



Guide to Network Security

These days, computer security is a serious and complex business. True security requires the coordination of staff and technology across the enterprise infrastructure, as well as educated and cooperative users. But even the best of information security policies and plans will fail if the underlying network is not secure. You may think you are doing all you can to protect your network, but think again. Security dangers you're not even aware can be lurking in every corner of your network. This package provides you with an overview of network security, including firewalls, intrusion detection, and virtual private networks, and offers practical guidelines you can put into place today to protect your company's infrastructure and critical data in the future.

Sponsored By:



Learning Guide

Table of Contents

[Section 1: Network Security Checklist](#)

[Section 2: The Network Administrator's Guide to Forensic First Response](#)

[Section 3: Five Common Insider Threats and How to Mitigate Them](#)

[Section 4: Perimeter Security Explored: Firewalls](#)

[Section 5: How to Choose a Firewall](#)

[Section 6: Hardening Your Router in 9 Easy Steps](#)

[Section 7: Selecting Intrusion Detection Devices](#)

[Section 8: Understanding the Differences Between IDS and IPS](#)

[Section 9: Beyond Wireless Intrusion Detection](#)

[Section 10: Virtual Private Network Trends](#)

[Section 11: Five Steps to Controlling Network Access](#)

[Section 12: Study: Network Security Market to Reach \\$6 Billion](#)

[Section 13: NAC Market Ready to Explode](#)

[Resources From ProCurve Networking by HP](#)

[About ProCurve Networking by HP](#)

Section 1: Network Security Checklist

by Chris Cox, November 23, 2005

Centuries ago, security professionals may have debated the merits of new technologies, like moats or drawbridges for example. Today, the equipment may have changed, but the debate remains the same.

Today, your network has become the castle; and instead of invading armies, the security professional is constantly besieged by organized crime looking for confidential data, twelve-year-olds with downloaded cracker suites and thirty-year-old entrepreneurs looking to host a new warez site. While 100% security is hardly a possibility, there are several things that you can do to make your network more secure.

1. Ensure That Your Firewalls are Up-to-Date and Properly Configured.

Yes, that is firewalls, as in more than one. The most secure configuration will include, at a minimum, two firewalls between any network client and the wild, wild Web. This includes a software firewall on the system, as well as a hardware firewall in the network path.

Although it is an excellent tool, most hardware firewalls have one fatal flaw: they are designed to trust all outgoing traffic. Unfortunately, this traffic may include captured keystrokes or other unwanted data. A software firewall, properly configured, is able to distinguish unsafe traffic from benign.

Your firewall manual will go into greater detail, but as a general rule of thumb, you should start by manually allowing all inbound and outbound traffic, and setting policies to allow only the desired packets.

2. Ensure that Virus Protection is Up-to-Date.

A virus will never be detected by your firewall, although some symptoms such as replication attempts may be flagged by your software firewall. A virus might be limited in scope and destroy data on one system (or server!), or might infect software firewalls and spread through the network. Once the software firewall is infected, the system is open to greater security risks.

Establishing and enforcing a policy of updates and regular virus scans now can save a weekend spent restoring a server and workstations later!

3. Maintain a Security Point of Contact (POC)

Having a dedicated point of contact for all security issues, whether an assigned member of the IT department or an entire CIRT team, will ensure that security efforts and responses are coordinated, trends and patterns can be identified, and other groups or departments can be warned before the incident affects them. Similarly, the POC can coordinate assistance if the organization does not have the resources to deal with the threat.

4. Is Your Data Passing Through an Unsecured Medium?

Each node that your data passes thorough must be considered a potential security risk. Physical security is paramount when the network path runs through wiring closets, hubs, etc. For that matter, are you sure that you can trust your ISP?

If you cannot guarantee the security of your datapath, you can encrypt your network traffic. Programs such as [Pretty Good Privacy](#) allow seamless encryption of network traffic, as well as e-mail and messaging protection.

5. Baseline Your Network.

The network administrator has the "home field advantage" over a potential attacker. As the network administrator, you should know what 'usual' network traffic is, and what could be an indication of an attack. Using a packet sniffer, such as [Ethereal](#), under normal network loads should give you a good indication of expected network activity.

6. Ensure that OS and Applications are Properly Patched.

A drawbridge will do you no good if you leave the key to the backdoor under that mat. Similarly, a firewall will do you no good if your OS opens a back door into your system. A recent example was the discovery that unpatched versions of Windows and MSN messenger can allow an attacker complete control over the system!

It is vital that each system OS is regularly patched, and at the very minimum, each program that accesses the Internet should be patched and upgraded in addition to being monitored by the firewall.

7. Utilize and Configure an IDS.

An intrusion detection system is a crucial piece of your network security toolkit. An IDS can be as simple as a laptop running [Snort](#) or a highly priced, dedicated Cisco device. This will allow you to identify trends and patterns, and respond to attacks while they are still in the reconnaissance phase.

An IDS is nothing without skilled analysis of the results, however. The analyst will validate positive matches from the IDS, and if an attack is suspected, must validate it with the system logs, if possible. Ensure that that all clocks on the network are synced. This allows you to identify reconnaissance activity preceding an attack, or to quickly determine the characteristics of an attack in progress. It's much easier to identify the scope of the attack if all the systems show that it happened at 11:03:28, rather than 11:01:15, 12:03:30 and 12:00:00!

8. Secure the Wireless Network

Approximately 80% of wireless networks are unsecured networks, and this could prove to be the Achilles heel of an otherwise secure network.

First, make sure that all access points (APs) are password protected. And it goes without saying that the default password doesn't count! This will prevent most users from accessing the AP through their browser and altering the security settings. Also, use 128 bit WEP to protect data while airborne. Most APs allow you to hide the SSID (check your product documentation for details), which makes it more difficult for unauthorized users to detect your wireless network.

Lastly, if your router offers it, filter traffic by MAC address, or at the very least, IP address. This ensures that only authorized users have access to the network. Again, it is important to consider backdoors. Make sure that all users are aware of network security policies, which should ban unauthorized APs on the network. Most users will not configure their AP security policies in accordance with your own.

9. Consider your Most Dynamic Security Threat: Human Nature.

At one time, it was said that the only way to truly secure a system was to unplug it and leave it off. Unfortunately, this is no longer true, in addition to being completely impractical!

Users are capable of unintentionally jeopardize the security of the network by failing to properly secure their own systems. A user may choose a weak password that is easy to remember, or the administrator may assign a strong password that the user ends up writing down and "hiding" under the keyboard.

You can enforce strong password policies by using the snap-in console "gpedit.msc." The selection "Computer Configuration," "Windows Settings," "Account Policies" and "Password Policies" will allow you to define policies for users.

Ensure that your users are briefed on the very real threat of social engineering. As an example: A user receives a call from tech support asking for help testing the new server. Tech support asks the user to change their password to "test," to log on to the server briefly, "for testing purposes." The user does so and is able to connect with no problems. Before hanging up, tech support reminds the user to change their password back to a private, secure selection, and stresses the importance of not saying the password out loud, even to the technician.

