Self - Defending Networks

Powered by CISCO

Vidhul Prasad , 41, 19132453

SEMINAR CONTENTS

- INTRODUCTION
- CATEGORIES OF SELF DEFENDING NETWORKS
- ARCHITECTURE OF NETWORK ADMISSION
- CONTROL (NAC) WAYS TO PREVENT ATTACKS IN NETWORK
- ADVANTAGES & DISADVANTAGES
- APPLICATIONS
- CONCLUSION

Introduction

- The Next Generation of Network Security helps networking professionals understand how to deploy an **end-to-end**, **integrated** network security solution.
- This security primer provides **unique insight** into the entire range of Cisco security solutions, showing what each element is capable of doing and how all of the **pieces work together** to form an **end-to-end Self-Defending Network**.

CATEGORIES OF SELF DEFENDING NETWORKS

- **Router**

A router is a **specialized networking device** connected to two or more networks running software that allows the router to move data from one network to another.

The Integrated Services Router

IS Routers provide security functionality that can be listed under four categories, namely:

- Trust and Identity
- Network Infrastructure Protection
- Secure Connectivity
- Threat Defense

Trust and Identity

This category aims to give the network the ability to control access at the endpoint, thus providing protection from end systems that connect to the network infrastructure.

1. Network Admission Control (NAC)
2. Authentication, Authorization and Accounting (AAA)
3. Network Infrastructure Protection
4. Control Plane Policing
5. Network-Based Application Recognition (NBAR)
6. Autosecure

Secure Connectivity

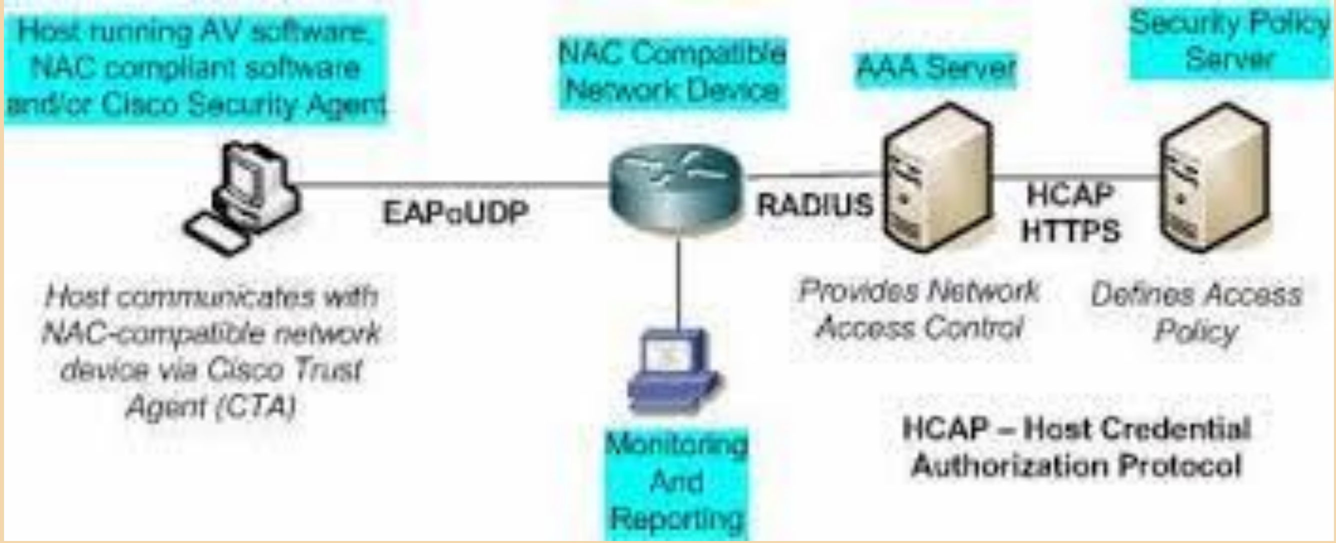
- It should be possible for the network to pass data in a manner that renders it secure. However, the methods used to secure data on the network should also be scalable. The Secure Connectivity category provides mechanisms to achieve this.

