Network Security and Networking Protocols

Arvind Kumar Sharma [1] and Chattar Singh Lamba [2]

[1] Research Scholar
arvind_vyas07@yahoo.co.in
[2] Research Guide
kunjean_lamba@yahoo.com

Abstract. In the field of networking, the specialist area of **Network Security** consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together.

The terms Network Security and Information Security are often used interchangeably. Network Security is generally taken as providing protection at the boundaries of an organization by keeping out intruders (hackers). Information Security, however, explicitly focuses on protecting data resources from malware attack or simple mistakes by people within an organization by use of Data Loss Prevention (DLP) techniques. One of these techniques is to compartmentalize large networks with internal boundaries. Employees have to cross these boundaries and be authenticated when attempting to access protected information.

1 Introduction

In the field of networking, the specialist area of **Network Security** consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together.

The terms Network Security and Information Security are often used interchangeably. Network Security is generally taken as providing protection at the boundaries of an organization by keeping out intruders (hackers). Information Security, however, explicitly focuses on protecting data resources from malware attack or simple mistakes by people within an organization by use of Data Loss Prevention (DLP) techniques. One of these techniques is to compartmentalize large networks with internal boundaries. Employees have to cross these boundaries and be authenticated when attempting to access protected information.

Network security starts from authenticating the user, commonly with a username and a password. Since this requires just one thing besides the user name, i.e. the password which is something you 'know', this is sometimes termed one factor authentication. With two factor authentication something you 'have' is also used (e.g. a security token or 'dongle', an ATM card, or your mobile phone), or with three factor authentication something you 'are' is also used (e.g. a fingerprint or retinal scan).

N. Meghanathan et al. (Eds.): NeCoM, WiMoN, and WeST 2010, CCIS 90, pp. 90–97, 2010.

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behavior and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Individual events occurring on the network may be logged for audit purposes and for later high level analysis.

1.1 Introduction to Networking

A basic understanding of computer networks is requisite in order to understand the principles of network security. In this section, we'll cover some of the foundations of computer networking, then move on to an overview of some popular networks. Following that, we'll take a more in-depth look at TCP/IP, the network protocol suite that is used to run the Internet and many intranets.

A "network" has been defined as any set of interlinking lines resembling a net, *a network of roads* an interconnected system, *a network of alliances*." This definition suits our purpose well: a computer network is simply a system of interconnected computers. *How* they're connected is irrelevant, and as we'll soon see, there are a number of ways to do this.

1.2 Network Security, Modern Network Security Threats

Router Based Network Security is a process, not a product. Network security encompasses those steps that are taken to ensure the confidentiality, integrity, and availability of data or resources. Network security is the protection of information and systems and hardware that use, store, and transmit that information.

Network security is now an integral part of computer networking. Network security involves protocols, technologies, devices, tools, and techniques to secure data and mitigate threats. Network security solutions emerged in the 1960s but did not mature into a comprehensive set of solutions for modern networks until the 2000s. When the first viruses were unleashed and the first DoS attack occurred, the world began to change for networking professionals. To meet the needs of users, network professionals learned techniques to secure networks. The primary focus of many network professionals evolved from designing, building, and growing networks to securing existing networks.

1.3 Risk Management – A Game of Security

It is very important to understand that in security, one simply cannot say ``what's the best firewall?" There are two extremes: absolute security and absolute access. The closest we can get to an absolutely secure machine is one unplugged from the network, power supply, locked in a safe, and thrown at the bottom of the ocean. Unfortunately, it isn't terribly useful in this state. A machine with absolute access is extremely convenient to use: it's simply there, and will do whatever you tell it, without questions, authorization, passwords, or any other mechanism. Unfortunately, this isn't terribly practical, either: the Internet is a bad neighborhood now, and it isn't long before some bonehead will tell the computer to do something like self-destruct, after which, it isn't terribly useful to you.

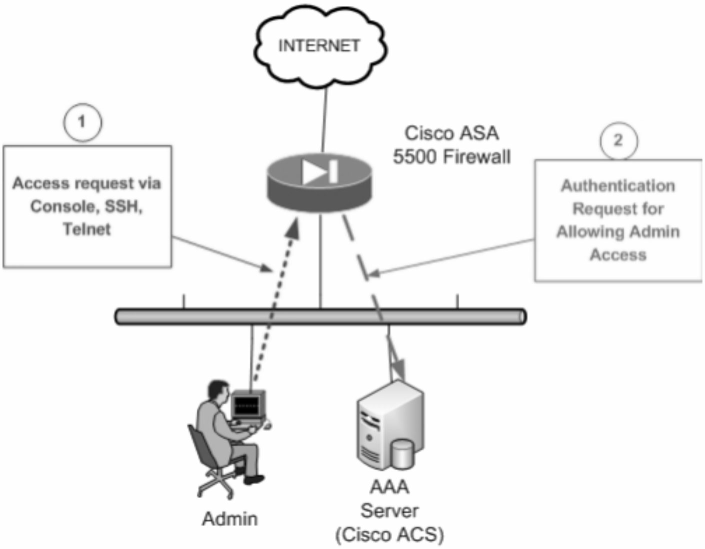
1.4 Securing Networking Devices

Securing outgoing network traffic and scrutinizing incoming traffic are critical aspects of network security. Securing the edge router, which connects to the outside network, is an important first step in securing the network.

