Cisco Secure Mobility Solutions

Are Your People on the Move?

With the rapid growth in consumer electronics such as tablet computers and smart phones, employees expect to connect any device to the network at any time and from anywhere. Providing a network that secures these devices will increase productivity and citizen satisfaction with your agency while protecting your information from security risks.

Do Employees Need to Work Remotely?

There are times when employees simply cannot come into the office. During the snow storms of 2011, roads were frequently closed for several days. In the event of a pandemic flu, it may not be safe for employees or citizens to congregate in an office building. Whatever the cause, many agencies must continue to function.

Offering a flexible environment in which employees can work part or all of the time from their homes is also a great tool for attracting the talented people your agency needs to accomplish its mission.

How Do You Maintain Security Policies?

Employee owned devices pose two major challenges for security policies:

- There is a vast array of different devices and software
- Employees may fail to install security updates

Using the network as the common platform for implementing security policy is a device agnostic approach.

Cisco Secure Mobility Solutions

Extending Your Agency's Network

Cisco Virtual Office and OfficeExtend solutions extend your agency's network across a public network and typically into employee's homes.

Cisco Virtual Office

Virtual office solutions provide full IP phone, wireless, data, and video services to staff wherever they may be located. Once established, additional locations can be added with zero-touch deployments.

The Cisco Virtual Office solution consists of the following components:

- Cisco 800 Series ISR
- Cisco Unified IP Phone
- Cisco Adaptive Security Appliance or VPN enabled router
- Cisco Secure Access Control System

Cisco OfficeExtend

The OfficeExtend access point plugs into any router that provides an Internet connection. Then, it establishes a secure tunnel to the corporate network so that remote employees can access data, voice, video, and applications the same way they do at the office.

The Cisco OfficeExtend Solution requires the following:

- Cisco Aironet 1140 or 1130AG Series Access Point
- Cisco 5500 Series Wireless LAN Controller
- Cisco Wireless Control System
- Cisco Secure Access Control System

CiscoOffice Extend is compatible with Cisco Unfied Wireless IP Phones.

Securing Devices Across Any Network

The Cisco AnyConnect Secure Mobility Solution provides a comprehensive, highly secure mobility solution. It combines industry-leading Cisco web security with next-generation remote access technology to help organizations easily manage the security risks.

Users can access the network with their device of choice, including laptops and handhelds. The Cisco AnyConnect Secure Mobility Solution offers:

- Security policy enforcement that is context-aware, comprehensive, and preemptive.
- Connectivity that is intelligent, simple, and always on.
- Highly secure mobility across the rapidly increasing number of managed and unmanaged mobile devices.

This solution requires the following:

- Cisco AnyConnect Secure Mobility Client
- Cisco Adaptive Security Appliance
- Cisco IronPort Web Security appliance for policy enforcement

Defending Your Network From Attacks

Cisco IronPort Email Security Appliance

This solution provides outstanding protection to agencies of all sizes. Sophisticated and scalable mechanisms minimize the risk of email-based attacks and data loss.

Best-in-class technologies work together to prevent and respond to multilevel threats. Capabilities include:

- Spam protection
- Data loss prevention (DLP)
- Virus defense
- Email encryption Tracking and reporting tools

Cisco IronPort Web Security Appliance

This appliance provides data loss detection and prevention against malware that could be used for attacks. Malware leveraging HTTP as a signaling protocol can be detected and blocked. It also defends against web-based applications that could be used to transfer information outside of an organization overtly. Web applications like blogs, email, social networking and any type of posts can be controlled in accordance with an organization's security policies.

Cisco Adaptive Security Appliance

Cisco ASA 5500 Series Adaptive Security Appliances provide reputation-based control for an IP address or domain name. This has proved to be very successful in combating rogue email and web servers that typically use dynamic or changing IP addresses.

The Cisco ASA Botnet Traffic Filter is integrated into all Cisco ASA appliances, and inspects traffic traversing the appliance. The Botnet Traffic Filter monitors all ports and performs a real-time lookup in its database of known botnet IP addresses and domain names.

Cisco Intrusion Prevention System

The Cisco IPS plays an important role in the overall security posture of an organization. Cisco's IPS offers many different form factors and allows an organization to deploy the right form factor based on the location and throughput requirements. Cisco's network-based intrusion prevention identifies, classifies, and stops known and unknown threats. Cisco's IPS is one of the most widely deployed intrusion prevention systems around the world and provides the following:

- Protection against more than 30,000 known threats
- Timely signature updates
- Cisco Global Correlation to dynamically recognize, evaluate, and stop emerging Internet threats

Learn More

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