Protecting DIGITAL IMAGING SYSTEMS on an open network

Summary

The recent explosion in Internet viruses and worms is causing major disruptions in the network world. As hosts become infected, network congestion increases and impacts the operations of network nodes, including DIGITAL IMAGING SYSTEMS. In a normal network node, such as a workstation, anti-virus software can be applied to the host to proactively detect, screen, and repair many types of viruses. This is a highly effective approach to ensuring host integrity.

Unfortunately, this approach cannot be easily implemented on DIGITAL IMAGING SYSTEMS. There are FDA regulations that impose strict control on how medical-related equipment can be modified. Often, extensive testing is required before anti-virus or other software can be implemented on the equipment. The speed at which new viruses and worms occur make this a non-trivial problem.

However, it is possible to provide limited protection to medical devices on the image network. Firewalls can be employed to filter non-essential traffic to devices, through which many infections occur. Intrusion Detection software can be implemented to provide real-time warning of virus-type activity on the network. Passive Tripwire applications can be applied to hosts to notify administrators of unauthorized activities. While network controls cannot protect against all vulnerabilities, they can greatly decrease the chances of infection.

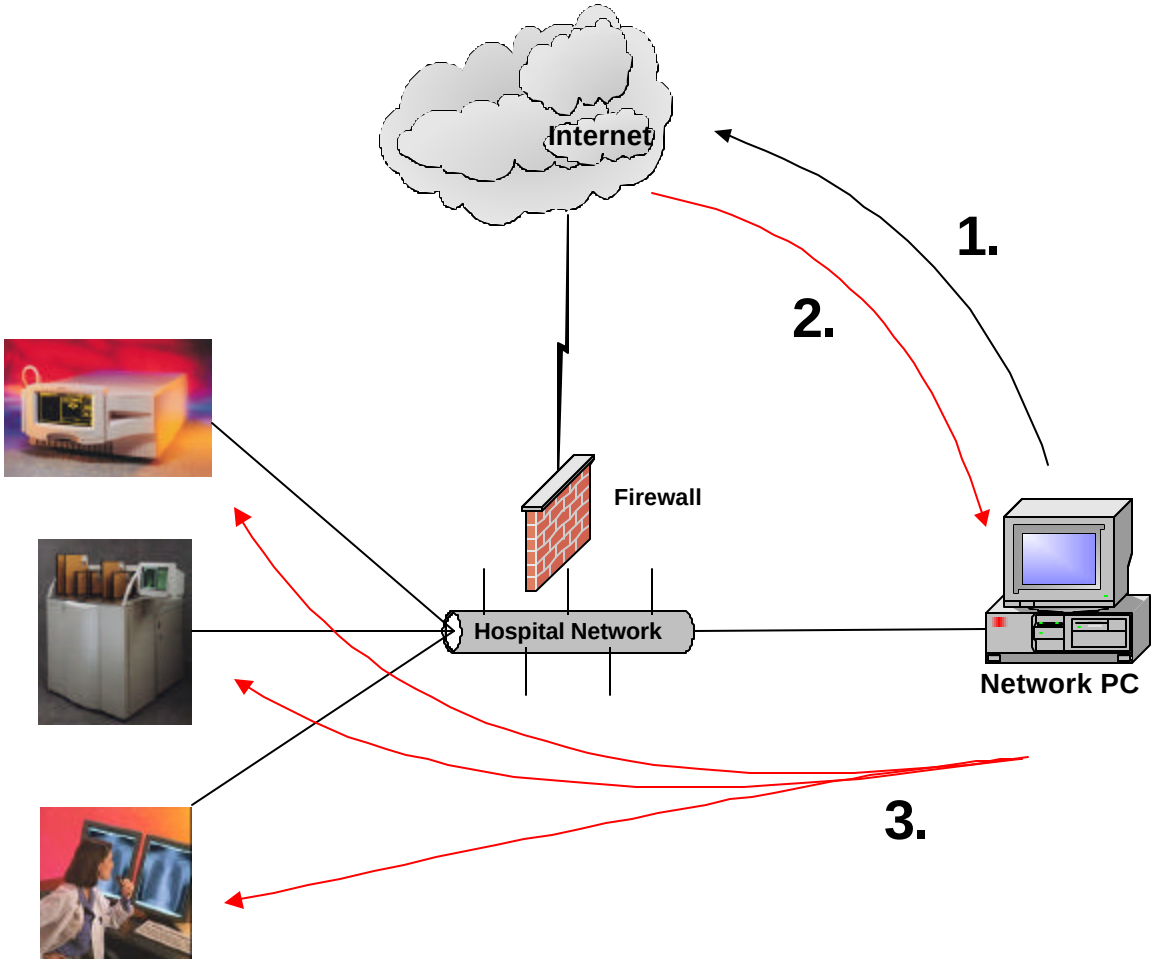
This document explains these approaches to protecting DIGITAL IMAGING SYSTEMS on the network.

