**Compliance Within the LAN-to-WAN Domain**

The purpose of the LAN-to-WAN Domain is to provide stable and controlled access from LAN resources to a WAN. You must ensure your

data is secure in the LAN-to-WAN Domain as well as in all other domains.

Devices and Components Commonly Found in the LAN-to-WAN Domain :

* **ROUTERS**

A router is a network device that connects two or more separate networks. In the context of the LAN-to-WAN Domain, a router makes the actual connection between the LAN and the WAN. A router can be a standalone network device or it can be software that runs on a computer. In either case, the hardware must contain at least two network interfaces—one for each network. A router works by inspecting the address portion of the packet and forwarding the packet to the correct network. The process of examining each packet is time consuming and can slow your network

down. Newer network devices and software often contain support for Multiprotocol Label Switching (MPLS). MPLS networks add a simple label to each network packet. The routing

devices in the network forward packets based on the address in the label as opposed to data in the header portion of the packet.

* **FIREWALLS**

A firewall is a network security measure designed to filter out undesirable network traffic.

Like a router, a firewall can be a network device or software running on a computer. Firewalls provide an important security capability. You can define rules for each firewall that

tell the firewall how to filter network traffic. You can restrict which packets you allow to flow through the LAN-to-WAN Domain. Firewalls give you the ability to aggressively control what types of information can travel between your LANs and WANs.

* **HONEYPOTS**

A honeypot is a server deliberately set up to trap attackers.

There are at least two dangers with honeypots. First, a honeypot that is connected to your LAN could provide an attacker with an entry point to your LAN. If the attacker successfully compromises the host, the attacker could access protected LAN resources.

Second, an attacker with any skill will likely eventually realize the honeypot for what it is. An attacker might assume an organization that goes to the trouble of setting up a honeypot might have a truly valuable resource they are trying to hide. In this case, the honeypot

actually draws more attention to your valuable resources instead of diverting attention away.

Honeypots require near-constant attention, both automated and by personnel. When a honeypot goes ignored for too long, the dangers just mentioned become real risks with dire

consequences.

* **Internet Service Provider Connections and Backup Connections**
* **Intrusion Detection Systems/Intrusion Prevention Systems**
* **Web Content Filtering Devices**
* **Traffic-Monitoring Devices**

Penetration Testing and Validating LAN-to-WAN Configuration :

Testing security controls and configuration settings is crucial to ensuring you have the right

controls in place. One particular type of testing simulates actions an attacker would take to attack your network. This type of test is called a penetration test because the purpose of the test is to attempt to penetrate, or compromise, your security controls.

External Attacks

The more common type of penetration test is from the perspective of the external attacker.

The penetration tester, also called the pentester, launches a series of attacks from outside the target’s network. In most cases, the pentester conducts the tests from a computer connected

to the Internet. The tester simulates the actions an attacker would take when developing an attack on your organization.