The entire transaction takes less than five minutes, but in that time a hacker has received unrestricted access to your network. No firewall could prevent it; no IDS can detect it.

In *The art of deception*, Kevin Mitnick describes several techniques that social engineers will use to exploit the trust of privileged users, and his guidelines should be part of any new employee training program. Remember, a hacker will never call up and ask for the big picture, but a piece of the puzzle. There may never be a way to plug every security hole, or to anticipate the new ones. However, a properly configured network, with an established security policy, can be the next best thing.

Chris Cox is a network administrator for the United States Army, based in Fort Irwin, California.

Section 2: The Network Administrator's Guide to Forensic First Response

Chris Cox, September 27, 2005

Very few companies employ a designated, trained forensic examiner to handle incidents such as unauthorized resource usage or suspected computer crimes. Rather, the majority of companies outsource such tasks to a specialist, such as [DIBS](#) or [CFS](#).

The time between discovery of an incident and the handover of digital evidence is critical for the possibility of successful evidence retrieval. Mishandled evidence, whether to be used in court or solely in house, can damage the integrity of the investigation. For instance, viewing pornographic images that were downloaded to an employee's computer will change the time/date stamp. If this occurs, there is no way to prove that it was the employee that downloaded the images and not the network administrator.

The most critical concern, then, is to create the most conducive environment possible for the forensic examiner. The following points will discuss vital considerations for the administrator acting in a first responder's role to maintain the integrity of evidence and accountability.

Avoid FUD

Fear, uncertainty and doubt will surely be some of your first reactions, especially in the instance of a network break-in. It is important to remember that you are not the first one that this has happened to and not to act rashly. For instance, if you notice that a system has been hacked into, it may be your first reaction to panic and pull the network cable. Although this can stop the attack, it may trigger a retaliatory routine planted by the hacker and cause further damage. By taking time to investigate and consult with a specialist, you may save the system from irreparable damage.

Secure the Suspected Devices

It is important to control access to the device or devices that are suspected as being evidence or as being compromised. Normally, this is achieved by keeping the items under observation until qualified relief arrives, but this can also be done over longer periods of time by keeping the devices under lock and key. It is essential to remember to control all secondary storage items as well. This includes floppy drives, CDs and flash media. It is worth noting that recently iPods and similar devices have been used for discreet data storage and should certainly be treated as suspect.

Consider Legal Aspects

One of the most important considerations is to protect yourself and your company from legal recourse. The fourth and fifth amendments may apply in your case, as discussed in the [Department of Justice report on computer seizures](#). Also, laws will vary from state to state, so it is important to check with your legal department or legal representation before pursuing a suspected offense.

Much of this can be avoided through policy letters and system banners which will clearly state the company's policy on data collection and interception, as well as defining acceptable use. Be warned, however, that even with policy letters and a statement of understanding, you do not generally have permission to randomly or constantly monitor electronic communications. Any monitoring that is done should be documented and justified in writing.

Write Down all Known Information About the System

When your network is under attack, it's difficult to know when not to act. While waiting for further guidance, it will help the investigator a great deal if the relevant information is collected and prepared as soon as possible. Your notes should include the IP address, the system time in relation to "wall time" (in other words, the system time, noting any offset with actual clock time), the computer name, running services or applications, plus any relevant information about the crime. This should include how the problem was discovered, by whom and when. It is also worth noting the primary use of the system, as a mail server would definitely be handled differently than a workstation!

Record All Actions Taken Upon Discovery

This is the point where the chain of custody begins. Any actions that you take could be called into question as to how they may have affected the validity of the recovered evidence.

Your actions should be recorded to include date/time, witnesses, etc., beginning with when you became aware of the incident and should document any time that the system or evidence was moved or changed hands. It is critical to note any time that the system was left alone, although this should not happen at any time.

Do Not be Tempted to Start the Investigation Yourself

If nothing else, this is vital. You may be tempted to start viewing files or Web histories, but don't do it. While you may be able to find the information that you were looking for, any evidence collected is no longer admissible into court, should that be required. Furthermore, it may be easily contested if used for grounds for employment termination.

Do Not Change The State of the System

If the system is off, leave it off. Likewise, if the system is on, leave it on. Changing the state of the system could destroy valuable potential evidence. For instance, some operating systems will clear the swap file upon restart, and shutting down the system will close all programs that are currently running. Also, systems may be "booby trapped" with startup routines designed to destroy or alter data.

Disable Virus Protection

Although a vital tool for network security, virus protection can be a nightmare for the forensic examiner. While performing a scan, the virus protection program will, in effect, access each file. This can not only alter the time/date stamp of critical suspected files, but certain tools such as Norton Antivirus will automatically detect and remove "hack tools" by default, which may be crucial to the investigation. It is imperative to stop all intrusive services such as virus scanners as soon as possible.

Consider Isolation

If there is an attack in progress, it is important to weigh the value of potential "live" evidence against the risk of an escalation. This should be discussed with the forensic examiner or incident response team as soon as possible to determine the best course of action.

Isolating a system from the network is typically only done in cases of intrusion attempts or virus activity, but it should be noted that network activity could write over data in certain cases.

The role of the first responder can be likened to the role of a paramedic. Your first job is to avoid causing further harm, while at the same time coordinating further professional support. By keeping a level head and clear policies, no incident will be a disaster.

Chris Cox is a network administrator for the United States Army, based in Fort Irwin, California.

Section 3: Five Common Insider Threats and How to Mitigate Them

Kevin Beaver, January 23, 2006

Despite the continuous growth of malware and other threats, insiders still pose a significant threat to enterprises. According to Gartner, more than 70% of unauthorized access to data is committed by an organization's own employees. But don't fret. There are steps you can take to protect against common insider threats without breaking the bank.

Let's look at five insider threats that pose a danger to sensitive information along with tactics for mitigating them.

1. Exploiting Information Via Remote Access Software

A considerable amount of insider abuse is performed offsite via remote access software such as Terminal Services, Citrix and GoToMyPC. Simply put, users are less likely to be caught stealing sensitive information when they can it do offsite. Also, inadequately protected remote computers may turn up in the hands of a third-party if the computer is left unattended, lost or stolen.

What you can do about it:

Solid share and file permissions are critical, as is OS and application logging. With many remote access solutions, you can also enable tighter security controls on certain features and system access, monitor employee usage in real time, generate usage logs and more. Look deeply into the configuration of your system and determine which features and audit trails can provide better management, reporting and security. Also, it's common for abuse to take place during non-business hours, so consider limiting the times that users can remotely access systems.

Strong passphrase requirements can thwart guessed logins, and screen saver timeouts on remote computers can keep unauthorized users locked out. Encrypting system hard drives helps protect systems that are lost or stolen.

2. Sending Out Information Via E-mail and Instant Messaging

Sensitive information can simply be included in or attached to an e-mail or IM. Although this is a serious threat, it's also one of the easiest to eliminate.

