netwrix

Network Security Best Practices

Understand the OSI Model

The International Standards Organization (ISO) developed the Open Systems Interconnect (OSI) model in 1981. It consists of seven functional layers that provide the basis for communication among computers over networks, as described in the table below. You can easily remember them using the mnemonic phrase "All people seem to need data processing." Understanding this model will help you build a strong network, troubleshoot problems, develop effective applications and evaluate third-party products.

Layer	Function	Protocols or Standards
Layer 7: Application	Provides services such as e-mail, file transfers and file servers	HTTP, FTP, TFTP, DNS, SMTP, SFTP, SNMP, RLogin, BootP, MIME
Layer 6: Presentation	Provides encryption, code conversion and data formatting	MPEG, JPEG, TIFF
Layer 5: Session	Negotiates and establishes a connection with another computer	SQL, X- Window, ASP, DNA, SCP, NFS, RPC
Layer 4: Transport	Supports end-to-end delivery of data	TCP, UDP, SPX
Layer 3: Network	Performs packet routing	IP, OSPF, ICMP, RIP, ARP, RARP
Layer 2: Data link	Provides error checking and transfer of message frames	Ethernet, Token Ring, 802.11
Layer 1: Physical	Physically interfaces with transmission medium and sends data over the network	EIA RS-232, EIA RS-449, IEEE, 802

Understand Types of Network Devices

To build a strong network and defend it, you need to understand the devices that comprise it. Here are the main types of network devices:

- ✓ **Hubs** connect multiple local area network (LAN) devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. Hubs do not perform packet filtering or addressing functions. Hubs operate at the Physical layer.
- ✓ **Switches** generally have a more intelligent role than hubs. Strands of LANs, are usually connected using switches. Mainly working at the Data Link layer, they read the packet headers and process the packets appropriately. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.
- ✓ **Routers** help transmit packets to their destinations by charting a path through the sea of interconnected network devices. They remove the packets from the incoming frames, analyze them individually and assign IP addresses. Routers normally work at the Network layer of the OSI model.
- ✓ **Bridges** are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware Media Access Control (MAC) addresses for transferring frames. Bridges work only at the Physical and Data Link layers of the OSI model.
- ✓ **Gateways** normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them.

Know Network Defenses

Using the proper devices and solutions can help you defend your network. Here are the most common ones you should know about:

- ✓ **Firewall** — One of the first lines of defense in a network, a firewall isolates one network from another. Firewalls either can be standalone systems or included in other devices, such as routers or servers. You can find both hardware and software firewall solutions; some firewalls are available as appliances that serve as the primary device separating two networks.

- ✓ **Intrusion detection system (IDS)** — An IDS enhances cybersecurity by spotting a hacker or malicious software on a network so you can remove it promptly to prevent a breach or other problems, and use the data logged about the event to better defend against similar intrusion incidents in the future. Investing in an IDS that enables you respond to attacks quickly can be far less costly than rectifying the damage from an attack and dealing with the subsequent legal issues.

- ✓ **Intrusion prevention system (IPS)** — An IPS is a network security solution that can not only detect intruders, but also prevent them from successfully launching any known attack. Intrusion prevention systems combine the abilities of firewalls and intrusion detection systems. However, implementing an IPS on an effective scale can be costly, so businesses should carefully assess their IT risks before making the investment. Moreover, some intrusion prevention systems are not as fast and robust as some firewalls and intrusion detection systems, so it might not be an appropriate solution when speed is an absolute requirement.

- ✓ **Network access control (NAC)** involves restricting the availability of network resources to endpoint devices that comply with your security policy. Some NAC solutions can automatically fix non-compliant nodes to ensure it is secure before access is allowed. NAC is most useful when the user environment is fairly static and can be rigidly controlled, such as enterprises and government agencies. It can be less practical in settings with a diverse set of users and devices that are frequently changing, which are common in the education and healthcare sectors.

- ✓ **Web filters** are solutions that by preventing users' browsers from loading certain pages from particular websites. There are different web filters designed for individual, family, institutional and enterprise use.

- ✓ **Proxy servers** act as negotiators for requests from client software seeking resources from other servers. A client connects to the proxy server, requesting some service (for example, a website); the proxy server evaluates the request and then allows or denies it. In organizations, proxy servers are usually used for traffic filtering and performance improvement.

- ✓ **Anti-DDoS** devices detect distributed denial of service (DDoS) attacks in their early stages, absorb the volume of traffic and identify the source of the attack.

