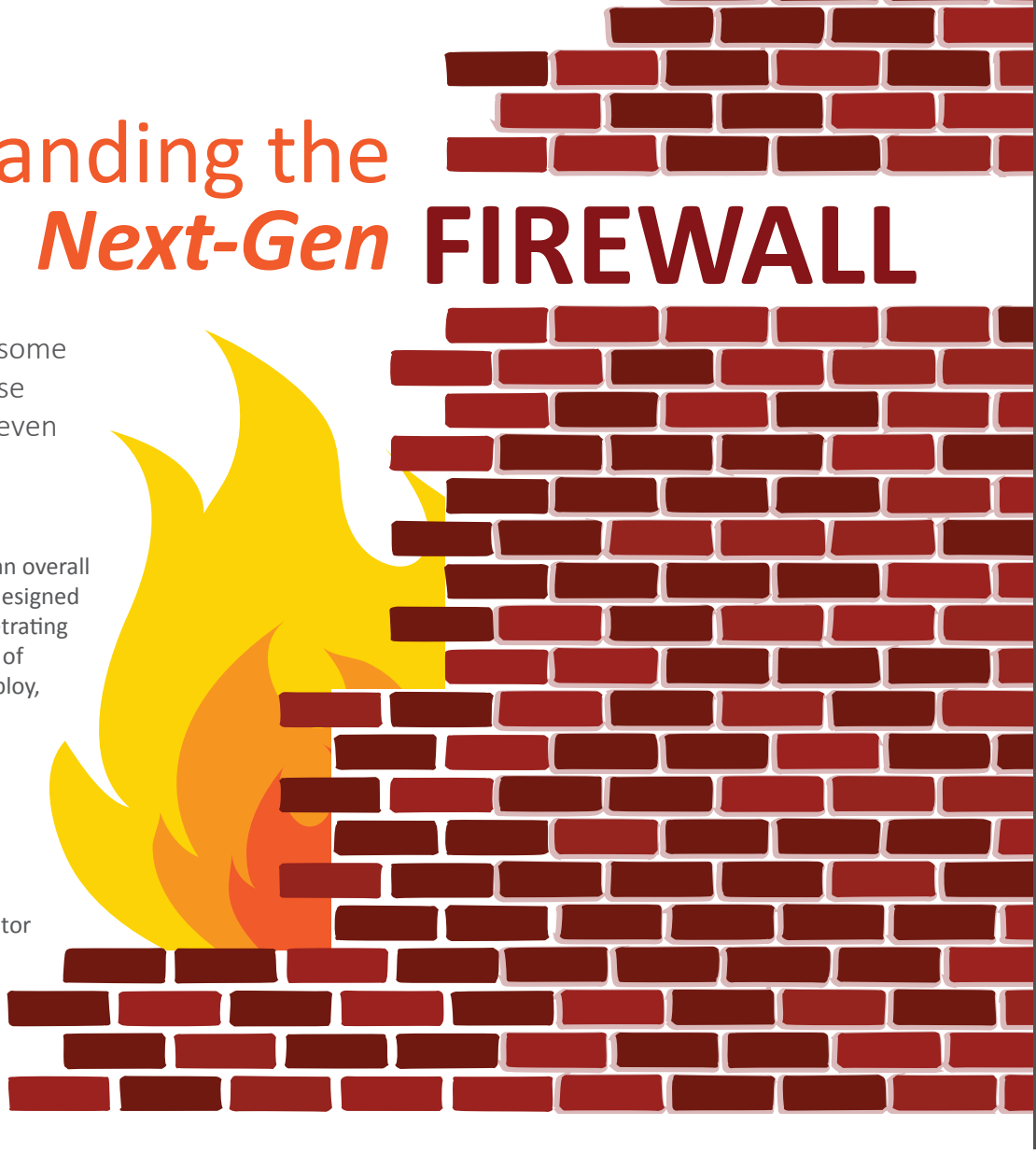
Understanding the *Next-Gen* FIREWALL



A majority of companies have some sort of firewall. Many feel a false sense of protection and don't even know the potential risks of insufficient armor.