What you can do about it:

An effective way to catch sensitive information leaving the network is to set up a network analyzer and filter keywords, specific attachments, etc.

You can also utilize client or server-based content filtering to catch and block sensitive information going out. However, perimeter-based or outsourced messaging security solutions offer content filtering and blocking that is much easier to manage.

Keep in mind that none of these work well if message traffic is encrypted. But filtering will at least highlight the fact that such communication is taking place. Speaking of which, perhaps now's a good time to review your firewall rules to determine not only what's allowed in but also what's allowed out of the network.

3. Sharing Sensitive Files on P2P Networks

Whether or not you allow peer-to-peer file sharing software such as Kazaa or IM on your network, odds are it's there and waiting to be abused. The inanimate software in and of itself is not the problem – it's how it's used that causes trouble. All it takes is a simple misconfiguration to serve up your network's local and network drives to the world.

What you can do about it:

If your organization allows P2P software, it behooves you to ensure that users are aware of the dangers. There are even certain perimeter-based P2P content monitoring solutions that can help keep sensitive data safe.

If you don't want P2P software on your network, you can try blocking it at the firewall; however, the software is smart enough to find open ports to go out. This is another good use for a network analyzer and even more justification for performing a firewall rule audit.

The ideal solution is to prevent P2P file sharing traffic from ever entering or leaving the network. The only effective methods I've found for this is to use a P2P firewall at the perimeter or personal firewall software with application protection.

4. Careless Use of Wireless Networks

Perhaps the most unintentional insider threat is that of insecure wireless network usage. Whether it's at a coffee shop, airport or hotel, unsecured airwaves can easily put sensitive information in jeopardy. All it takes is a peek into e-mail communications or file transfers for valuable data to be stolen. Wi-Fi networks are most susceptible to these attacks, but don't overlook Bluetooth on smartphones and PDAs. Also, if you have WLANs inside your organization, employees could use it to exploit the network after hours.

What you can do about it:

You cannot control the airwaves outside of your office, but you can enable secure wireless hotspot usage for your Wi-Fi users. This entails using a VPN for remote network connectivity, a personal firewall to keep users from connecting to the wireless computer and SSL/TLS for all messaging (i.e., Webmail via HTTPS, POP3s, IMAPs and SMTPs).

Ensure your internal wireless networks are secure. Use proper encryption and authentication (preferably WPA or WPA2) and enable logging. Also, try to use directional antennae and drop down the power levels on your access points to keep wireless signals inside your building. Disabling Bluetooth if it's not needed or at least making your devices non-discoverable can also cut down on wireless attacks.

5. Posting Information to Discussion Boards and Blogs

Quite often users post support requests, blogs or other work-related messages on the Internet. Whether intentional or not, this can include sensitive information and file attachments that put your organization at risk.

What you can do about it:

Filtering content in HTTP and e-mail communications at the network perimeter is the best way to check for and block sensitive information from going out to such sites. However, there's always a chance that information may leak out via encrypted transmissions or from users' personal machines. In either case, it pays to stay abreast of new

information about your organization on the Web. A good way to do this is to subscribe to Google Alerts so you can be alerted anytime certain keywords show up on the Internet. General Google Web and Groups queries can often uncover material as well. However, this only works for information made available to Google's bots, which may exclude a large number of discussion boards.

If you implement these technical safeguards alone, they'll work (albeit in a vacuum) for the short-term. However, for long-term business value, you've got to ensure they're mated to business policies outlining "this is how we do it here." This, combined with user awareness and security metrics for determining if your countermeasures are working appropriately, can provide excellent protection against insider threats. Who knows, maybe this can even provide some justification for a high-end network-based content monitoring solution down the road.

Kevin Beaver is an independent information security consultant, author and speaker with Atlanta-based Principle Logic, LLC.

Section 4: Perimeter Security Explored: Firewalls

Mark Edmead, March 13, 2004

It's dangerous to dismiss the fact that there is authorized and unauthorized traffic that travels on your network. We've read stories of malicious attacks from hackers and other tales of harmful traffic being passed through your networks from your own employees. How do you limit or control that traffic to make your networks more secure? Firewalls are the first line of defense in your network architecture.

What exactly is a firewall? Many people might think that a firewall is a single device on your network, configured to protect your internal network from the external world. In the real world, a firewall is a system (or a group of systems) that enforces an access control policy between two networks.

The main purpose of a firewall is to disallow unauthorized and/or malicious traffic from traveling on your network. That could be in the form of traffic traveling from the outside to the internal network or traffic originating from the internal network and being sent to the outside world. For a firewall to work it needs to be part of the security architecture, and most important, firewalls can't protect you from attacks that don't go through it. That is, even if you have the most securely configured firewall in the world, if there's another entry point to your network not protected by a firewall, then your network isn't secured.

There are various types of firewalls, including the following:

- **Packet filtering firewalls.** This type of firewall examines the source and destination address of the data packet and either allows or denies the packet from traveling the network.
- **Application layer firewalls.** Also known proxy firewalls they are typically firewalls that run on a host computer.
- **Stateful inspection firewalls.** These firewalls capture and inspect the network packet. They examine the state and the context of the packets.
- **Dynamic packet filtering firewalls.** These firewalls can remember the network packets and can dynamically decide whether to enable packets to pass through the firewall.
- **Kernel proxy firewalls.** These firewalls provide a modular multilayer session, typically running in the operating system's lower-level kernel code.

Regardless of which firewall configuration you use there are some basic security strategies that are prudent to observe, such as the following:

1. Explicitly deny all traffic except for what you want. The default policy should be that if the firewall doesn't know what to do with the packet, deny it.
2. Don't rely only on your firewall for protection. While the firewall is there to protect your network, remember that it's only a device, and devices do fail. Make sure you implement what's called "defense in depth." That means that you should have multiple layers of network protection.

3. Make sure all of the network traffic passes through the firewall. If there's another way in to the network (like a modem pool or a maintenance network connection), then this connection could be used to enter the network completely bypassing the firewall protection.
4. If the firewall becomes disabled, then disable all communication. In the event the firewall fails, it's a good security practice to make sure that it fails in such a way that it denies access to incoming or outgoing traffic.

Firewalls should be the first line of defense in your perimeter network architecture. Properly configured a firewall prevents "most" network attacks, but it can't protect the network from network attacks that bypass the firewall or from traitors inside your network.

Mark Edmead CISSP, SSCP, TICSIA, is president of [MTE Software, Inc.](http://www.mtesoft.com) (www.mtesoft.com) and has more than 22 years' experience in software development, product development and network systems security.

Section 5: How to Choose a Firewall

Mike Chapple, August 17, 2005

There are dozens of firewalls on the market today. Choosing one for your organization can be a daunting task – especially in an industry filled with buzzwords and proprietary trademarks. Let's take a look at the basics of firewall technology and five questions you should ask when choosing a firewall for your organization.