Device hardening is an essential task that must never be overlooked. It involves implementing proven methods for physically securing the router and protecting the router's administrative access using the command-line interface (CLI) as well as the Router and Security Device Manager (SDM). Some of these methods involve securing administrative access, including maintaining passwords, configuring enhanced virtual login features, and implementing Secure Shell (SSH). Because not all information technology personnel should have the same level of access to the infrastructure devices, defining administrative roles in terms of access is another important aspect of securing infrastructure devices.

1.5 Authentication, Authorization and Accounting

AAA (Authentication, Authorization and Accounting) is a way to securing Routers in networks. AAA Plays different rolls in the network Security, Like Authentication tell you that who are you, Authorization tells you that what you can do and Accounting tell you that what you did.

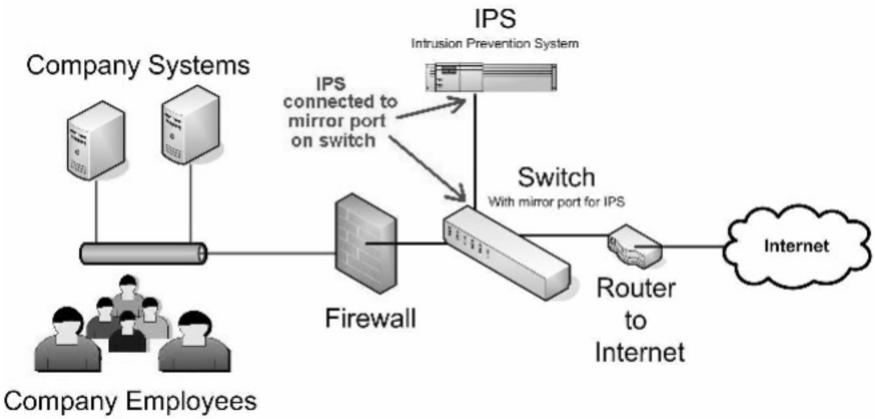

INTERNET
1
Access request via Console, SSH, Telnet
Cisco ASA 5500 Firewall
2
Authentication Request for Allowing Admin Access
Admin
AAA Server (Cisco ACS)

1.6 Implementing Firewall Technologies

A firewall is a secure and trusted machine that sits between a private network and a public network. The firewall machine is configured with a set of rules that determine which network traffic will be allowed to pass and which will be blocked or refused. In some large organizations, you may even find a firewall located inside their corporate network to segregate sensitive areas of the organization from other employees. Many cases of computer crime occur from within an organization, not just from outside.

1.7 Implementing Intrusion Prevention System

Intrusion prevention is a preemptive approach to network security used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) monitors network traffic. However, because an exploit may be carried out very quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the network administrator. For example, an IPS might drop a packet that it determines to be malicious and block all further traffic from that IP address or port. Legitimate traffic, meanwhile, should be forwarded to the recipient with no apparent disruption or delay of service.