Anatomy of a worm

Typically, an unprotected PC or node will contract the virus through contact with an infected machine. The source may be the Internet, another machine on the hospital network, or an infected file from floppy, network, or other media. Once infected, the PC performs a ping sweep on the local network to detect what machines are active on the network. Any address that is active is then attacked on TCP port 135. Lacking any kind of protection, the target machines are themselves infected, and the cycle begins again.

This illustration uses the recent blaster virus as an example of how nodes get infected.

HEALTH IMAGING
A BETTER VIEW OF LIFE.



Example Hospital Network

1. **Unprotected host contracts virus from the Internet or other source**
2. **Protected host becomes infected**
3. **Infected host broadcasts on network and infects DIGITAL IMAGING SYSTEMS**

In the case above, one solution is to shut down all ports on the target machine that are enabled by default, but are not used by the application. This is called "hardening the system". This approach is effective, but in the case of blaster, the port being attacked may be required. One effective way of neutralizing this threat is to make the target machine invisible to the infected PC using network segmentation. There are two ways to provide this isolation, VLANs and Firewalls.

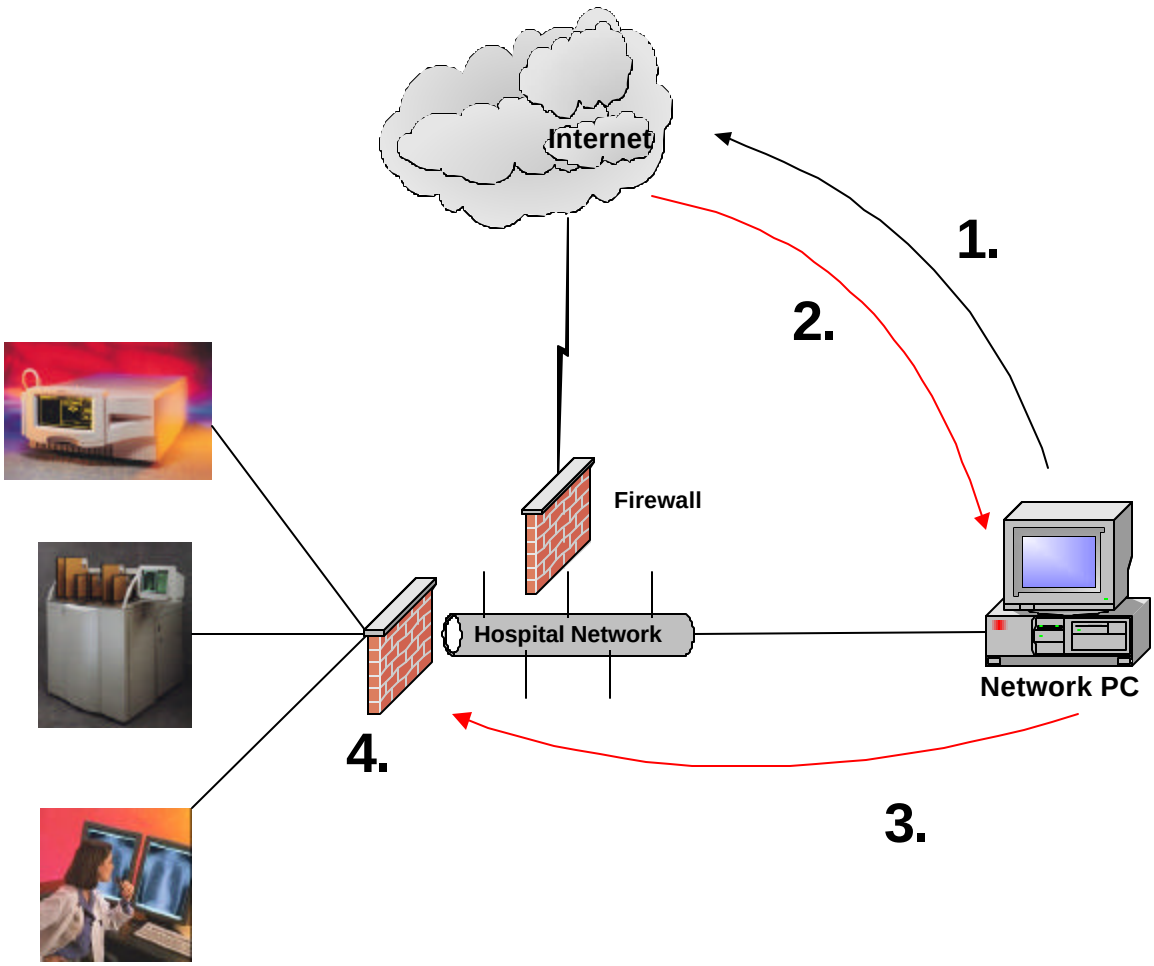
VLAN Isolation – Virtual LANS, or VLANs, are a logical construct in a switched network that effectively isolated equipment on a separate network segment. This provides isolation by blocking broadcast protocols that can be used to locate and infect machines. Vlans are generally inexpensive to implement if the network has adequate equipment. However, VLANs are not adequate protection against worms like blaster, which uses directed probes to scan for machines. These directed probes can span networks and VLANs.