- 1. Why are you implementing a firewall?** Sure, this sounds like a simple question. You're probably thinking to yourself, "Because we need one!" But it's important that you take the time to define the technical objectives that you have for implementing a firewall. These objectives will drive the selection process. You don't want to choose an expensive, feature-rich firewall that's complicated to administer when your technical requirements could be met by a simpler product.
- 2. How will the firewall fit into your network topology?** Will this firewall sit at the perimeter of your corporate network and be directly connected to the Internet, or will it serve to segment a sensitive LAN from the remainder of the organization? How much traffic will it process? How many interfaces will it need to segment your traffic? Performance requirements such as these contribute a significant amount to the total cost of new firewall implementations, making it easy to under- or over-purchase.
- 3. What type of traffic inspection do you need to perform?** This is where the buzzwords start to come into play. Every vendor out there has a different trademark for their traffic-inspection technology, but there are essentially three different options (listed in order of increasing complexity and cost):
 - *Packet-filtering* firewalls use simple rules to evaluate each packet they encounter on its own merits. They maintain no history from packet to packet, and they perform basic packet header inspection. The simplicity of this inspection makes them speed demons. They're the most inexpensive option, but they are also the least flexible and vulnerable. There's a good chance you already own equipment capable of performing packet filtering – your routers!
 - *Stateful-inspection* firewalls go a step further. They track the three-way TCP handshake to ensure that packets claiming to belong to an established session (i.e., the SYN flag is not set) correspond to previous activity seen by the firewall. Requests to open the initial connection are subject to the stateful-inspection firewall rulebase.
 - *Application-proxy* firewalls contain the highest level of intelligence. In addition to stateful inspection, they broker the connection between client and server. The client connects to the firewall, which analyzes the request (including application-layer inspection of packet contents). If the firewall rules indicate that the communication should be allowed, the firewall then establishes a connection with the server and continues to act as an intermediary in the communication. When combined with Network Address Translation, both hosts may not even be aware that the other exists – they both believe they are communicating directly with the firewall.

4. **Is your organization better suited for an appliance or a software solution?** Appliances are typically much easier to install. You normally just plug in the appropriate Ethernet cables, perform basic network configuration and you're ready to configure your firewall rules. Software firewalls, on the other hand, can be tricky to install and require tweaking. They also lack the security that's often built into the hardened operating systems of firewall appliances. What's the tradeoff? You guessed it! Appliances are more expensive.

5. **What operating system is best suited for your requirements?** Even appliances run an OS and, chances are, you'll need to work with it at some point in your firewall administration career. If you're a Linux jockey, you probably don't want to choose a Windows-based firewall. On the other hand, if you don't know `/dev/null` from `/var/log`, you probably want to steer clear of Unix-based solutions.

While I can't recommend a specific firewall to you without knowing your needs, the process of answering these questions can help you solidify your thoughts and put you in the right direction. With these answers in hand, you should be able to intelligently evaluate the cost/benefit tradeoff for the various products available on the market today.

Mike Chapple, CISSP is an IT security professional with the University of Notre Dame who previously served as an information security researcher with the National Security Agency and the U.S. Air Force.

This tip originally appeared on SearchSecurity.com.

Section 6: Hardening Your Router in 9 Easy Steps

Chris Cox, August 11, 2005

For most enterprise LANs, the router has become one of the most critical security appliances in use. Generally, most networks have one primary access point, which is referred to as a "border router," that is often paired with a dedicated firewall.

Configured properly, it can keep all but the most determined bad guys out, and if you want, it can even keep the good guys in. But an improperly configured router is only marginally better than having no security in place at all.

In the following tip, we'll explore nine easy steps that you can take to ensure that you have a brick wall protecting your network and not an open door.

1. Change the Default Password!

According to CERT/CC at Carnegie Mellon University, 80% of security incidents are caused by weak passwords. Extensive lists of default passwords are available online for most routers, and you can be sure that *someone*, somewhere knows your birthday. SecurityStats.com maintains a thorough [do/don't list for passwords](#), as well as a password strength test.

2. Disable IP Directed Broadcasts

Your router is obedient. It will do what it's told, no matter who's doing the telling. A Smurf attack is a version of a Denial of Service (DOS) attack in which an attacker sends an ICMP echo request to your network's broadcast address using a spoofed source address. This causes all the hosts to respond to the broadcast request, which will slow down your network, at the very least.

Consult your router's documentation for information on how to disable IP directed broadcasts. For instance, the command "Central(config)#no ip source-route" will disable IP directed broadcasts on Cisco routers.

3. Disable HTTP Configuration for the Router, if Possible

As outlined in a Cisco Tech Note, "The authentication protocol used for HTTP is equivalent to sending a cleartext password across the network, and, unfortunately, there is no effective provision in HTTP for challenge-based or one-time passwords."

Although it may be convenient to configure your router from a remote location (from home for example), the fact that you can do it means that anyone else can as well. *Especially* if you're still using the default password! If you must remotely manage the router, make sure that you are using SNMPv3 or greater, as it supports hashed passwords.

4. Block ICMP Ping Requests

The primary purpose of a ping request is to identify hosts that are currently active. As such, it is often used as part of reconnaissance activity preceding a larger, more coordinated attack. By removing a remote user's ability to receive a response from a ping request, you are more likely to be passed over by unattended scans or from "script kiddies," who generally will look for an easier target.

Note that this does not actually protect you from an attack, but will make you far less likely to become a target.

5. Disable IP Source Routing

The IP protocol allows a host to specify the packet's route through your network, instead of allowing the network components to determine the best path. The only legitimate use that you may come across for this feature is to troubleshoot connections, but this is rare. It's far more common to be used to map your network for reconnaissance purposes, or when an attacker is attempting to locate a backdoor into your private network. Unless specifically needed for troubleshooting, this feature should be disabled.

6. Determine Your Packet Filtering Needs

There are two philosophies to blocking ports, and which one is appropriate for your network depends on the level of security that you require.

For a high-security network, especially when storing or maintaining confidential data, it is normally recommended to "filter by permission." This is the scheme in which all ports and IP address permissions are blocked, except for what is explicitly required for network functions. For instance, port 80 for web traffic and 110/25 for SMTP can be allowed to come from a dedicated address, while all other ports and addresses can be disabled.

Most networks will enjoy an acceptable level of security by using a "filter by rejection" scheme. When using this filtering policy, ports that are not used by your network and are commonly used for Trojan Horses or reconnaissance can be blocked to increase the security of your network. For instance, blocking ports 139 and 445 (TCP and UDP) will make your network more difficult to enumerate, and blocking port 31337 (TCP and UDP) will make you more secure from Back Orifice.

This should be determined during the network planning phase, when the level of security required is compared to the needs of the network users. Check out this [extensive list of ports](#) with their normally associated uses.