- ✓ **Load balancers** are physical units that direct computers to individual servers in a network based on factors such as server processor utilization, number of connections to a server or overall server performance. Organizations use load balancers to minimize the chance that any particular server will be overwhelmed and to optimize the bandwidth available to each computer in the network.

- ✓ **Spam filters** detect unwanted email and prevent it from getting to a user's mailbox. Spam filters judge emails based on policies or patterns designed by an organization or vendor. More sophisticated filters use a heuristic approach that attempts to identify spam through suspicious word patterns or word frequency.

Segregate Your Network

Network segmentation involves segregating the network into logical or functional units called zones. For example, you might have a zone for sales, a zone for technical support and another zone for research, each of which has different technical needs. You can separate them using routers or switches or using virtual local area networks (VLANs), which you create by configuring a set of ports on a switch to behave like a separate network.

Segmentation limits the potential damage of a compromise to whatever is in that one zone. Essentially, it divides one target into many, leaving attackers with two choices: Treat each segment as a separate network, or compromise one and attempt to jump the divide. Neither choice is appealing. Treating each segment as a separate network creates a great deal of additional work, since the attacker must compromise each segment individually; this approach also dramatically increases the attacker's exposure to being discovered. Attempting to jump from a compromised zone to other zones is difficult. If the segments are designed well, then the network traffic between them can be restricted. There are always exceptions that must be allowed through, such as communication with domain servers for centralized account management, but this limited traffic is easier to characterize.

Segmentation is also useful in data classification and data protection. Each segment can be assigned different data classification rules and then set to an appropriate level of security and monitored accordingly. An extreme example of segmentation is the air gap — one or more systems are literally not connected to a network. Obviously, this can reduce the usefulness of many systems, so it is not the right solution for every situation. In some cases, however, a system can be sensitive enough that it needs to not be connected to a network; for example, having an air-gapped backup server is often a good idea. This approach is one certain way of preventing malware infections on a system.

Virtualization is another way to segment a network. Keep in mind that it is much easier to segment virtual systems than it is to segment physical systems. As one simple example, consider a virtual machine on your workstation. You can easily configure it so that the virtual machine is completely isolated from the workstation — it does not share a clipboard, common folders or drives, and literally operates as an isolated system.

Types of Network Segments

Network segments can be classified into the following categories:

- ✓ **Public networks** allow accessibility to everyone. The internet is a perfect example of a public network. There is a huge amount of trivial and unsecured data on public networks. Security controls on these networks are weak.
- ✓ **Semi-private networks** sit between public networks and private networks. From a security standpoint, a semi-private network may carry confidential information but under some regulations.
- ✓ **Private networks** are organizational networks that handle confidential and propriety data. Each organization can own one or more private networks. If the organization is spread over vast geographical distances, the private networks at each location may be interconnected through the internet or other public networks.
- ✓ **Demilitarized zone (DMZ)** is a noncritical yet secure region at the periphery of a private network, separated from the public network by a firewall; it might also be separated from the private network by a second firewall. Organizations often use a DMZ as an area where they can place a public server for access by people they might not trust. By isolating a server in a DMZ, you can hide or remove access to other areas of your network. You can still access the server using your network, but others aren't able to access further network resources.
- ✓ **Software-defined networking (SDN)** is a relatively recent trend that can be useful both in placing security devices and in segmenting the network. Essentially, in an SDN, the entire network is virtualized, which enables relatively easy segmentation of the network. It also allows administrators to place virtualized security devices wherever they want.

Place Your Security Devices Correctly

As you design your network segregation strategy, you need to determine where to place all your devices. The easiest device to place is the firewall: You should place a firewall at every junction of a network zone. Each segment of your network should be protected by a firewall. This is actually easier to do than you might think. All modern switches and routers have firewall capabilities. These capabilities just need to be turned on and properly configured. Another device that obviously belongs on the perimeter is an anti-DDoS device so you can stop DDoS attacks before they affect the entire network. Behind the main firewall that faces public network, you should have a web filter proxy.

To determine where to place other devices, you need to consider the rest of your network configuration. For example, consider load balancers. If we have a cluster of web servers in a DMZ, then the load balancer needs to be in the DMZ as well. However, if we have a cluster of database servers in a private network segment, then the load balancer must be placed with that cluster. Port mirroring will also be placed wherever your network demands it. This is often done throughout network switches so that traffic from a given network segment is also copied to another segment. This can be done to ensure that all network traffic is copied to an IDS or IPS; in that case, there must be collectors or sensors in every network segment, or else the IDS or IPS will be blind to activity in that segment.