Firewall isolation – a better way to protect networks is to place all DIGITAL IMAGING SYSTEMS on a single segment and install a firewall device between the DIGITAL IMAGING SYSTEM network and the hospital network. The firewall can be programmed to block the directed probes used by worms. By only allowing specific hosts to access DIGITAL IMAGING SYSTEM hosts on restricted ports, the likelihood of a DIGITAL IMAGING SYSTEM contracting a virus via network is greatly reduced. Implementing a firewall has the following benefits:

- Restrict access to only authorized devices – enforces HIPAA requirements for unauthorized access.
- Block all unauthorized traffic and broadcasts – improves network performance
- Provides detailed logs to assist in auditing and troubleshooting.

The following illustration illustrates the use of a firewall in a hospital environment:

HEALTH IMAGING
A BETTER VIEW OF LIFE.



Firewall-protected Network

1. **Unprotected host contracts virus from the Internet or other source**
2. **Protected host becomes infected**
3. **Infected host broadcasts on network**
4. **Firewall blocks probes – DIGITAL IMAGING SYSTEMS protected**

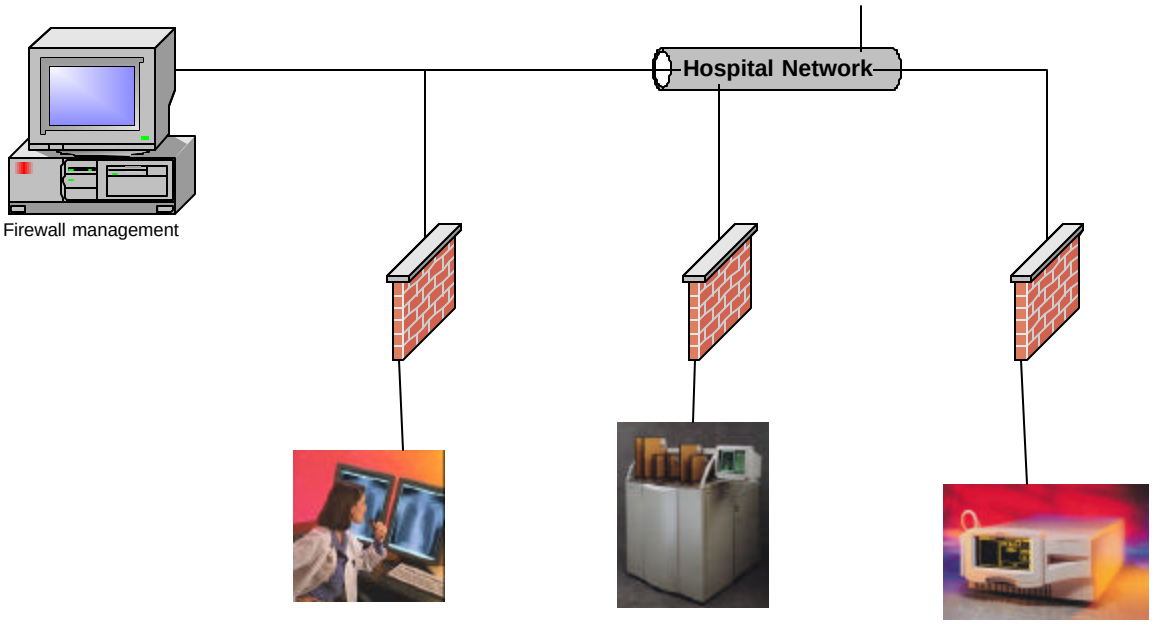