7. Establish Ingress and Egress Address Filtering Policies.

Establish policies on your border router to filter security violations both outbound (egress) and inbound (ingress) based on IP address. Except for unique and unusual cases, all IP addresses that are attempting to access the Internet from inside of your network should bear an address that is assigned to your LAN. For instance, 192.168.0.1 may have a legitimate need to access the Internet through the router, but 216.239.55.99 is most likely to be spoofed, and part of an attack.

Inversely, traffic from the outside of the Internet should not claim a source address that is part of your internal network. For that reason, inbound addresses of 192.168.X.X, 172.16.X.X and 10.X.X.X should be blocked.

And lastly, all traffic with either a source or a destination address that is reserved or unroutable should not be permitted to pass through the router. This can include the loopback address of 127.0.0.1 or the class E address block of 240.0.0.0-254.255.255.255.

8. Maintain Physical Security of the Router

A router is much more secure than a hub, especially from network sniffing. This is because a router intelligently routes packets based on IP destination, where a hub broadcasts the data to all nodes. If one system that is connected to that hub places their network adapter in promiscuous mode, they are able to receive and view all broadcasts, including passwords, POP3 traffic and web traffic.

It is important then to make sure that physical access to your networking equipment is secure to prevent the placement of sniffing equipment, such as an unauthorized laptop, on the local subnet.

9. Take the Time to Review the Security Logs

Reviewing your router's logs (via its built-in firewall functions) is often the most effective way to identify security incidents, both in-progress attacks and indicators of upcoming attacks. Using outbound logs, you can also identify Trojans and spyware programs that are attempting to establish an outbound connection. Attentive security administrators were able to identify the Code Red and Nimda attacks before antivirus publishers were able to react.

Also, generally, the router is on the perimeter of your network, and allows you to get an overall picture of the inbound and outbound activity of your network.

Chris Cox is a network administrator for the United States Army, based in Fort Irwin, California.

Section 7: Selecting Intrusion Detection Devices

David Jacobs, February 7, 2006

Hackers are constantly at work developing new ways to attack your network, so guarding against these attacks requires eternal vigilance. Intrusion prevention devices are one essential element of defense.

Firewalls and antivirus software remain necessities, but dedicated intrusion prevention products must be added to your network. Firewalls can scan for viruses in incoming mail, but can't protect against viruses introduced when an infected laptop is connected to the network. While antivirus software has been enhanced with spyware protection, it is ineffective against "day zero" threats—that is, new threats for which no defense has been developed. Antivirus software is also ineffective against phishing attempts.

Intrusion prevention devices are available from a wide variety of vendors. Small vendors focus on the intrusion prevention market alone and offer dedicated intrusion protection appliances. The large network equipment vendors also offer dedicated appliances and, in addition, integrate intrusion protection into switches and firewalls.

How Intrusion Prevention Works

Intrusion prevention appliances use a combination of signature-based and behavior-based methods to detect and prevent attacks. A signature is a description of a particular attack technique. For example, phishing attempts have taken advantage of ways of encoding a URL in a mail message so that it appears to be a legitimate link. The signature provides a directive to the appliance on how to scan for this format.

New threat types are developed every day, so the appliance vendor must maintain a group of support engineers who monitor news of new threat types and quickly develop and distribute new signatures. The vendor must provide an efficient means of informing customers of new threats and updating customer appliances with new signatures with minimal delay.

Behavior-based methods protect against "day zero" threats. Behavior-based techniques monitor the network for behavior that is out of the ordinary. For example, a workstation that sends out a rapid stream of e-mail may have been infected and has come under the control of a spammer. A workstation that sends out TCP SYN packets but does not complete the TCP connection sequence may be infected and is taking part in a denial of service attack.

Detecting threats using either signatures or behavior-based methods requires the appliance to analyze entire packets, not just packet headers. Hackers sometimes fragment packets or send them out of order to evade less sophisticated tools. Appliances must defragment packets and resequence out-of-order packets in order to analyze the entire message.

Device Options

It isn't always possible to detect a threat by analyzing packets individually. Intrusion prevention appliances must monitor and track the state of all the connections passing through them. Analyzing entire packets, defragmenting and resequencing packets while keeping track of potentially thousands of connections without slowing down the

network or adding unacceptable levels of latency requires custom ASICs designed for these tasks. Software-based implementations cannot meet these requirements.

Appliances must be positioned along each major link in the network to inspect and block any packet. Switch vendors have developed intrusion prevention modules that fit into switches. These can be an excellent option if the module can match standalone appliances in performance and in the range of threats they can meet.

Intrusion prevention devices—either standalone appliances or switch modules—must be supported by management facilities that enable network staff to monitor the number and type of threats encountered without producing an overwhelming volume of reports. Management tools must offer ways to tune the units to avoid reporting and blocking connections based on false positives, network occurrences that are not threats but appear to be.

Finally, intrusion prevention devices are only part of the answer to network threats. The user community must be trained and constantly reminded how to avoid introducing attackers, and the network staff must stay up to date on the latest threats and how to counter them.

David B. Jacobs has more than twenty years of networking industry experience. He has managed leading-edge software development projects and consulted to Fortune 500 companies as well as software start-ups.

Section 8: Understanding the Differences Between IDS and IPS

Brien M. Posey, October 11, 2005

As we all know, the universal presence of the Internet has completely changed networking as we know it. Networks that were once completely isolated are now connected to the world. This universal connectivity allows companies to achieve things never before imaginable. At the same time though, there is a dark side. The Internet is a haven for cyber criminals who use the connectivity to launch an unprecedented number of attacks against companies.

When the Internet first started to gain popularity, companies started to realize that they needed to implement firewalls in an effort to prevent attacks against them. Firewalls work by blocking unused TCP and UDP ports. Although firewalls are effective at blocking some types of attacks, they have one major weakness: You simply can't close all of the ports. Some ports are necessary for things like HTTP, SMTP and POP3 traffic. Ports corresponding to these common services must remain open in order for those services to function properly. The problem is that hackers have learned how to pass malicious traffic through ports that are commonly left open.

In response to this threat, some companies started to deploy intrusion detection systems (IDS). The idea behind an IDS is that it monitors all of the traffic that makes it through your firewall, and looks for any traffic that might be malicious. The idea sounds great in theory, but in reality, IDS systems really don't work that well for several reasons.

Early IDS systems worked by looking for any traffic that was out of the ordinary. When such traffic was detected, the activity was logged and an administrator was alerted. There are a few problems with this though. For starters, looking for abnormal traffic patterns produces a lot of false positives. After a while, the administrator becomes so annoyed with receiving constant false alerts that they start to ignore the alerts altogether.

The other major flaw in IDS systems is that they only monitor traffic. If an attack is detected, it's up to the administrator to take action. In a way this might be considered to be a good thing though. After all, since IDS systems produce a lot of false positives, would you really want them to take action against legitimate network traffic?

Over the last few years, IDS systems have evolved considerably. Today IDS systems work more like anti-virus programs. An IDS system contains a database of known attack signatures. The system constantly compares inbound traffic to the database and if an attack is detected then the IDS reports the attack.