As the first required building block for an overall network security posture, a firewall is designed to block unauthorized traffic from penetrating the network. In addition to a vast array of security policies a company should employ, maintaining a firewall can stretch far beyond a full-time job and ties up a lot of IT resources.

Having a firewall alone is not enough. A firewall does not prevent viruses or malware from entering the network, it cannot detect intruders nor can it monitor network traffic. Next-Gen Firewalls are the evolution of the enterprise firewall coupled with a number of network devices filtering and security features to protect customers.

Verizon's DBIR reports more than
2,100 data breaches
in 2014 alone.

It is estimated that it takes most companies more than
200 days
to detect a data breach.

With so many cyber security risks it makes sense to invest in a managed firewall solution.

Traditional firewalls include:

- Packet Filtering
- Network Address Translation
- URL Blocking
- Virtual Private Networks (VPN)

A managed firewall solution takes on management, maintenance and reporting. It includes:

The Device	A centralized virtual or physical appliance (usually an enterprise-grade Palo Alto or Fortinet device) now part of a monthly contract moving it from CapEx to OpEx. As needs grow and a larger device is required, scale the solution without having to purchase a new device.
Firewall Maintenance	Updates, patch management, change management and other maintenance is handled 24x7x365 by the vendor. This service will occur within an agreed upon SLA to ensure needs are met in an acceptable timeframe.
Portal	Continuous visibility into perimeter security for monitoring, logging and reporting, all done through a cloud-based portal. View data and analytics, assess trends, utilize logs for audits and compliance requirements.

Managed Firewall Add-Ons

With a next-gen firewall, additional features are layered on with QoS, no additional devices needed. Additions can include:

Intrusion Detection System (IDS)
IDS identifies malicious traffic targeting the network and provides alerts. Activity is logged to provide an audit trail available for review in a portal.

Intrusion Prevention System (IPS)
IPS works in conjunction with IDS to block malicious traffic and quarantine suspicious traffic. Parameters can be set through the cloud-based portal.

Antivirus
Antivirus software/applications protects inbound and outbound traffic against viruses, worms, trojans and other malware. Protection is at the edge of the network and in real time. Threats are logged in the same SIEM portal.

Content Filtering/URL Filtering
Often the last piece of the security puzzle, content filtering protects your internal network. This web filtering blocks access to web sites outside of a company's Internet "Acceptable Use Policy", ranging from social media sites and YouTube to gambling and drugs.

Deep Packet Inspection (DPI)
DPI grabs pieces of each packet to thoroughly inspect and identify anomalies or violations of normal protocol/communications.

Application Awareness
Log and track application use throughout the network to create a baseline and use these parameters to set policy around which users can access what.

Active Directory/LDAP Integration
This integration allows a higher level of content/URL filtering based on the user's roles within Active Directory.

*Reasons to Switch to **Next-Gen/Managed Firewall***

- Current Firewall EOL
- Upgrading Firewall
- Device Consolidation
- Realign IT Staff to More Strategic Projects
- More Active Management of Solution

Fee Structure:
Managed Firewall vs. Traditional Firewall

24x7x365 management and monitoring of the company's network is resource intense and time consuming.

	Managed Firewall	DIY Security Monitoring
HARDWARE	Included	CapEx
STAFF – MAINTENANCE	Included	$80K-$150K/employee
STAFF – MONITORING	Included	$80K-$150K/employee
STAFF – INSTALLS	Included	$80K-$150K/employee plus T&E for site visits
TRAINING	Included	Cost of certifications and continued education
AVAILABILITY	24x7x365	8 hour days, 5 days/week
THREAT INTELLIGENCE	Included	Subscription based
TOTAL COST	**Beginning at $5,000/month**	**Cost of hardware, software, subscriptions and personnel**

Points to Consider

When considering a new or upgraded solution, assess your entire security policy, upcoming needs and how you plan to evolve their security posture in our ever changing, high threat environment.

Do you have a security policy?

What does it include?

- Acceptable use policy?
- Password policy?
- Data protection policy?
- Data destruction policy?
- Security reporting procedure?
- Are you compliant with any additional regulatory and compliance standards?

Do you employ any security staff currently?

