WHITE PAPER

NETWORK SECURITY OVERVIEW AND SOLUTIONS

Ricardo Villa
BCN Director of IT & Managed Services

THE CASE FOR NETWORK SECURITY

In any type of network services deployment, a thorough review and understanding of potential threats and a resulting plan for Network Security is not only essential, but critical. Every organization, from enterprise-level businesses with large user groups, to SMBs with smaller user groups, face the same challenge of securing their IT network and connected end-point devices. Regularly we learn of network breaches perpetrated by individuals and organizations intent on attacking and penetrating a company's network and devices with the goal of taking control of and harming those networks and devices. The impact of a security breach can range from inconvenient to catastrophic.

Attacks can range from the defacing of company web sites to the installation of ransomware. Often, seemingly random attacks, aim to bring down a network and cripple a business. Regardless of the type of attack, or the underlying intent, once end-point devices (computers and other connected hardware) in a network are compromised, those devices can be used to launch attacks against other networks further exposing the business to liability.

KEY SECURITY POINTS IN ANY NETWORK

Network Security is divided within two key security points within any IT network. The first security point is **"Perimeter"** security. The second security point is **"Internal Network and Device"** security.

Perimeter Security is the point at which the internal network meets the Internet.

All Perimeter Security connection points need to be secured and monitored to guard against direct attacks via the Internet which can be launched towards the device at the edge of the network.

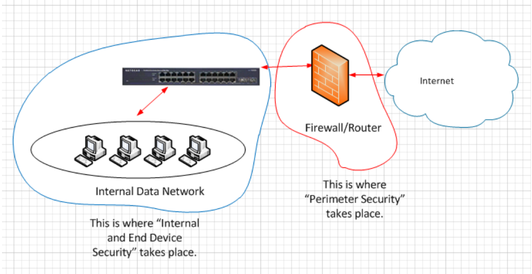
WHITE PAPER

NETWORK SECURITY OVERVIEW AND SOLUTIONS

Ricardo Villa
BCN Director of IT & Managed Services

Internal Network and End Device Security pertains to individual computers and equipment that lie inside the internal network in the form of hardware, servers and software.

Anti-Virus software and Operating System patches/fixes are examples of Internal Network and End Device security.


Internet
Firewall/Router
Internal Data Network
This is where "Perimeter Security" takes place.
This is where "Internal and End Device Security" takes place.

BCN SOLUTIONS FOR PERIMETER SECURITY

The BCN portfolio includes a full line of products and services that address the security of the Perimeter Network. These solutions include BCN provided physical hardware and add-on license software to address the many needs of Perimeter Security protection.

Managed Firewall Equipment

In the hardware space, BCN offers **Managed Firewall Equipment**. Customers should consider a Firewall as the minimum Perimeter Security Protection requirement. Firewalls are simple but effective devices that "inspect" and "police" all inbound and outbound traffic. The administrator creates rules that allow/deny traffic into and out of the organization. Whether the rules are simple or highly complex they require careful planning.

A Perimeter Security solution cannot be achieved by a Firewall alone. Proper configuration, monitoring and maintenance of a Firewall is necessary to ensure a customer's network is adequately protected. A BCN Managed Firewall does just that. The fully managed solution supports those customers who may not be staffed with skilled personnel or simply do not want to assume the burden of managing and monitoring their Firewall equipment. BCN's ability to centralize the monitoring and maintenance of these devices, whether at one location or multiple locations provides the customer with a single point of contact for design, deployment and support.

When a fully Managed Firewall device is enhanced with available software license add-ons that further target aspects of Perimeter Security, it becomes a fully functional Security Appliance. BCN offers software license add-ons address that address two main areas of security including Threat Management and Web Filtering

Advanced Security Services

The software license add-ons available from BCN add both **Intrusion Detection and Prevention (IDP)** and **Internet Security/Web Filtering** to a **Perimeter Security** solution.

Threat Management: **Intrusion Detection & Prevention (IDP)**

An IDP Signature Database is the foundation of an Intrusion Detection and Prevention (IDP) solution. The database contains definitions of different objects—such as attack objects, application signatures objects, and service objects—that are used in defining IDP policy rules. In essence the database catalogs previously pre-configured and pre-determined attack patterns known as signatures. Updated on a regular basis, an IDP signature database monitors packets in the Network and compares them with these pre-configured and pre-determined attack signatures enabling the Firewall to block the packets.

Web Filtering / Internet Security

At the core of Web Filtering security is the availability of URL Databases; the foundation for both comprehensive web filtering and policy management. These databases contain a continuously updated and comprehensive classification of URLs into category sets. Classification of URL categories help ensure real-time protection against today's targeted and advanced threats.
These categories can include areas such as Gambling, Travel, Social Media, and more.

A BCN solution allows a customer to restrict access to a pre-determined category of web sites. Furthermore, it can protect the organization from known sites that host viruses that can be downloaded by end users. For example, if a user inadvertently clicks on a hyperlink in an email that is designed to take them to the “virus mothership”, the technology within the solution will block the request.

BCN PERIMETER SECURITY SOLUTIONS

Entry Level Firewall Equipment / Cradlepoint

Cradlepoint Firewalls
Model/Description

CP-AER1650
250 Mbps Firewall with 4 LAN Ports and 1 WAN Port

CP-AER 1600
250 Mbps Firewall with Wi-Fi, 4 LAN Ports and 1 WAN Port

Mid-range Firewall Equipment / Cisco-Meraki

Cisco Firewalls
Model/Description

Meraki MX65
250 Mbps Firewall with 10 LAN Ports and 2 WAN Ports

Meraki MX65W
250 Mbps Firewall with Wi-Fi, 10 LAN Ports and 2 WAN Ports

Meraki MX84
500 Mbps Firewall with 8 LAN Ports and 2 WAN Ports

Software License Add-ons for Cradlepoint Firewall Equipment:

Enhanced Cradlepoint Services

- **Cradlepoint Threat Management**
  A comprehensive IPS (intrusion protection system) and IDS (intrusion detection system). Only available on Cradlepoint AER Series

- **Cradlepoint Zscaler™ Internet Security**
  Intelligent and scalable Web Filtering Service. Only available on Cradlepoint AER Series.

Software license add-ons for the Meraki Firewall Equipment:

Cisco Meraki
Advanced Security Services

Advanced Security License includes content filtering, intrusion prevention, anti-virus, and anti-phishing.

- **MX65 Advanced Security License**
- **MX65W Advanced Security License**
- **MX84 Advanced Security License**

CONNECT IT. MANAGE IT. MONITOR IT. SECURE IT.

The combination of Perimeter and Internal Network and Device Security allows any business to operate with critical protection against a wide variety of attempted network breaches.

The BCN portfolio which contains 75+ carrier networks for access is just the beginning. Securing that access at the Perimeter can and should be a vital component of any BCN solution. The management and monitoring available in BCN's Managed Firewall offerings, coupled with the perimeter protection available through advanced, add-on security licenses delivers customer's a solution that fits today's business requirements.