These newer systems tend to be much more accurate than their predecessors, but the database must be constantly updated to remain effective. Furthermore, if an attack occurs and there is not a matching signature in the database, the attack may be ignored. Even if an attack is detected and confirmed to be a real attack, the IDS is powerless to do anything other than alert the administrator and log the attack.

This is where IPS systems come in. IPS stands for intrusion prevention system. An IPS is similar to an IDS, but it has been designed to address many of an IDS's shortcomings.

For starters, an IPS sits between your firewall and the rest of your network. That way, if an attack is detected, the IPS can stop the malicious traffic before it makes it to the rest of your network. In contrast, an IDS simply sits on top of your network rather than in front of it.

IPS systems also differ from IDS in the way that they detect attacks. There are a wide variety of IPS systems available and they don't all use the same techniques, but generally speaking, IPS systems tend to rely on packet inspections. The IPS will examine inbound packets and determine what those packets are really being used for before making a determination as to whether or not to allow those packets to make it onto your network.

As you can see, there are some important differences between IDS and IPS systems. If you are shopping for an effective security device, your network will usually be more secure if you use an IPS rather than an IDS.

Brien M. Posey, MCSE, is a Microsoft Most Valuable and has written for Microsoft, CNET, ZDNet, TechTarget, MSD2D, Relevant Technologies and other technology companies.

Section 9: Beyond Wireless Intrusion Detection

Lisa Phifer, December 16, 2004

Unauthorized devices pose a threat to every wireless LAN. In fact, "rogue" access points are so common that the need to defeat them has created a fertile market for wireless intrusion detection and prevention systems.

Like their wired counterparts, wireless intrusion detection systems (WIDS) are designed to monitor network traffic 24x7. Although product architectures vary, WIDS typically depend upon remote sensors, distributed throughout the monitored network. Sensors passively observe wireless activity, reporting back to a central IDS server. That server is responsible for analyzing reported activity, generating intrusion alarms and a history database. Results may be presented on the server itself, or remotely through some type of IDS client.

Today, there are many WIDS products and services, capable of detecting not only rogue devices, but dozens of common WLAN attack signatures, deviations from baselined behavior, and security policy violations. Some WIDS examples include AirDefense Enterprise, AirMagnet Enterprise, AirTight SpectraGuard, Bluesocket BlueSecure, Highwall Enterprise, Network Chemistry RFprotect, Newbury Networks WiFi Watchdog, Red-M Red-Detect, and VigilantMinds AirXone.

Early Detection

Any WLAN with multiple sites or over a dozen APs can probably benefit from deploying a WIDS. Distributed full-time monitoring is far more timely, complete, and cost-effective than ad hoc stumbling, traffic sampling, and human analysis. Without a WIDS, you're unlikely to spot a war driver briefly camped in your parking lot. You may discover a rogue AP planted in your facility, but probably after damage has been done. Risky mis-configuration of legitimate stations and APs may go unnoticed indefinitely.

Early WIDS products focused exclusively on detection, generating alerts that warn about potential security and performance problems. Considerable tuning of thresholds and policies can be required to eliminate *false positives*—intrusion alerts that reflect normal, innocuous behavior. But over-aggressive tuning can lead to *false negatives*, creating a false sense of security. Establishing proper balance is essential—a lesson that network administrators learned long ago in with wired network intrusion detection.

A well-tuned WIDS can provide a strong foundation for defense, but alerts alone do not stop attacks or remedy underlying vulnerabilities. When someone breaks into your home, a siren is invaluable—but not enough to safeguard you or your belongings. Similarly, WLAN owners need to look beyond intrusion detection alerts and WIDS vendors are moving quickly to fill that need.

An Ounce of (Wireless) Prevention

Recently, several WIDS products have added strike-back capabilities to temporarily or permanently inhibit a wireless attacker's ability to communicate with your WLAN or any adjacent wired network.

Temporary wireless blocking can discourage an attacker, just as an alarm siren can scare away a burglar. Persistent blocking can give you time to find and eliminate a rogue, without continuing to jeopardize your network during investigation.

For example, a rogue station spotted using wireless reconnaissance and attack tools may be seeking a way into your network via wireless. Some WIDS can aim 802.11 deauthenticate frames at that station's MAC address, preventing association with nearby APs. Alternatively, some WIDS can jam the channel occupied by a rogue AP to prevent it from being used as a backdoor into your network.

Selective deauthentication is less disruptive to bystanders than jamming, but an incited attacker can change his own address to elude MAC-based countermeasures. When using either method, one must consider the consequences—is that really a malicious AP, or your new neighbor's AP? You may want to start with manually-initiated termination, implementing policy-based termination after you've learned the ropes.

A Pound of Cure

Most WIDS offer configurable device lists to differentiate between authorized APs, neighbor APs, and all others. But such lists require on-going maintenance. In densely-populated urban areas, investigating every new device is at best labor-intensive, at worst impossible. Many WLAN owners prefer to be alerted only when an unknown device has actually penetrated their network, and then take wired-side steps to neutralize that threat.

A few WIDS products are now capable of inspecting IP payload to analyze traffic streams and behavior over time to determine whether a station or AP is communicating with an upstream network. As in the wired world, payload encryption can make this task more difficult. Ideally, this "true rogue" determination should be made as fast as possible to limit your network's exposure.

Some WIDS products have added wired-side countermeasures, through direct interaction with wired network switches, or by interfacing with wired-side network management systems. For example, AirMagnet Enterprise can use SNMP and CDP to query nearby Ethernet switch CAM tables, then disable the port used by a detected rogue. AirDefense Enterprise can interface with Cisco WLSE to initiate "port suppression," based on a detected rogue's MAC address.

Wired-side countermeasures like these are attractive because they can be focused and persistent. Watch for continued innovation here, as a complement to (not replacement for) wireless blocking. Interoperability with your organization's wired network hardware and management software may be a limiting factor.

Hide and Seek

Intrusion blocking—even persistent blocking—is a stop-loss tactic. Eventually, you'll need to find the intruder and eliminate the threat at its source. Here again, WIDS products are expanding to better support this task.

Several WIDS products now incorporate location detection to some degree. One method is to manually search around the sensor receiving the strongest signal from the transmitter. Another method is triangulation—comparing the signal received by three or more sensors to better pinpoint a transmitter's probable location. A third method is RF fingerprinting—modeling RF characteristics within a coverage area for comparison to received signal strength to predict the transmitter's location.

WIDS products also vary in how they present location information and what they do with that knowledge. For example, Newbury's Wi-Fi Watchdog uses device location as a criteria for WLAN access control—stations outside authorized regions are not permitted to pass 802.1X authentication.

What You Don't Know CAN Hurt You

Finally, automated prevention and location techniques aren't going to help much if you're blind to intrusions or missing the forest for the trees. Every WIDS must be able to accurately observe and intelligently analyze network activity.