1. **Virtual Private Network (VPN) Encryption and Tunneling**
2. **Dynamic Multipoint VPN (DMVPN)**
3. **Voice and Video Enabled IPSec (V3PN)**
4. **Multi-Protocol Label Switching (MPLS) & IPSec Integration**
5. **Identity-Based Network Services - IEEE 802.1x**

ARCHITECTURE OF NETWORK ADMISSION CONTROL (NAC)

- NAC is an industry wide initiative, sponsored by Cisco, which enables the network to interrogate end-systems for compliance with a security policy.
- It is designed to control initial network access, either by allowing, blocking or quarantining end systems.

Obviously, such functionality requires more than just intelligent network elements. For this reason, NAC is a multi-vendor collaboration, involving representations from network, anti-virus, OS management and specialized security vendors.


Host running AV software, NAC compliant software and/or Cisco Security Agent
NAC Compatible Network Device
AAA Server
Security Policy Server
EAPoUDP
RADIUS
HCAP HTTPS
Host communicates with NAC-compatible network device via Cisco Trust Agent (CTA)
Provides Network Access Control
Defines Access Policy
Monitoring And Reporting
HCAP – Host Credential Authorization Protocol

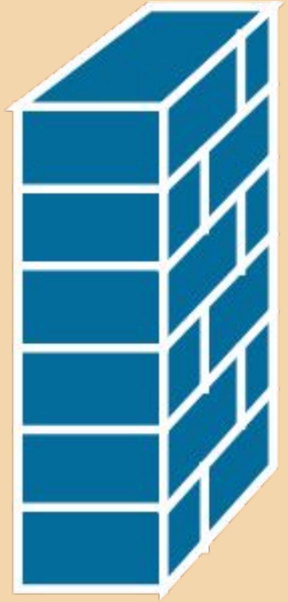
- The initial phases of NAC are supported on Cisco routers, giving access control at the IP level. The CTA on the end system communicates with the NAC router using Extensible Authentication Protocol over User Datagram Protocol (EAPOUDP).
- This requires authentication at layer 2 of the OSI model. EAPOUDP operates at layer 3 so, for future phases of NAC, an additional technology will be used for switches, APs, etc; IEEE802.1x with EAP.

WAYS TO PREVENT ATTACKS IN NETWORK

Threat Defense

This category provides ways in which the network can prevent and respond to attacks.

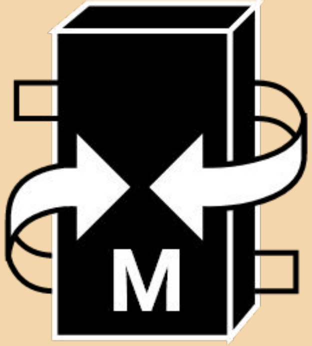
- IOS Firewall
- Transparent Firewall
- Intrusion Prevention



ADVANTAGES

- The Self-Defending Network provides the capability to map IPSec sessions into MPLS VPNs.
- Autosecure
- Secure Connectivity

DISADVANTAGES



- If any router fails then any hacker can access the network and send unnecessary packets thus creating congestion in the network.

APPLICATIONS

- **FIPS**

FIPS are standards developed by the National Institute of Standards and Technology (NIST) for use in United States federal computer system.

- **ICSA**

IOS Firewall has attained ICSA Certified Firewall status against version 4.1 of its certification criteria k. ICSO certification is aimed at the commercial sector, allowing prospective clients to identify products that have been independently certified. against industry-accepted standards

CONCLUSIONS

- As attacks become more sophisticated and attack vectors become more diverse, it is clear that IT infrastructures must be in a position to defend and react against these more effectively.
- This applies to both the enterprise and service provider environments. Cisco views the network as a core element in infrastructure security and has articulated this philosophy through their Self-Defending Network strategy

CONCLUSION

- True network security intelligence will be a network that can automatically gather information on known attacks from various sources, monitor the data that it carries (on an infrastructure scale, not per element), analyze that traffic for known and also potential attacks (using anomaly detections), reconfigure itself to control the attack and report what is happening.

- This will be a true, **Self-Defending Network**.

THaNK YoU