

Layered Network Security Design Considerations: When Layers Collide

Donald MacLeod
Senior Incident Response Officer
Office of Critical Infrastructure Protection and Emergency Preparedness

David Whyte
Senior Incident Response Officer
Office of Critical Infrastructure Protection and Emergency Preparedness

© Minister of National Defence, on behalf of The Office of Critical Infrastructure Protection and Emergency Preparedness, Canada, 2001.

In consideration for this workshop, we submit the following position paper. This paper should not be taken or interpreted as representing the views of our employer, The Department of National Defence / Office of Critical Infrastructure Protection and Emergency Preparedness, nor those of the Government of Canada.

Computer networks are complex and heterogeneous environments. Internet connectivity compounds the problem by exposing the network to a host of security concerns. To address these concerns and to effectively safeguard organizational assets an appropriate security posture is required. One such security posture is called “layered network security”. Layered network security involves the development of sound organizational security policies and the strategic deployment of appropriate risk-based security measures thereby reducing the possibility of circumvention through single points of failure.

Layered network security is not confined to the application of multiple technologies such as a firewalls, and intrusion detection systems (IDS). Layering can be multiple applications of the same or similar technologies. An example of this would be the deployment of an IDS in the network segment in front of a firewall and an IDS in the corresponding network segment behind the firewall. The benefit of this strategy is that it gives not only added degrees of the same protection, but also different vantages on suspicious network activity. For example, a network based intrusion detection system might detect an attack but be unable to say if the attack was successful. A complimentary host based IDS would often be in the best position to determine if the attack was successful.

In order to identify and implement the proper countermeasures required to secure a computer network a detailed analysis of the threats to those assets must be undertaken. It is essential during this process to properly articulate the threats to the network. A useful characterization of threats includes identifying the following attributes: threat agent, motivation, expertise, previous reconnaissance activities, and suspected attack methods. Once the identification of threats is complete the proper combination of countermeasures to provide essential security services (i.e. confidentiality, integrity, and availability) can be selected and applied.

Network architectures that adopt a layered network security approach are better able to effectively contend with network attacks. These networks are designed to implement a robust security posture capable of resisting, responding and recovering from attacks. Achieving a layered security architecture, however, is not without challenges. As with most IT solutions they are subject to the often competing constraints of:

- operational requirements
- ease of use
- cost
- adherence to organizational security policies
- resources (personnel/time)

Effective layered network security designs must take into consideration all these factors and ensure that the overall security posture of the network is improved with the deployment of each additional countermeasure. Security solutions designed to work in concert, not isolation, achieve a higher security posture. There are some instances when the deployment of security countermeasures can be detrimental to the overall security posture if the entire network is not treated as a single virtual unit. Security countermeasures used to mitigate a threat can actually impede or negate the effectiveness of the other security countermeasures resident on the network. Assessing if the overall survivability of the network has been enhanced, maintained or reduced can be a difficult task. Large organizations that separate technology and security into autonomous units are especially susceptible to this phenomenon.

The following table, *Potential security countermeasure conflicts*, contains examples of how the overall security posture of a network can be possibly weakened by the deployment of security countermeasures that do not take into consideration the overall network security posture. The intent is not to provide an exhaustive list but to highlight the challenges that organizations face when attempting to implement effective layered security to aid overall survivability. It is not our intention to discourage the deployment and use of multiple layers of security devices within a network; rather it is to emphasize that organizations must assess and understand the impact of their interactions.

Potential security countermeasure conflicts

<p>Virtual Private Network (VPN)</p> <p>VPN technology has greatly enhanced the ability of organizations to use the untrusted Internet as a trusted network by securely connecting remote workers or business partners. VPN technology relies on the use of encryption to secure all transmitted data. Many IDS are signature-based; that is they contain a repository of patterns or signatures that known attacks generate. IDS inspects network traffic as it is transmitted and compares it to these signatures raising an alarm if a match is found. Encryption insures the confidentiality of the data but it also impedes IDS. If network traffic is encrypted, pattern matching will not be possible and the IDS will fail to work properly.</p>
<p>Switches</p> <p>A network that employs switching technology increases both throughput and security. A switched network fabric insures that the network traffic is not broadcast to all hosts on the network segment but only to the intended hosts. Network traffic is separated and sent only to the port on the switch that is servicing the receiving host. Successful network penetrations are often followed by the installation of packet sniffers to gain further access to the network. One of the methods to help mitigate this type of threat is the use of a switched network fabric. A network sniffer in such an environment would not be able to collect all network traffic, only that traffic sent to the compromised system hosting the packet sniffer. While this can be effective in reducing the impact of a illicit sniffer, that same technology will make the effective deployment of an IDS problematic. Although many switches have the capability to mirror all data to a single port, often referred to as a monitor port, these ports are often in high demand. Network operations staff are in competition with the network security staff for these ports. In the worst case the deployment of an IDS can be totally ineffective if the network staff are not aware of the special needs of an IDS sensor and it is not connected to the monitor port. There are also bandwidth aggregation issues, where the entire volume of data on the switch might not effectively be transmittable to one port.</p>
<p>Encrypted E-mail</p> <p>The use of E-mail encryption can be very effective in maintaining the confidentiality of the data in the e-mail message. Once encrypted E-mail is sent the sender can be reasonably sure that no one except the intended recipient can read the message. Virus scanning at the gateway of an organization provides very effective risk mitigation against the threat of viruses. A virus scanner works by opening the e-mail message and looking for suspicious attributes. If messages are encrypted, then scans of the messages for viruses will be ineffective. Certain e-mail virus scanners can detect the use of encryption and quarantine the document as precaution. Quarantining, however, is a non-transparent and time-consuming solution.</p>
<p>Multiple Internet connections</p> <p>Denial of Service attacks are prevalent on the Internet, and organizations require practical solutions to help reduce their effects. An effective but expensive solution is to simply purchase and deploy more IT infrastructure to cope with the increase in network traffic. This can involve the installation of multiple data lines from multiple ISP's in order to have more robust network architectures. In such complicated network architectures, however, the deployment of security devices such as IDS now also becomes more complicated. If data from all the IDS sensors cannot be fused and correlated, the organization could be missing key information about malicious activity being directed towards their network.</p>
<p>Network Address Translation (NAT)</p> <p>A firewall that performs network address translation can help to mask a network topology from the outside by assigning a single IP address to a traffic that originates from the network. One of the key items an organization will use to determine who is directing malicious activity at their network is the IP address. The NAT makes incident investigation more complicated as the security personnel have to correlate IP addresses with attacks on internal systems that all have the same address, that of the firewall. Organizations that do not log properly, use dynamic IP addresses, or perform incident analysis in non-real time will face significant incident management challenges.</p>