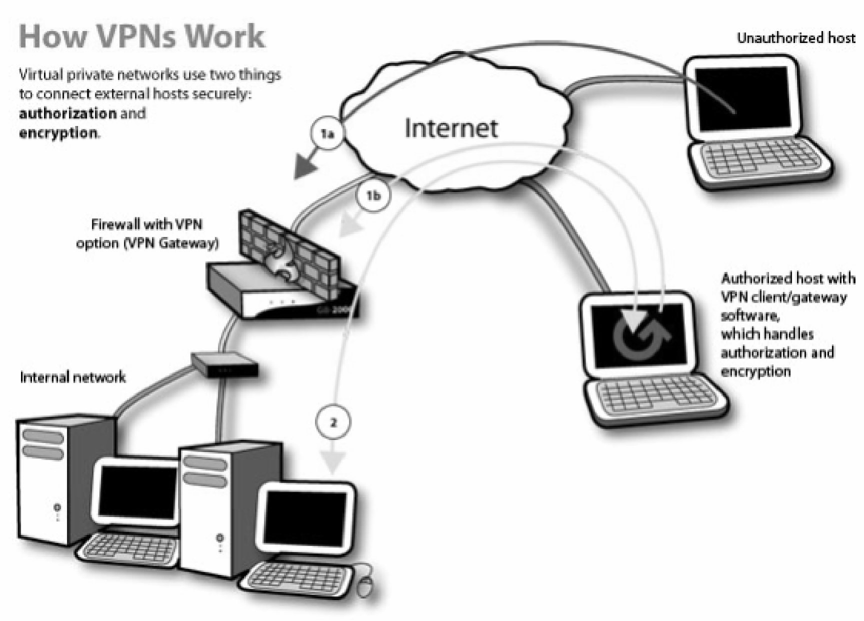


1.8 Securing Local Area Networks

In the Local Area Networks, There are so many types of internal threats regarding break you network. We can stop these type activities by the End Point Security, VLAN's, NAC Devices, Port Security, and your date by the SAN Security.

1.9 Implementing Virtual Area Networks

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.


How VPNs Work
Virtual private networks use two things to connect external hosts securely: **authorization** and **encryption**.
Unauthorized host
Internet
1a
1b
2
Firewall with VPN option (VPN Gateway)
Authorized host with VPN client/gateway software, which handles authorization and encryption
Internal network

2 Network Protocols

Network protocols define a language of rules and conventions for communication between network devices.

2.1 Definition

A **network protocol** defines rules and conventions for communication between network devices. Protocols for computer networking all generally use packet switching techniques to send and receive messages in the form of *packets*.

Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. Some protocols also support message acknowledgement and data compression designed for reliable and/or high-performance network communication. Hundreds of different computer network protocols have been developed each designed for specific purposes and environments.

2.2 Internet Protocols

The Internet Protocol family contains a set of related (and among the most widely used network protocols. Besides Internet Protocol (IP) itself, higher-level protocols like TCP, UDP, HTTP, and FTP all integrate with IP to provide additional capabilities. Similarly, lower-level Internet Protocols like ARP and ICMP also co-exist with IP. These higher level protocols interact more closely with applications like Web browsers while lower-level protocols interact with network adapters and other computer hardware.

2.3 Routing Protocols

Routing protocols are special-purpose protocols designed specifically for use by network routers on the Internet. Common routing protocols include EIGRP, OSPF and BGP.

2.4 How Network Protocols Are Implemented

Modern operating systems like Microsoft Windows contain built-in services or daemons that implement support for some network protocols. Applications like Web browsers contain software libraries that support the high level protocols necessary for that application to function. For some lower level TCP/IP and routing protocols, support is implemented in directly hardware (silicon chipsets) for improved performance.

2.5 OSI Layers and Their Protocols

2.5.1 Layer 1 Protocols (Physical Layer)

ADSL Asymmetric digital subscriber line, ISDN Integrated Services Digital Network, T-carrier (T1, T3, etc.),E-carrier (E1, E3, etc.), RS-232 (a serial line interface originally developed to connect modems and computer terminals).

2.5.2 Layer 1+2 Protocols

Ethernet, OTN ITU-T G.709 Optical Transport Network also called Optical Channel Wrapper or Digital Wrapper Technology.

2.5.3 Layer 2 Protocols (Data Link Layer)

ARCnet Attached Resource Computer Network, CDP Cisco Discovery Protocol, DCAP Data Link Switching Client Access Protocol, Dynamic Trunking Protocol, FDDI Fiber Distributed Data Interface, Frame Relay, ITU-T G.hn Data Link Layer, HDLC High Level Data Link Control, IEEE 802.11 WiFi, IEEE 802.16 WiMAX, LocalTalk, L2F Layer 2 Forwarding Protocol, L2TP Layer 2 Tunneling Protocol, PPP Point-to-Point Protocol, PPTP Point-to-Point Tunneling Protocol, NDP Neighbor Discovery Protocol, SLIP Serial Line Internet Protocol (obsolete), STP Spanning Tree Protocol, Token ring, VTP VLAN Trunking Protocol, Layer 2+3 protocols, ATM Asynchronous Transfer Mode, Frame relay, a simplified version of X.25, MPLS Multi-protocol label switching, X.25, ARP Address Resolution Protocol, RARP Reverse Address Resolution Protocol.

2.5.4 Layer 1+2+3 Protocols

MTP Message Transfer Part, NSP Network Service Part, Layer 3 protocols (Network Layer), EGP Exterior Gateway Protocol, EIGRP Enhanced Interior Gateway Routing Protocol, ICMP Internet Control Message Protocol, IGMP Internet Group Management Protocol, IGRP Interior Gateway Routing Protocol, IPv4 Internet Protocol version 4, IPv6 Internet Protocol version 6, IPSec Internet Protocol Security, IPX Internetwork Packet Exchange.