- How many employees do you have?
- Are your employees trained on the security measures in place for them?

What are your security challenges?

What cloud-based “as-a-service” resources do you consume?

Do you run audits on your security?

- Do your auditors rotate or do you always use the same auditors?
- When was your last audit?
- When was the last time you completed a security assessment?
- Where are your biggest security risks within your network?

Do you have an incident response plan?

Do you have a disaster recovery or business continuity plan?

Vendors to Explore

airespring™ Cloud, Fully Managed and Connected

AT&T Solution Provider

CenturyLink Channel Alliance DIAMOND PARTNER

FORSYTHE®

hypercore networks

MASERGY PLATINUM PARTNER

MegaPath™

MetTel®

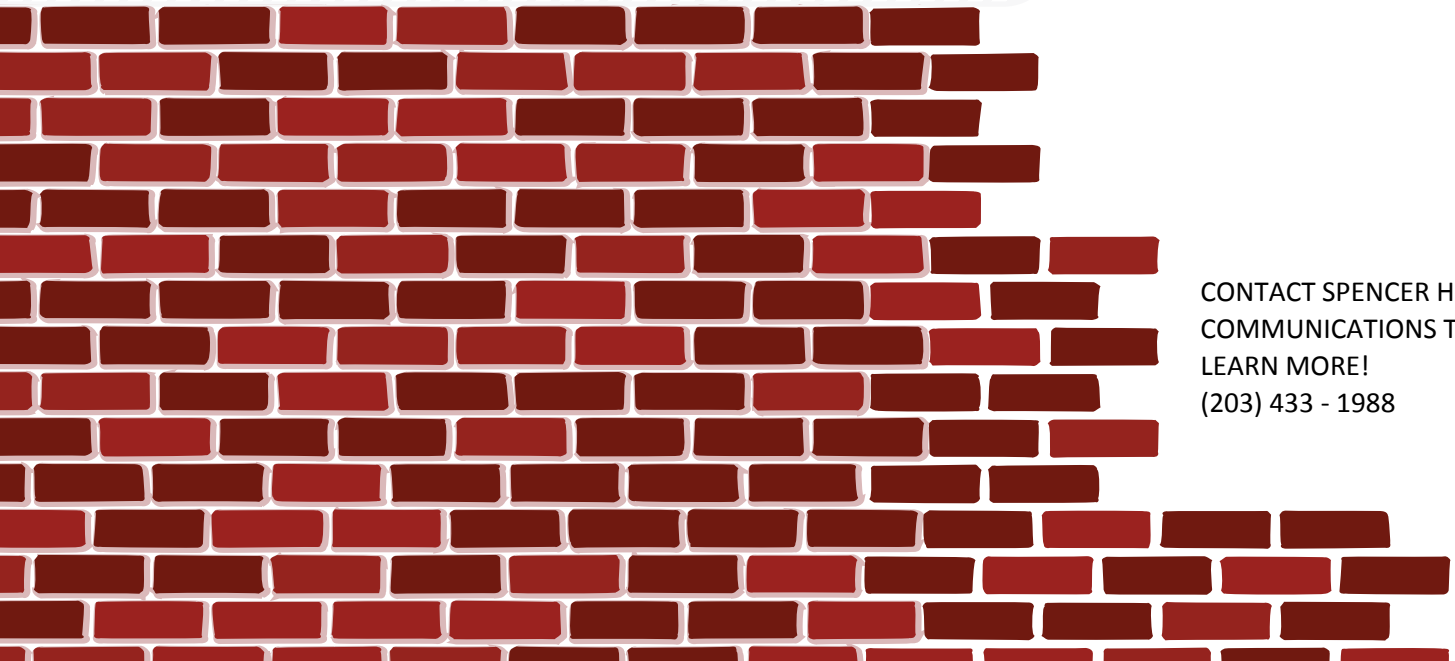
TATA

TELSTRA

TPX COMMUNICATIONS

windstream® Platinum Channel Partner

verizon partner program - platinum



CONTACT SPENCER HILL COMMUNICATIONS TODAY TO LEARN MORE!
(203) 433 - 1988