Many WIDS products gather data from an overlay network of purpose-built sensors – passive listening devices. But proper sensor positioning is critical, so look for tools and tips to ensure adequate coverage. For example, AirTight SpectraGuard works in tandem with SpectraPlan to help plan for sensor placement.

Some vendors argue that APs, already installed throughout your WLAN, should double as sensors. For example, the Airespace Wireless Protection System leverages Airespace APs to monitor traffic to gather both security and performance information. Ask your AP vendor about their plans (if any) to provide WIDS capabilities or integrate with your WIDS server.

Compare any new WIDS release to the previous and you'll find a longer alert list. These products will forever be playing catch-up, adding detection signatures for new attack tools and methods. A strong signature database is important, but *more* is not always *better*. Look carefully at each product's expert analysis and event correlation. A system that can accurately roll a dozen symptoms into a single root cause intrusion alert will help you stop intrusions faster.

Lisa Phifer is vice president of Core Competence, Inc., a consulting firm specializing in network security and management technology.

Section 10: Virtual Private Network Trends

Robbie Harrell, January 5, 2006

Privacy and security are critical aspects of any enterprise network as we move into 2006. Today's security solutions consist of firewalls, virtual private network gateways, intrusion detection sensors (IDS) and proactive queries of operation systems in order to ensure that the client's virus and worm protections are up to date. Any and all of these technologies can be part of overall security architecture. Encryption of data as it traverses WLAN networks and the public Internet is driving a tremendous amount of development in the VPN gateway market.

Traditional encryption-based VPNs utilized IPsec as the technology of choice for building tunnels across the Internet and within the enterprise. However, Secure Sockets Layer (SSL) gateways are becoming more commonplace as the numbers of vendors, platforms and features/functionality expand.

With the advent of Web-based applications, the explosion of SSL to support Web-based security is not as surprising as it would seem. SSL has been around for quite some time, but is just now gaining traction in the marketplace (in the last two years).

The expansion of SSL has lead to VPN products offering multiple features and functionality to the enterprise. VPN gateways can now be categorized into four different categories based on the feature set supported by each. The four categories are as follows:

1. **SSL VPN Gateway:** SSL VPN, access control, access policy and client-audit capabilities
2. **Hybrid VPN Gateway:** SSL and IPsec and access policy
3. **Multi-function VPN Gateway:** SSL, IPsec and application and network-level security
4. **Multi-function Hybrid VPN Gateway:** Combination of 2 & 3

Each of these classes of VPN gateways offers different levels of capabilities and control. Based on your enterprise-specific needs, one of these should provide the level of security you require.

The key point is the development of the multi-function VPN gateway that provides the application level visibility. This combines both VPN capabilities and firewall-type capabilities within the same platform. This is extremely attractive in terms of consolidation of capabilities within a single box. However, this consolidation is not just a "nice-to-have" feature. It is extremely important to realize that an SSL VPN solution can render perimeter security via firewalls ineffective if the traffic is encrypted and cannot be screened by a firewall. This means that the trust boundary of the network has been pushed all the way to the VPN gateway. The advent of worms, viruses and malicious hackers requires firewalling your network. The introduction of granular-based access controls and application-layer visibility within the gateway makes SSL VPN gateways a reality for today's extremely critical security requirements.

The explosion of Web-based applications has created a requirement for SSL as a VPN technology to support secure data transfers across public or unprotected networks. The vendor community has responded by developing application-aware VPN gateways capable of supporting access control, security policies and network security within the VPN gateway itself. This supports secure access into the enterprise via a "gateway" technology that serves as a single threshold between protected assets and unwanted users or viruses.

Robbie Harrell (CCIE#3873) is the National Practice Lead for Advanced Infrastructure Solutions for SBC Communications.

Section 11: Five Steps to Controlling Network Access

Wes Noonan, November 16, 2004

One common security mistake is to treat the network and applications as separate entities that never interact. You may have separate people maintaining them, separate security policies, separate procedures and so on. Hardening Windows servers will go a long way toward protecting the integrity of the data on those servers, but you must also harden the network infrastructure itself. Start by taking the following five steps.

1. Implement Access Control Lists (ACLs)

If someone can get inside your network, they can gain access to your systems. You need to implement strict ACLs on your network equipment and grant access only to those users that require it. For example, do users in Houston ever need access to systems in New York? If not, chances are the traffic passing between those systems isn't essential to the business.

2. Implement Network-Based Access Control (NBAC)

Connecting systems to the network used to be a hassle: You had to build the network drivers, assign addresses and physically connect systems to get them to talk. Although this made it difficult for unauthorized systems to easily connect to the network, it created excessive administrative overhead. Then technologies like star-wired networks and Dynamic Host Configuration Protocol (DHCP) made it exceedingly simple to connect systems to the network. At first I rejoiced! But now I realize anyone can connect to the network. In fact, approximately 90% of the customers I visit have live network jacks that I can easily plug into to gain network access even if they have some written policy that states unauthorized connections are not permitted.

NBAC seeks to provide an enforcement mechanism to support those written policies. With NBAC, you want to define an authorized user and ensure connected systems are running the appropriate patches and software versions. If they aren't, they are placed in quarantine until the system is patched or updated.

3. Restrict Remote Connections

Implementing a VPN can be a risky endeavor. It permits network access for both users and viruses. Instead of allowing VPN access to your entire network, implement network ACLs that restrict remote users only to the servers and resources they need. For instance, using a VPN to connect Citrix or Terminal Server farms ensures that the only traffic allowed through the VPN is the Citrix traffic to the Citrix servers; if a remote client's system is infected, it will not infect your network.

4. Restrict and Secure Wireless Connections

If implemented behind your firewall, wireless LAN connections create a particularly large, gaping hole in your network perimeter. As a result, your wireless LAN connections should be treated like any other remote connection: Terminate them outside your firewall and require a VPN connection to gain access to internal and protected resources.

5. Implement IPsec

Implementing IPsec on your network is a great way to protect data in transit from being compromised. But it's no panacea. For example, if a machine is infected with Slammer, IPsec will only ensure the Slammer traffic is encrypted before it is transmitted. When used in conjunction with the other hardening methods, however, IPsec can serve as an effective method for protecting your internal traffic from prying eyes.

Due to network de-perimeterization, you can no longer rely exclusively on the network perimeter to protect systems and data. Removing the perimeter entirely is not the solution, nor is hardening the perimeter alone. You must also harden your Windows systems and network infrastructures to protect data in the event that the network perimeter fails or is circumvented.

Wesley J. Noonan is the author of "Hardening Network Infrastructures," and a senior network consultant for Collective Technologies, LLC.

This article originally appeared on SearchWindowsSecurity.com.

Section 12: Study: Network Security Market to Reach \$6 Billion

Andrew R. Hickey, SearchNetworking.com News Writer, December 19, 2005

Network security software and hardware is expected to be a \$6 billion market by 2008, a jump fueled primarily by the increasing need for companies to purchase products that secure content and devices, such as intrusion prevention systems (IPS) and network access control (NAC) equipment.

