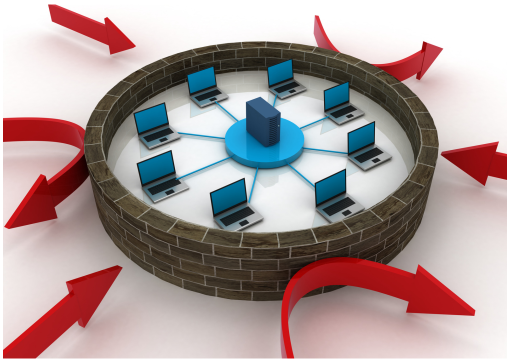
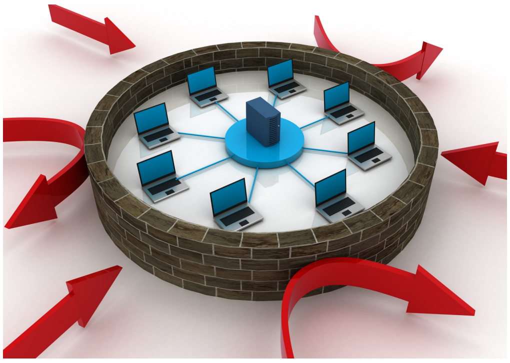


PCI DSS REQUIREMENT 1: TERMS & DEFINITIONS

This reference sheet contains the terms and definitions used in our course, "Build & Maintain a Secure Network: What You Need to Know to Monitor & Manage PCI DSS Requirement 1.

Term	Definition
Network Security Controls (NSCs)	NSCs are Firewalls and other network security technologies that act as network policy enforcement points.
Firewall	Firewalls typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules.
Firewall rules	Firewall rules are what defines how the firewall will be configured and managed to properly perform their security function. Firewall rules determine the traffic that's allowed or denied and control how organizations protect their networks from malicious activity
Router	A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.
Switch	A network switch connects devices within a network (often a local area network, or LAN*) and forwards data packets to and from those devices. Unlike a router, a switch only sends data to the single device it is intended for (which may be another switch, a router, or a user's computer), not to networks of multiple devices.



PCI DSS REQUIREMENT 1: TERMS & DEFINITIONS

This reference sheet contains the terms and definitions used in our course, "Build & Maintain a Secure Network: What You Need to Know to Monitor & Manage PCI DSS Requirement 1.

Term	Definition
Trusted Network	A Trusted Network is a network of devices that are connected to each other, open only to authorized users, and allows for only secure data to be transmitted.
Untrusted Network	An Untrusted Network (The internet...) is a network that is external to the networks belonging to an organization and which is out of the organization’s ability to control or manage.
DMZ	A DMZ is a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic. A DMZ is considered an untrusted network
Anti-Spoofing	Anti-Spoofing - this is a mechanism to detect and prevent incoming traffic from a false source address.
Network Address Translation (NAT)	Network Address Translation (NAT) is designed for IP address conservation as well as securing private networks. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT allows a single device, such as a router or firewall, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.