of opportunity.



With air-gap layer 1 network access control you can enable or disable the connection between one or more work stations and the network to help prevent unauthorized file transfers.

Likewise, if sections of your network do not typically require external access, doesn't it make sense to only connect these segments when needed, and then only when direct monitoring can help prevent unauthorized transfers and attacks? Controlling the connection in this way also "randomizes" access, making it much harder for a hacker to penetrate your network.

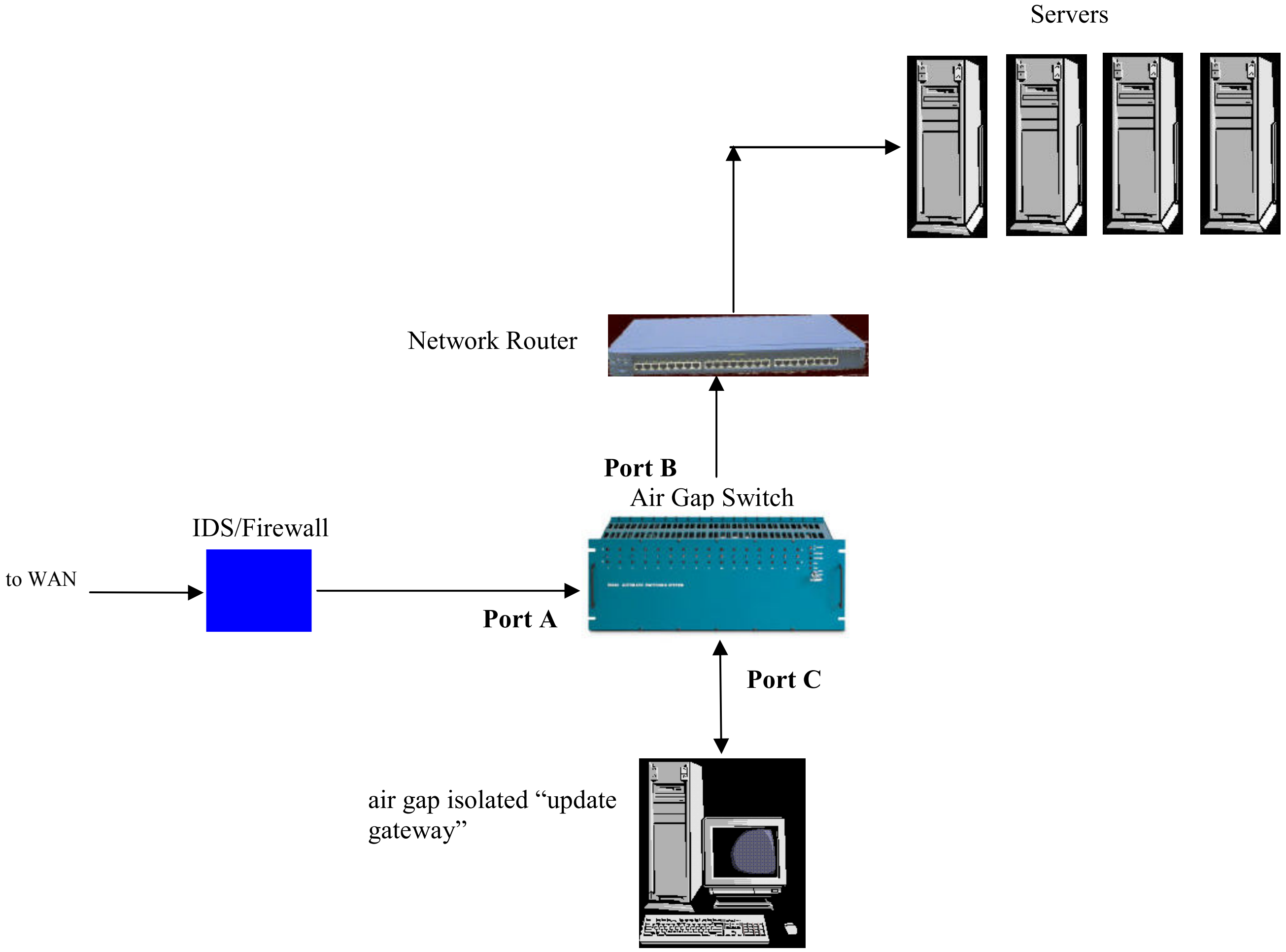
Should your IDS or IPS detect an attack in progress, using an air gap switch to break the network connection can be the difference between containment and becoming front page news. You may not be able to prevent an attempt, but you can take positive steps once an attack is detected to minimize the damage. The first step often should be to isolate the point of attack from the rest of the network. You may also want to isolate different network segments from one another to help prevent the spread of viruses or other malware. Air-gap switches properly deployed at key points in your network will help you contain the attack and limit its damage.



An air-gap layer 1 switch can be used to automatically disable various connections in your network when your Intrusion Detection System detects an attack in progress.

What about wireless, you ask? Proper security measures need to include limiting the operating modes of wireless end-point devices so that they can only connect to your trusted access points and not be used as a backdoor entry into your network. Additionally, air gap switches that disconnect your access points from the network after hours or when threats are detected provide additional security, again reducing the window of opportunity that perpetrators have for gaining access to your assets.

Periodic maintenance and updates can often be made easier as well as more secure using air-gap switches. By dedicating an air-gap isolated device for use as an "update gateway", you can first verify the update on the dedicated device, and then once you are satisfied the update is clean and doesn't introduce any other problems (i.e. unadvertised features ;-) you can roll out the update across any required sections of your network.



Limit your exposure to infected patches and malware when downloading updates by using an air-gap isolated, dedicated workstation to inspect, validate and test the update in an isolated environment prior to distributing the update across your network.

No one network security device/approach should be trusted to protect your information and resources from all threats. By developing an overall security plan and regularly reviewing it against new threats and changes to your environment, you can make it very very hard for the bad guys. A friend in the pest control business once told me that it isn't always necessary to kill all the pests around your house, you can often achieve good results by simply making your house a lot less desirable than your neighbors'. Market Central layer 1 air gap switches can do this for your network.