According to a third-quarter study by Campbell, Calif.-based Infonetics Research Inc., NAC is now the "Holy Grail" of network security, pushing the total market for security products to \$1 billion this year.

But NAC isn't the sole contributor to the booming security market. According to Infonetics principal analyst Jeff Wilson, hackers are inventing new ways to attack corporate networks, and vendors are just as quickly devising ways to protect against them. Those innovations, he said, will continue to push the security market higher.

"First, there's a real need for enterprise-class security for handheld devices, especially wireless client devices, such as Wi-Fi VoIP handsets," said Wilson in a second study, "User Plans for Security Products and Services: North America 2005." "Second, as the next step in perimeter security, network IPS is beginning to make the transition from niche security technology to core network infrastructure. ... And, finally, enterprises are fed up with viruses, spyware and malware, and are willing to make significant investments to put a stop to them."

Infonetics identified the following trends in the burgeoning security market:

- Software, hardware appliances and security routers are the preferred security for most respondents and will continue to be through 2007. Secure routers show the most growth.
- Forty-eight percent of respondents have purchased wireless LAN security products, while 29% said they will buy or are considering buying WLAN security.
- The need to block viruses and the fear of hackers are prompting respondents to buy security products and services en masse.
- Increased service reliability is the most important payback respondents expect from managed security service. Respondents also thought organizations should focus on core competencies, have access to more advanced technology and have access to better expertise.

Regardless of corporations' wants and needs, the studies noted that network security is already a \$1 billion market, with Cisco Systems Inc. ruling the overall hardware and software spaces with a 35% stake. Cisco is followed by Check Point Software Technologies, which comes in second with 10%, and Juniper Networks ranked third with an 8% share. A lot of Cisco's success comes from its NAC framework, which in October was updated with several enhancements, Wilson said.

Infonetics also found that VPN and firewall products make up 77% of security revenue, while intrusion detection and prevention systems rake in 14%, and gateway antivirus 9%. By 2008, however, the research firm predicted intrusion detection and prevention make up 15% of the market, while gateway antivirus products will jump to 12% by 2008.

Section 13: NAC Market Ready to Explode

Andrew R. Hickey, SearchNetworking.com News Writer, January 26, 2006

Not that anyone needs further convincing that network access control (NAC) tools are becoming the "holy grail" of network security, a recent study by Infonetics Research predicts the market for all NAC enforcement will grow an astronomical 1,101% over three years.

According to the study, released last week by the Campbell, Calif.-based research firm, revenue from NAC enforcement will skyrocket from \$323 million in 2005 to \$3.9 billion in 2008.

"Network access control, or NAC, is considered the holy grail of network security, as it is an intelligent network infrastructure that can identify users, identify and do integrity checks on the computers they are using, and then grant them access to specific locations and/or resources and set policies based on user and machine identity," the report states.

The report focuses primarily on NAC enforcement appliances, including network integrated enforcement devices, appliances and Secure Sockets Layer (SSL) VPNs for NAC enforcement, which are expected to have the most dramatic increase.

Network integrated NAC enforcement devices include switches, routers, firewalls and other appliances that support 802.1x authentication and talk to NAC clients and policy servers and then act as the policy enforcement point in a NAC architecture. Some devices also perform firewall, intrusion detection and prevention and other functions.

"By far the largest portion of NAC enforcement revenue between now and 2008 comes from network-integrated enforcement devices, but the biggest change is in NAC enforcement appliances, whose share of the market nearly triples between 2005 and 2008," according to the report's author, Infonetics principal analyst, Jeff Wilson.

The report identifies the "three big guns" that are taking advantage of the booming NAC market: Cisco Systems Inc., Microsoft Corp. and the Trusted Computing Group. Cisco and Microsoft both have their own NAC solutions, with the latter calling it NAP, short for network access protection. The Trusted Computing Group is an independent consortium working on standard implementations for NAC.

The report also highlights that several more companies are emerging with NAC systems, since the hot market is becoming a breeding ground for startups. Some startups that have started to fill the NAC space include InfoExpress, Lockdown and Vernier Networks.

While some of the many startups are likely to find their niche in the vast, growing NAC market, the report said Cisco's NAC framework is the most recognized of the three major players, followed closely by Microsoft. The Trusted Computing Group's Trusted Network Connect NAC options place a distant third.

Over the next three years, as the market for NAC tools begins to consolidate, Infonetics predicts the NAC enforcement appliance segment alone will start to see dramatic growth this year, ultimately shooting up 3,062% between 2005 and 2008.

Along with the overall explosion of NAC enforcement devices, the study also suggests that the market for SSL VPNs for NAC enforcement will see a 798% growth over the same time period.

Infonetics said the most common type will be Ethernet switches that support 802.1x and work with NAC clients and policy servers.

Copyright 2006 TechTarget

Resources From ProCurve Networking by HP



Please click on the white paper title to be directed to the listed white paper.

[**Delivering Intelligent Network Access through Identity Driven Management**](#)

In establishing information technology (IT) networks, companies have traditionally focused on the connection between user devices and the corporate infrastructure, ignoring the unique needs of individuals and groups using the network. Not only does this emphasis hinder workforce productivity, it also creates problems for network security, management and performance.

Discover a new centralized strategy which implements identity driven management (IDM) functionality that is able to automatically configure the network edge through security and management policies defined in a centrally administered database. These IDM solutions facilitate networks that behave uniquely and appropriately for every user.

Learn about the benefits that implanting this strategy would deliver:

- Improvement in productivity
- Improvement in network security
- Improvement in management
- Improvement in performance

[**Identity Driven Management: Technical Brief**](#)

This paper discusses the transition to IDM and highlights ProCurve's IDM solution. It also describes how the solution integrates with a company's existing security and access framework to improve workforce productivity, enhance network security, management and performance, and better serve overall business needs.

[**Interconnecting the Intelligent Edge**](#)

ProCurve Networking by HP offers new strategies and solutions that place and integrate critical intelligence and functionality at the network edge for automated, dynamic configuration of network behavior. This paper will explore the changing networking environment and how this new design approach helps organizations improve business and technology performance while minimizing investment risk. In addition, ProCurve's intelligent EDGE solutions, including the new ProCurve Interconnect Fabric offerings, will be highlighted.

About ProCurve Networking by HP

When the world demands more from your business, you demand more from your network. With [ProCurve Networking by HP](#), you can get more of everything to meet your needs.

ProCurve offers a holistic approach to the design, deployment, and management of secure, mobile, multi-service networks. Its Adaptive EDGE Architecture puts you in control with more intelligence and high-availability gigabit performance at the edge, managed from the core of your network.

With ProCurve, you can get more security, more mobility, more performance, and ultimately more for your money. Because when you protect assets, increase productivity and simplify communications within an integrated architecture strategy based on open standard network technology, your business can grow more.

The bottom line for your bottom line is simple. ProCurve Networking by HP provides a cost-effective, no-compromise network solution that seamlessly adapts to your changing business needs.