2.5.5 Layer 3 Protocols (Network Layer Management)

IS-IS Intermediate system to intermediate system, OSPF Open Shortest Path First, BGP Border Gateway Protocol, RIP Routing Information Protocol, ICMP Router Discovery Protocol, Gateway Discovery Protocol.

2.5.6 Layer 3.5 Protocols

Layer 3+4 protocol suites, Xerox Network Systems, Layer 4 protocols (Transport Layer), AHAH Authentication Header over IP or IPSec, ESPESP Encapsulating Security Payload over IP or IPSec, GRE Generic Routing Encapsulation for tunneling, IL Originally developed as transport layer for 9P, SCTP Stream Control Transmission Protocol, Sinec H1 for telecontrol, SPX Sequenced Packet Exchange, TCP Transmission Control Protocol, UDP User Datagram Protocol, Layer 5 protocols (Session Layer), 9P Distributed file system protocol developed originally as part of Plan 9, NCP NetWare Core Protocol, NFS Network File System, SMB Server Message Block, SOCKS "SOCKetS".

2.5.7 Layer 7 Protocols (Application Layer)

BitTorrent, A peer-to-peer file sharing protocol, BOOTP, Bootstrap Protocol, Diameter, an authentication, authorization and accounting protocol, DNS Domain Name System, DHCP, Dynamic Host Configuration Protocol, ED2K, A peer-to-peer file sharing protocol, FTP, File Transfer Protocol, Finger, which gives user profile information, Gnutella, a peer-to-peer file-swapping protocol, Gopher, a hierarchical hyperlinkable protocol, HTTP, HyperText Transfer Protocol, IMAP, Internet Message Access Protocol, Internet Relay Chat (IRC), LDAP Lightweight Directory Access Protocol, MIME, Multipurpose Internet Mail Extensions, MSNP, Microsoft Notification Protocol (used by Windows Live Messenger), MAP, Mobile Application Part, NetBIOS, File Sharing and Name Resolution protocol - the basis of file sharing with Windows, NNTP, News Network Transfer Protocol, NTP, Network Time Protocol, NTCIP, National Transportation Communications for Intelligent Transportation System Protocol, POP3 Post Office Protocol Version 3, RADIUS, an authentication, authorization and accounting protocol, Rlogin, a UNIX remote login protocol, rsync, a file transfer protocol for backups, copying and mirroring, RTP, Real-time Transport Protocol, RTSP, Real-time Transport Streaming Protocol, SSH, Secure Shell, SISNAPI, Siebel Internet Session Network API, SIP, Session Initiation Protocol, a signaling protocol, SMTP, Simple Mail Transfer Protocol, SNMP, Simple Network Management Protocol, SOAP, Simple Object Access Protocol, STUN, Session Traversal Utilities for NAT, TUP, Telephone User Part, Telnet, a remote terminal access protocol, TCAP, Transaction Capabilities Application Part, TFTP, Trivial File Transfer Protocol, a simple file transfer protocol, WebDAV, Web Dist Authoring and Versioning.

3 Conclusions

Security is a very difficult topic. Everyone has a different idea of what ``security" is, and what levels of risk are acceptable. The key for building a secure network is to *define what security means to your organization*. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. Projects and systems can then be broken down into their components, and it becomes much simpler to decide whether what is proposed will conflict with your security policies and practices.

Many people pay great amounts of lip service to security, but do not want to be bothered with it when it gets in their way. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him. Users who find security policies and systems too restrictive will find ways around them. It's important to get their feedback to understand what can be improved, and it's important to let them know *why* what have been done has been, the sorts of risks that are deemed unacceptable, and what has been done to minimize the organization's exposure to them.

References

1. Watkins, M., Wallace, K.: CCNA Security: Official Exam Certification Guide. Pearson Education, London
2. Lammle, T.: CCNA: Cisco Certified Network Study Guide. Sybex
3. Odom, W.: CCNA Exam Certification Guide. Cisco Press,
4. Lowe, D.: Networking: All-in-one Desk reference for Dummies. Wiley, Chichester
5. Stewart, B.D., Gough, C.: CCNP BSCI Official Exam Certification Guide. Cisco Press,
6. Hucaby, D.: CCNP BCMSN Official Exam Certification Guide. Cisco Press
7. Tanenbaum, A.S.: Computer Networks. Pearson Education, London
8. Morgan, B., Lovering, N.: CCNP ISCW Offical Exam Certification Guide. Cisco Press
9. Bastien, G., Degu, C.: CCSP Cisco Pix Firewall Advance Exam Certification Guide. Cisco Press
10. Hall, E.: Internet Core Protocols, The Definitive Guide. O’Reilly, Sebastopol