Kodak Health Imaging, unparalleled expertise in imaging and information management technology, is uniquely qualified to create secure, efficient and cost-effective digital environments

The firewall isolation method is effective when all DIGITAL IMAGING SYSTEMS can be consolidated onto a single network or VLAN. In certain cases, equipment may be widely distributed across networks that cannot be VLAN'd. In this case, a centralized firewall does not offer adequate protection.

Distributed firewalls

One way to protect equipment in a distributed network is to use small, inexpensive firewall devices between each piece of equipment and the hospital network. A small appliance, such as a PIX firewall can protect up to several devices in an area. The firewalls can all be securely controlled from a centralized management station on the network.

Refer to the following illustration:



Firewall-protected Devices

The cost associated with this solution is greater, but if proactive protection is required, it is an option.

Intrusion Detection

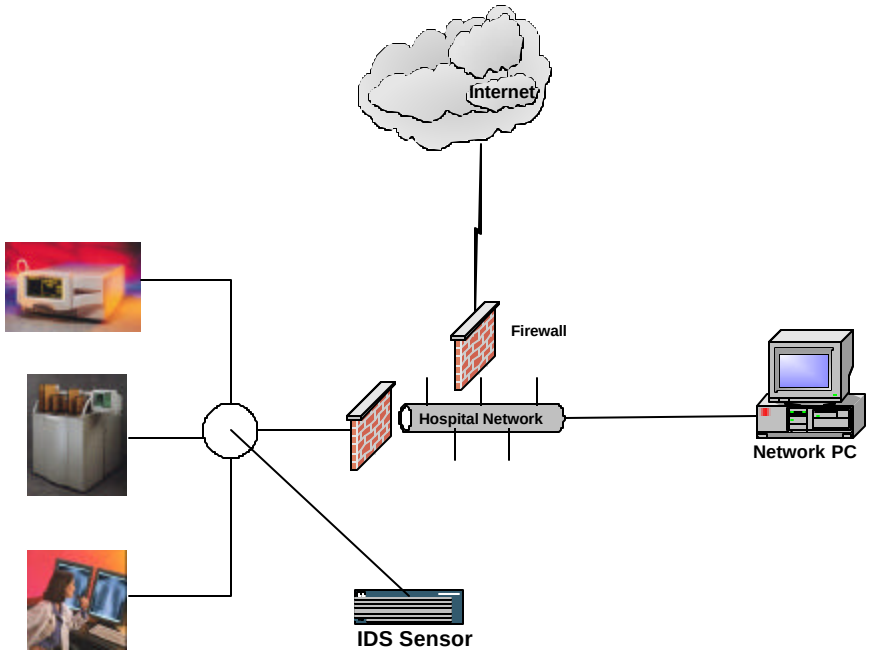
Network Intrusion Detection (IDS) provides real-time detection and reporting of suspicious network activity. It does the by passively monitoring all network traffic and detecting virus and attack patterns against a continuously-updated database of known signatures.

