Global Information Assurance Certification Paper

Cisco Way

By Joseph S. White

This document will be an overview to " Cisco SAFE: "A Security Blueprint for Enterprise Networks" (Convery). The purpose of Cisco SAFE is to give network designers a guide to designing and implementing secure networks. SAFE assumes you have a security policy in place and does not recommend deploying security technologies without such a policy. While SAFE is a guide for Enterprise networks, its information can certainly be used for smaller networks. Remember there are no hard and fast rules, not all the recommendations in SAFE are viable options for all networks. Depending on your budget constraints, personnel, geographic location, etc. you may need to make changes accordingly.

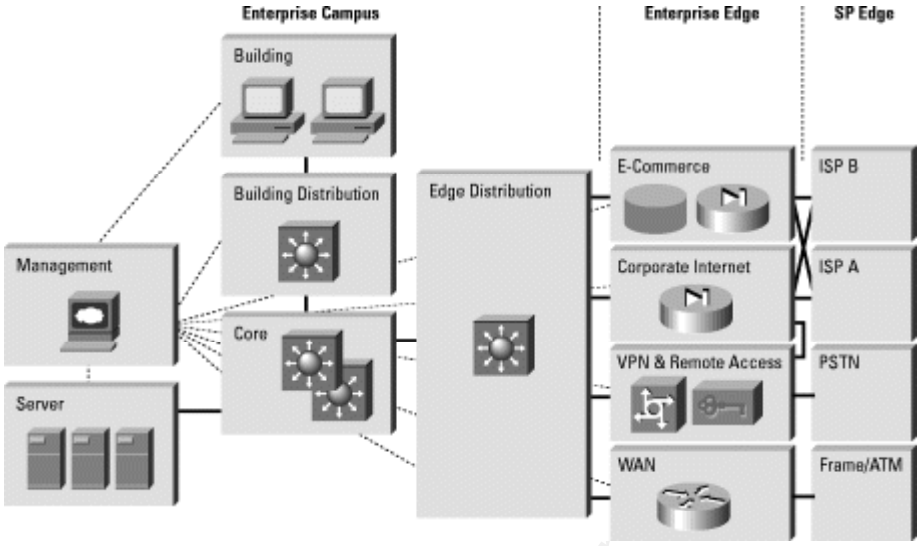
SAFE is a security architecture, which uses a modular approach to network design. The modular approach lets designers view the relationships and implement security on a module-by-module basis, rather than the single enterprise wide approach. Each module represents a functional area within the enterprise. We have various top level and secondary modules represented below:

1. Enterprise Campus
    a. Management Module
    b. Server Module
    c. Building Module
    d. Building Distribution Module
    e. Core Module
    f. Edge Distribution Module

2. Enterprise Edge
    a. Corporate Internet Module
    b. WAN Module
    c. VPN & Remote Access Module
    d. E-Commerce Module

    Note: WAN, VPN, and E-Commerce modules will be outside the scope of this document.

3. Service Provider Edge – This module is not the responsibility of the enterprise, but a close working relationship with your service provider is necessary to obtain your security goals.
    a. ISP B
    b. ISP A
    c. PSTN
    d. Frame/ATM



Cisco Safe: Enterprise SAFE Block Diagram

SAFE describes various targets inside the enterprise network and the basic precautions that should be implemented to protect them. These targets include routers, switches, hosts, and the network as a whole.

Routers move network traffic from network to network. Routers advertise networks, filter traffic and provide access. Securing your routers should be a very high priority. Some of the things you can do include:

a. Lock down telnet access.
b. Lock down SNMP access.
c. Turn off unused services.
d. Authenticate routing updates.
e. Log what is appropriate.

Switches provide us a fast, flexible, scaleable and cost effective way to expand your network, but not without risk. A few things you can do to secure a switch include:

a. Disable all unused ports.
b. Turn on port security.
c. Turn off trunking on ports that don't need it.
d. Make sure trunk ports have a unique VLAN number.

Note: As with any critical device such as routers and switches providing good physical security is a must.