Network aggregation switches are another device for which there is no definitive placement advice. These switches aggregate multiple streams of bandwidth into one. One example would be to use an aggregation switch to maximize bandwidth to and from a network cluster.

Use Network Address Translation

Network address translation (NAT) enables organizations to compensate for the address deficiency of IPv4 networking. NAT translates private addresses (internal to a particular organization) into routable addresses on public networks such as the internet. In particular, NAT is a method of connecting multiple computers to the internet (or any other IP network) using one IP address.

NAT complements firewalls to provide an extra measure of security for an organization’s internal network. Usually, hosts from inside the protected networks, which have private addresses, are able to communicate with the outside world, but systems that are located outside the protected network have to go through the NAT boxes to reach internal networks. Moreover, NAT enables an organization to use fewer IP addresses, which helps confusing attackers about which particular host they are targeting.

Don’t Disable Personal Firewalls

Personal firewalls are software-based firewalls installed on each computer in the network. They work in much the same way as larger border firewalls — they filter out certain packets to prevent them from leaving or reaching your system. The need for personal firewalls is often questioned, especially in corporate networks, which have large dedicated firewalls that keep potentially harmful traffic from reaching internal computers. However, that firewall can’t do anything to prevent internal attacks, which are quite common and often very different from the ones from the internet; attacks that originate within a private network are usually carried out by viruses. So, instead of disabling personal firewalls, simply configure a standard personal firewall according to your organization’s needs and export those settings to the other personal firewalls.

Use Centralized Logging and Immediate Log Analysis

Record suspicious logins and other computer events and look for anomalies. This best practice will help you reconstruct what happened during an attack so you can take steps to improve your threat detection process and quickly block attacks in the future. However, remember that attackers are clever and will try to avoid detection and logging. They will attack a sacrificial computer, perform different actions and monitor what happens in order to learn how your systems work and what thresholds they need to stay below to avoid triggering alerts.

Use Web Domain Whitelisting for All Domains

Limiting users to browsing only the websites you've explicitly approved helps in two ways. First, it limits your attack surface. If users cannot go to untrusted websites, they are less vulnerable. It's a solid solution for stopping initial access via the web. Second, whitelisting limits hackers' options for communication after they compromise a system. The hacker must use a different protocol, compromise an upstream router, or directly attack the whitelisting mechanism to communicate. Web domain whitelisting can be implemented using a web filter that can make web access policies and perform web site monitoring.

Route Direct Internet Access from Workstations through a Proxy Server

All outbound web access should be routed through an authenticating server where access can be controlled and monitored. Using a web proxy helps ensure that an actual person, not an unknown program, is driving the outbound connection. There can be up-front work required to reconfigure the network into this architecture, but once done, it requires few resources to maintain. It has practically no impact on the user base and therefore is unlikely to generate any pushback. It raises the level of operational security since there is a single point device that can be easily monitored.

Use Honeypots and Honeynets

A honeypot is a separate system that appears to be an attractive target but is in reality a trap for attackers (internal or external). For example, you might set up a server that appears to be a financial database but actually has only fake records. Using a honeypot accomplishes two important goals. First, attackers who believe they have found what they are looking for will leave your other systems alone, at least for a while. Second, since honeypots are not real systems, no legitimate users ever access it and therefore you can turn on extremely detailed monitoring and logging there. When an attacker does access it, you'll be gathering an impressive amount of evidence to aid in your investigation.

A honeynet is the next logical extension of a honeypot — it is a fake network segment that appears to be a very enticing target. Some organizations set up fake wireless access points for just this purpose.

Protect Your Network From Insider Threats

To deal with insider threats, you need both prevention and detection strategies. The most important preventive measure is to establish and enforce the least-privilege principle for access management and access control. Giving users the least amount of access they need to do their jobs enhances data security, because it limits what they can accidentally or deliberately access and ensures that is their password is compromised, the hacker doesn't have all keys to the kingdom. Other preventative measures include system hardening, anti-sniffing networks and strong authentication. Detection strategies include monitoring users and networks and using both network- and host-based intrusion detection systems, which are typically based on signatures, anomalies, behavior or heuristics.

End users also need to be trained in how to deal with the security threats they face, such as phishing emails and attachments. The best security in the world can be undermined by end users who fail to follow security policies. However, they cannot really be expected to follow those policies without adequate training.