IDS allows an organization to monitor the network not only for virus and worm patterns, but also for network attacks, such as denial of service attacks. The IDS systems have graphical interfaces that can easily pinpoint the source of infection or attack to allow very fast problem identification and resolution.

IDS systems can also be configured to alert using e-mails, pagers, or SNMP traps.

IDS systems also generate metrics and reports, and are ideal for capturing traffic for analysis and forensic evidence.

Refer to the following illustration:



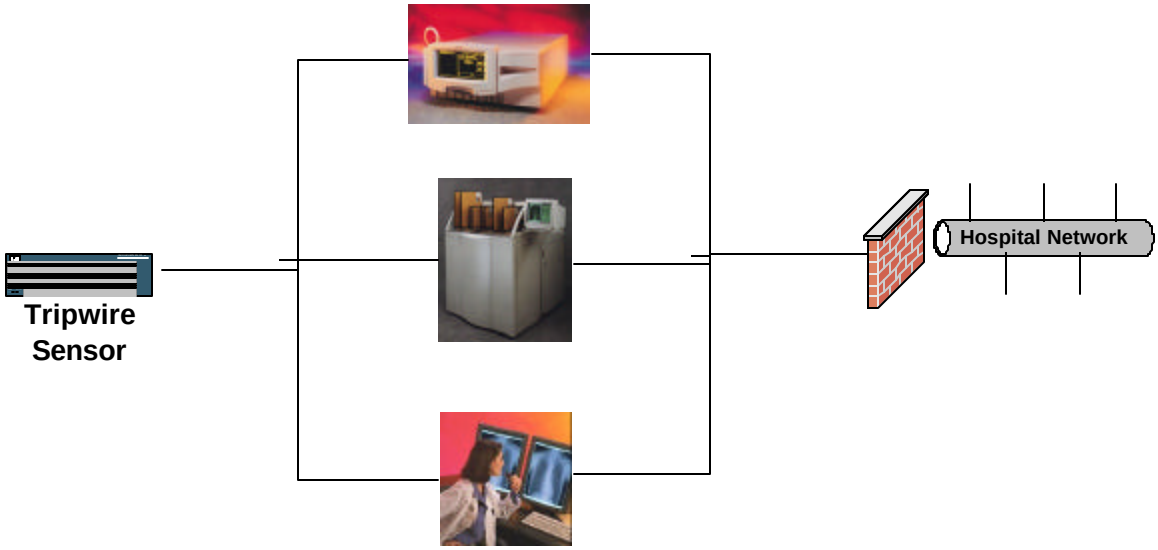
IDS-monitored Network

In the above example, the IDS sensor inspects and correlates all network packets. If a virus or scan signature is detected, an alert is generated indicating an attack and pin-pointing the source so preventative and corrective action can be taken.

Tripwire – monitoring the DIGITAL IMAGING SYSTEMS

Another option for securing the network is the use of tripwire type software. This software watches the target machine continuously and creates an alert if files or registry entries are changed. This provides near real-time notification of virus or penetration events, and is especially useful for monitoring web server applications and Microsoft file systems.
Tripwire software is also available that runs on the target system and when a file change is detected, can automatically overwrite the modified file with a known clean copy from CD.

Refer to the following diagram:



Tripwire-monitored devices

The combination of network IDS and tripwire host protection is very effective at drastically reducing the chance of infection and also provides attack detection and mitigation.

Conclusion

Industry best practices dictate that anti-virus software on the target machine is the most effective solution to preventing infections. However, in the event where anti-virus software is not possible, or where higher levels of security are required, the above-mentioned network controls can be used to protect DIGITAL IMAGING SYSTEMS.

Network Services position is that all DIGITAL IMAGING SYSTEMS be on an isolated network, with a firewall between the DIGITAL IMAGING SYSTEMS and hospital networks. The DIGITAL IMAGING SYSTEM network should employ Intrusion Detection Systems to provide proactive and real-time notification of scans or attacks. Tripwire solutions should be implemented to quickly detect when a change has occurred and help restore the system as fast as possible.

Network services specialize in the above solutions and have successfully helped hospital networks protect their DIGITAL IMAGING SYSTEMS from viruses and worms.