Hosts come in all different shapes and sizes, different hardware

platforms, operating systems and are used by individuals of varying degrees of expertise. That's why hosts are hacker's favorite targets and the most successfully compromised. To secure host you must keep up with the latest updates, patches, firmware and bug fixes. This can be an overwhelming task in its self, especially for an already task saturated IT staff.

Networks can come under attack in the form of distributed denial of service (DDoS), such as ICMP floods, TCP SYN floods, and UDP floods. This type of an attack is when numerous machines flood an IP address (i.e. your router) with bogus data, essentially making your network unreachable by legitimate users or customers. To thwart such an attack you must have the cooperation with your ISP as mentioned before. Your ISP can limit the rate of the data outbound to your site.

The DDoS attacks that made headlines recently, where using vulnerable systems in corporations, university and libraries to launch attacks against the big boys eBay and Amazon (Hale), making those businesses unreachable.

Your ISP should also be defending against IP Source Address Spoofing, which is outlined in RFC 2827 (Ferguson). IP Spoofing is where an attacker attempts to conceal the location of where the attack originated. By changing the source IP address to a private IP address or to that of a legitimate public IP address. Internal address defined in RFC 1918 should never be used on a public network; as such your ISP should be able to use filtering rules to block these easily. If the attacker changes the IP to a legitimate network address any filtering you do to block that address may also block legitimate users and customers on that network from reaching your network, making them victims as well. For more information please refer to the RFC documents mentioned above.

Defending against Viruses, Trojans and Worms is a battle usually waged at the server and workstation level. With the onslaught of the Code Red Worm not only where Cisco services that rely on Microsoft IIS web server affected, but side-effects caused by the worm can expose unrelated problems on other products.

When the traffic from the worm reaches a significant level, a Cisco CSS 11000 series Content Service Switch may suffer a memory allocation error that leads to memory corruption and will require a reboot. As a separate side effect, the URI used by the worm to infect other hosts causes Cisco 600 series DSL routers to stop forwarding

traffic. An affected 600 series router that has been scanned by the "Code
Red" worm may not resume normal service until the power has been cycled (Cisco Security Advisory).

The **Enterprise Campus** has two major threats, internal and external users. While most companies defend heavily against the external threat, few steps are taken to defend against the internal threat. Fact is that most threats to an Enterprise network come from personnel on the inside. The inside threat can come from disgruntled, curious or careless employees, and through corporate espionage.

Management Module allows for secure management of all devices and hosts inside the enterprise SAFE architecture. The management module gathers logging and reporting information, while pushing content, configurations and updates out to the network. Management module consists of various elements: SNMP management host, NIDS host (Network Intrusion Detection System), NIDS appliance for layer 4-7 monitoring, Syslog servers, Cisco IOS firewalls, Layer 2 switches with VLAN support. Since the management module has access to all devices on the network, allowing an attacker access here could be disastrous.

The management module is broken into two network segments each on their own subnet, separated by an IOS router acting as a firewall. These two subnets are separated from the production network, to ensure they are not advertised in routing updates. The network segment outside the firewall consists of host and devices that require management and the segment inside the firewall consist of the management devices. For the inside segment the firewall is configured to allow only the traffic needed, syslog information, telnet, SSH and SNMP and only if it was first initiated on the inside. IDS systems flagging any other traffic require an immediate response.

SNMP will be kept on its own isolated management segment when pulling data from devices. SNMP on devices on the production network are set “read only” and are not allowed to push data to the management module.

Syslog information is crucial to network security. Log just data needed to secure the network. Don’t log more information than you can effectively analyze.

Out-of-band management is where your management data does not traverse the same segments as the production environment. Out-of-band

management is preferred, but not always possible. Where in-band management is needed use secure encrypted transports such as SSH, SSL etc. Out-of-Band management of network resource can be a tricky task. If you use the network to reach your devices, switches, routers, etc. and the network fails for whatever reason, so has your ability to manage. Through the use of console servers and the trusted serial dial-in connection we can maintain out-of-band management at a very low cost. Console server is made up of many serial ports, an Ethernet connection, and software to support many applications. This allows you to connect many devices (switches, routers) directly to the console server, giving you a central point from which you can remotely manage all the devices, either thru Ethernet or serial connection (Prowten).