Monitor and Baseline Network Protocols

You should monitor the use of different protocol types on your network to establish baselines both the organization level and a user level. Protocol baselining includes both wired and wireless networks. Data for the baseline should be obtained from routers, switches, firewalls, wireless APs, sniffers and dedicated collectors. Protocol deviations could indicate tunneling information or the use of unauthorized software to transmit data to unknown destinations.

Use VPNs

A virtual private network (VPN) is a secure private network connection across a public network. For example, VPNs can be used to connect LANs together across the internet. With a VPN, the remote end appears to be connected to the network as if it were connected locally. A VPN requires either special hardware or VPN software to be installed on servers and workstations. VPNs typically use a tunneling protocol, such as Layer 2 Tunneling Protocol, IPSec or Point-to-Point Tunneling Protocol (PPTP). To improve security, VPNs usually encrypt data, which can make them slower than normal network environments.

Use Multiple Vendors

In addition to diversity of controls, you should strive for diversity of vendors. For example, to defend against malware, you should have antimalware software on each of your computers, as well as on the network and at the firewall — and use software from different vendors for each of these places. Because each vendor uses the same malware detection algorithms in all its products, if your workstation, network and firewall antimalware solutions all come from vendor A, then anything missed by one product will be missed by all three. The best approach is to use vendor A for the firewall antimalware, vendor B for the network solution, and vendor C to protect individual computers. The probability of all three products, created by different vendors and using different detection algorithms, missing a specific piece of malware is far lower than any one of them alone missing it.

Use Your Intrusion Detection System Properly

An IDS can be an important and valuable part of your network security strategy. To get the most value from your IDS, take advantage of both ways it can detect potentially malicious activities:

- ✓ **Anomaly detection** — Most systems maintain a certain baseline of activity on their networks and sensitive hosts. An IDS can record that baseline and scan for abnormal activity. If something unusual happens, such as a spike in activity that could indicate a ransomware or SQL injection attack, it sends an alert so the administrator can analyze the event and take action as soon as possible.
- ✓ **Misuse detection** — The IDS will also compare activities with attack signatures, which are sets of characteristic features common to a specific attack or pattern of attacks. This helps them spot attacks even if they don't generate activity that violates your organization's baseline.

Automate Response to Attacks when Appropriate

Many network devices and software solutions can be configured to automatically take action when an alarm is triggered, which dramatically reduces response time. Here are the actions you can often configure:

- ✓ **Block IP address** — The IDS or firewall can block the IP address from which the attack originated. This option is very effective against spam and denial-of-service attacks. However, some attackers spoof the source IP address during attacks, so the wrong address will be blocked.
- ✓ **Terminate connections** — Routers and firewalls can be configured to disrupt the connections that an intruder maintains with the compromised system by targeting RESET TCP packets at the attacker.
- ✓ **Acquire additional information** — Another option is to collect information on intruders by observing them over a period of time. By analyzing the information you gather, you can find patterns and make your defense against the attack more robust. In particular, you can:
  - **Look for the point of initial access,** how the intruders spread and what data was compromised. Reverse-engineer every piece of malicious software you find and learn how it works. Then clean up the affected systems and close the vulnerability that allowed initial access.
  - **Determine how malicious software was deployed.** Were administrative accounts used? Were they used after hours or in another anomalous manner? Then determine what awareness systems you could put in place to detect similar incidents in the figure.

Physically Secure Your Network Equipment

Physical controls should be established and security personnel should ensure that equipment and data do not leave the building. Moreover, direct access to network equipment should be prohibited for unauthorized personnel.

Improve the Security of Your Network

with Netwrix Auditor for Network Devices

- Get complete visibility into configuration changes and logon attempts to your network devices
- Monitor remote access to both your network and your network devices
- Be notified about scanning threats to your network
- Stay on top of hardware issues in your network devices
- Automate compliance reporting to internal and external auditors

Download Free 20-Day Trial

About Netwrix

Netwrix Corporation is a software company focused exclusively on providing IT security and operations teams with pervasive visibility into user behavior, system configurations and data sensitivity across hybrid IT infrastructures to protect data regardless of its location. Over 10,000 organizations worldwide rely on Netwrix to detect and proactively mitigate data security threats, pass compliance audits with less effort and expense, and increase the productivity of their IT teams.

Founded in 2006, Netwrix has earned more than 140 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information about Netwrix, visit www.netwrix.com.