Network security policy
A documented network security policy is a cornerstone for good security; a firewall that does not comply with a well thought out and documented security policy can quickly suffer from rule creep. However if the high-level policy staff do not understand front-line operations, the resulting policy can leave the system security staff unable to effectively defend the network.
Distributed IDS
Distributed IDS systems across an enterprise can provide invaluable information when the alarm data can be centrally collected and analyzed. In order for this data to be transmitted back to a central operations console inside a network, it generally has to be passed through the firewall. Usually a port on the firewall has to be opened to allow connections so that data transfer can occur thus weakening the security posture of the firewall.
High speed lines
High-speed lines are a common occurrence in modern networks. One advantage of this increase in bandwidth is it allows security staff to rollout large patches and upgrades quickly to a distributed server network. IDS systems can often have problems with high-speed networks if the traffic volume or traffic distribution overwhelms either the IDS sensor or the human dealing with the alerts.
Multiple vendor solutions
Many organizations when layering security will deploy multiple vendor products to form their security perimeter in order to mitigate the results of a vulnerability in one vendor-specific product at any given point in time. Given the complexity and functionality of many modern security devices it may be difficult for the security staff to competently deploy these devices on the network. Security staff will be burdened with having to configure and operate new and unfamiliar network devices. This increases the probability of configuration errors and thus vulnerabilities.
Active response
Many IDS products have the capability to automatically respond to attacks by reconfiguring firewalls, routers and other network devices. Active response allows for lights-out operations of a network when staff are not able to manually respond. When the firewall is reconfigured, it is trusting that the IDS has made a correct determination of the data in question; this can be a false assumption. Current IDS technology is still a "human in the loop" endeavor. Having a firewall and an IDS working in concert is a very effective layering of defence, however when the normal traffic is misidentified, or a malicious actor spoofs IP's, you can perform a self denial of service against trusted partners or even on your own network.
Network taps
Networks taps are effective at making an IDS sensor invisible to a network by allowing only one-way communication from the network to the sensor. This allows the IDS sensor to discreetly collect data in hostile or scrutinized environments. A number of IDS system allow the IDS to take action against the attacker when an alarm goes off by issuing TCP resets against the traffic stream. In the case of an IDS behind a tap, this cannot happen since the tap will prohibits outbound traffic.

Conclusions

Just as security is often a balance between performance and functionality, security by itself can be a balancing between different security countermeasures and methodologies. Without objective metrics to evaluate the effectiveness of security systems, and the complete knowledge of the interactions and dependencies between the various systems, an organization cannot adequately understand all of the risks they have assumed under their threat risk assessment.

Regardless of the specific network architectures there exists a number of concepts, which if adhered too will lead to effective layered security:

1. Malicious network activity must be detected before effective response can occur
2. Avoid single points of failure
3. Security solutions should be architected to work in concert not isolation
4. Anything not explicitly allowed should be denied
5. Systems will be compromised. They must be designed to resist attacks and subsequent compromises
6. Scalability, distributed solutions, and interoperability increase complexity and may introduce non-linear security challenges
7. Network topologies as well as security countermeasures must be constantly updated as they can only defend against known and current threats and vulnerabilities
8. Active scanning should be an ongoing part of the security posture
9. Minimize the footprint of the network visible to the Internet
10. Push security solutions away from the end user. Unless security is transparent it will probably be ignored or turned off

Designing secure network architectures is a daunting and asymmetrical task. Network architects must identify and ensure that all vulnerabilities are adequately addressed in order to secure a network. Attackers only have to identify and exploit enough vulnerabilities to penetrate a network. Networks that employ a layered network security posture are attack-resistant, robust, more secure and therefore more survivable.