Core module is responsible for routing and switching data as fast as possible from the building distribution module to the edge module. Follow the guidelines on securing your routers and switches stated previously. There are no SAFE implementations needed for this module.

Building Distribution Module provides services to the switches located in the building module. Services provided include routing, quality of services and access control. Through the use of VLAN's and good access controls in this module we can effectively block access between various departments, stopping the majority of the inside threats.

Building Module is where your end-users, their computers, IP phones and the layer-2 devices they access can be found. At this module is where host based virus and trojan scanning software will be implemented. With no layer-3 devices in this module to provide access control, this seems like a good place for personal firewall software to help mitigate the insider threat even farther. While personal firewall software was not mentioned in the SAFE documentation, it seems like a logical step.

Server Module is the primary target for the insider threat. This module contains the bulk of your business data, you can ill-afford mistakes here. Limiting user access and setting good password policies for your administrators is not enough. To protect your servers you need to bring in many of the tools we've discussed before: host and network IDS, access controls, VLAN, virus and trojan protection, up-to-date software and patches.

Edge Distribution Module provides connectivity of all the Enterprise Edge Modules. All the Edge Modules send their data to the Edge Distribution Module for layer-3 filtering and routing to the Core

Module. Edge Distribution Module is the last line of defense before data reaches the Enterprise Campus. If you elect to use layer-3 switches in this module you can increase security by using IDS line cards inside the layer-3 switch, (Cisco Systems).

Enterprise Edge Module contains four modules: Corporate Internet Module, VPN Module, WAN Module and E-Commerce Module. As stated before I will only be covering the Corporate Internet Module.

Corporate Internet Module provides connection to Internet services and provides access to public corporate servers for users on the Internet. While the data that is kept on this module is probably not mission critical, it usually makes the news headlines when compromised, i.e. defaced web sites etc. This can bring on a lack of confidence about the company as a whole.

We use two firewalls in this module, one to protect resources from external attacks and one to defend against the internal threat. Using stateful inspection to insure only legitimate traffic crosses the firewall. We also set our edge routers according to RFC 1918 and 2827, to crosscheck our ISP's settings. SAFE suggest having the NIDS appliance on the public side of the firewall monitoring for layer 4-7 based attacks. Since our routers and ISP routers are doing a lot of access control and filtering we need the NIDS systems looking for the more cleaver of attacks.

Outside attackers are going to pound on this module. For the most part the attackers rely on our laziness or careless oversights to compromise these systems. The importance of up to date software and security patches for your web, ftp and dns servers cannot be emphasized enough.

This concludes the overview of Cisco SAFE. For an in depth look into the SAFE architecture please refer to the SAFE documentation (Convery) and the many references to supporting documentation provided.

Works Cited

Cisco Security Advisory. "Code Red" Worm - Customer Impact. Aug 11, 2001. http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml

Cisco Systems Inc. "Intrusion Detection Product Update". Dec 2000. http://www.cisco.com/networkers/nw00/pres/2505.pdf

Convery, Sean and Bernie Trudel. "Cisco SAFE": A Security Blueprint for Enterprise Networks. Internet. Monday June 25, 2001. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

Hale, Ron. "Many roads to Intrusion Detection". Cisco World Magazine. June 2001: 20.

Prowten, Mark. "Out-of-Band Management". Everything Old Is New Again. December 2000. http://www.ciscoworldmagazine.com/monthly/2000/12/outofband.shtml

Ferguson, Paul. "Request for Comments: 2827". Network Ingress Filtering: Defeating Denial of Service Attacks, which employ IP Source Address Spoofing. Internet. May 2000. http://rfc.net/rfc2827.html

Rekhter, Yakov, et al. "Request for Comments: 1918". Address Allocation for Private Internets. Internet. February 1996. http://rfc.net/rfc1918.html