Cisco Identity Solutions

What is Connected to Your Network?

The rapid growth of personal devices that can be connected to your network is dramatically increasing your network's vulnerability to attacks. Employees, contractors and citizens can easily introduce the following to your network:

- Personal computers
- Tablet computers
- Smart phones
- Printers
- Gaming systems
- Wireless Access Points

Many people fail to keep their security patches, virus protection and operating systems up to date. Furthermore as personally owned devices, people commonly use these devices on unsecured networks for recreational purposes that can increase there exposure to malware.

When these devices are connected to your network, your risk of being attacked can increase significantly

What Can You Do?

The average cost of a security breach is $3.4 million and can be as high as $31 million*. But, there are many shortcomings to traditional approaches to access control:

- Manually tracking MAC addresses is time consuming and can easily become inaccurate.
- Asset and patch management solutions do not address unmanaged assets or relate to the network topology
- Legacy access control mechanisms are difficult to deploy and inflexible.

With so much at stake, you need an automated solution that will adapt to your needs and minimize your risk.

* 2009 Annual Study: Cost of Data Breach, Ponemon Institute

Cisco's Identity Solution

Cisco switching, policy and virtual private network products include several technologies that – when used together – provide three key capabilities:

- Visibility into who and what is connected to your network.
- Automation for simplifying operations and adapting to changing needs.
- Controls for limiting access to information and resources.

Depending on the needs of your network, these technologies can be used in varying degrees from a monitor only mode to enforcing stringent control.

Cisco Switches

802.1X – Open Mode

This unique capability allows us to deploy 802.1X-based access-control technologies in a monitor only mode. In Open Mode, you will be alerted to 802.1X exceptions, but the connections will be allowed. This is particularly useful in the early stages of an 802.1X deployment.

Flexible Authentication (Flex-Auth)

Not all devices can be authenticated by a single method. Flex-Auth cycles through three different authentication modes: 802.1X, MAC Authentication Bypass, and Web Authentication. This provides the most comprehensive solution for authenticating all the devices on your network.

Security Group Tags

Role-based access control is simplified by removing the dependency on network topology. With Cisco switches, you no longer need to reallocate IP addresses, deploy MPLS or VRFs, and change VLANs to implement role-based access control.

Network Device Access Control

Cisco switches can also be authenticated – in addition to the endpoints. This helps to ensure the integrity and authenticity of your network by controlling what network devices are added to the network.

802.1AE – Port Level Encryption

Cisco switches provide confidentiality and integrity to data packets entering and leaving our switches. This helps to prevent unauthorized network taps, packet manipulation, and spoofing of other user's credentials within the network.

Cisco Policy Engines

Cisco Secure Access Control System (ACS) 5

ACS provides a rule-based policy-engine that can be used to define access to the network in a customizable way. Most organizations have unique network access policies policy requirements. ACS 5 provides customizable logic to support the most complex deployments with ease.

Cisco Network Access Control (NAC) Profiler

Devices such as printers, IP phones, and badge readers often need to be identified without an authentication taking place. Profiler analyzes data taken from the network switches to categorize what type of devices are accessing the network, so that effective access controls can be put in place for these devices.

Cisco Identity Services Engine

The Cisco Identity Services Engine combines the functionality of ACS 5, NAC Profiller, Endpoint Compliance and guest services into a single solution for managing policy.

Cisco Virtual Private Networks

AnyConnect 3

Simplify network access with a unified wired & wireless supplicant, VPN client, and cloud-based web proxy services for remote users. AnyConnect 3 delivers a consistent interface to network resources whenever users are wired, wireless, or remote and using a VPN.

Learn More

For more information, please go to the following website:
www.cisco.com/go/cyber