Next Generation UTMs
for SOHO SMB – Wire-Speed Security
Contents

Summary 1
Introduction 2
Gigabit Internet Speeds 3
Generic Threats Fill the Fat Pipe 4
BYOD – Device Density 4
  - Multiple OS – Multiplying Vulnerabilities
The Rise of Apps 5
  - The Rise of Application Threats
Shift in Security Fundamentals 5
  - Gigabit Security for Gigabit Networks 6
  - Deep Inspection – Converging on HTTP/HTTPS 6
  - Multiple Intelligence 6
Conclusion – Next Generation UTM is the Future 7
Gigabit Security for SOHO-SMBs – Cyberoam Next Generation UTM Appliances 7
Summary

Affordable gigabit Internet speeds and cloud-based solutions are driving SOHO-SMBs to adopt a wide range of IT solutions for the first time to streamline and enhance their business. Living under a changed life style regime, employees are bringing multiple devices, including laptops, tablets and smart phones to work, expecting anywhere, anytime, any device access for work and personal uses. At the same time, business and personal applications are proliferating, often without security credentials.

These factors are contributing to a rise in the volume of threats to SOHO-SMB networks in addition to exposing the latter to fresh vulnerabilities. Security devices must carry next generation gigabit-capability with deep inspection and multiple intelligence, involving application-user-device identity, content and context-aware intelligence to meet the security challenges of SOHO-SMBs.
Introduction

A look at the brief but intense history of Internet security reveals the fact that it has been a war of us vs them – us being organizations’ networks and users; them being the threats that target users and networks.

As the pattern of network and Internet usage underwent incremental changes, it invariably challenged the network security in organizations, pushing it to shift and adapt to these changes. However, today the pattern is undergoing a tremendous shift that is nothing short of a life style change, demanding a transformation in security capability.

At the root of this shift is the gigabit-speed Internet that is reaching users, driving them to change how they access the Internet and what they do with the Internet. Users are bringing multiple devices and a variety of always-on applications into organizations. This shift is taking networks from the equivalent of the early-nineteenth century to the mid-twenty first century.

For the first time, gigabit Internet speeds are bringing a wide range of solutions within reach of SOHO-SMB organizations. Simultaneously, they are placing enormous pressure on security devices. The question that arises is, what does it take for security devices to keep pace with the shift?
Gigabit Internet Speeds

The gigabit broadband pipe that is acting as a catalyst to the change is the equivalent of massive expressways to the doorstep. Data is set to move at 100 times the current Internet speed. Google Fiber which brings Fiber-to-the-Home (FTTH) is offering 1000 MBPS upload and download speeds at affordable rates. With existing average speeds languishing anywhere between 1 and 6 MBPS, this is a steep jump.

The UK Government is mulling a law that guarantees the legal right for all householders to high speed broadband, placing it at par with guaranteed utilities like water and gas. The Government aims to focus on providing speeds of 40 MBPS or more by 2017. In India, Bharat Sanchar Nigam Limited (BSNL), the country’s state service provider is to provide FTTH with 100 MBPS speed.

With high-speed Internet reaching homes themselves, it no longer remains the privilege of enterprises. The massive speed that these enormous data pipes generate allows SOHO-SMBs to adopt solutions for the first time that had once been the preserve of enterprises, enabling the former to systematize business processes, expand opportunities and help them meet the requirements of large buyers.

Business Use: The fact that high-speed Internet has transformed yesterday’s SMBs into today’s enterprises and yesterday’s SOHOs into today’s SMBs has driven solution providers to provide SOHO-SMB solutions that are geared to meet the specific needs of individual industries. These range from healthcare, oil and gas, to sub-segments of industries such as chemicals, electronics, logistics and more.

From solutions that systematize business processes like BPM, ERP, CRM, SCM and monitoring solutions like dashboards, reporting and analytics to productivity solutions like Adobe Acrobat and Google Drive, many are finding place in SOHO-SMB organizations. A wide range of SOHO-SMBs, from catering companies to children’s charities, Internet marketing technology firms and school districts to manufacturing firms are turning to these solutions and applications extensively.

Personal Use: Employees’ personal use of high speed Internet is a matter of concern for organizations since users have begun to perform business and personal work over the same devices, placing corporate data and networks at risk. From entertainment to news updates to presence on social media platforms like Facebook and Twitter, users’ personal activity in the virtual world is meshing with their business activity.
Generic Threats Fill the Fat Pipe

At the most basic level, there exists a direct equation between high-speed broadband which leads to growth in Internet and the rise in security incidents. The higher the traffic, the higher the volume of threats. Generic threats in the form of probes, scans, account and root compromise, packet sniffers, exploitation of trust, malicious code, phishing, viruses, worms, Trojans and a host of other attacks are growing rapidly with the growth in traffic volume. They are entering the network through susceptible applications and devices, compromising data and resources.

But there is more to it than just a straightforward rise in threats. It becomes necessary to take a look at what organizations and employees do with the gigabit speeds at their disposal.

Whereas earlier, business solutions were available as server and client installations within the network or were being accessed over the browser as Salesforce was, today, many are available as cloud services accessed through applications over mobile devices. These cloud-based solutions along with the organization’s data backup in the cloud are facilitating anywhere access to organizational data and systems which users are accessing through multiple devices which have emerged as an employee expectation.

BYOD – Device Density

Organizations are adopting a BYOD (Bring Your Own Device) policy or in technical parlance, the “Consumerization of IT” has come to stay. The aim is to offer employees the flexibility to access their work anytime, anywhere, from any device, enhancing productivity and responsiveness.

Employees are bringing in devices, otherwise used to access personal data – laptops, tablets and smart phones, to the work place, accessing the Internet, systems and data through each of these devices. Using these mobile devices which are fraught with risks in the absence of adequate security mechanisms, employees are accessing a range of the organization’s systems and resources in the course of their work, leaving corporate networks highly vulnerable.

However, contradictory to the earlier network dynamics where a single user brought in one device to the network, today, on an average, an employee brings in anywhere from 2-5 devices to the organization, leading to higher device density and too much load on the network. The network traffic now encompasses traffic from multiple devices of a single user from within the network perimeter or outside, accessing data stored within the network or in the cloud, multiplying network security complexities by many times.

Multiple OS – Multiplying Vulnerabilities

While organizations implement a BYOD policy for safe device usage, the devices themselves are based on the individual’s choice leading to different laptops, tablets and smart phones introducing multiple operating systems into organizational networks. From a scenario of a single operating system, today, security solutions face the complex scenario where they oversee between 2-5 operating systems across multiple devices. And the vulnerabilities of each operating system cumulate on the network as threats. The attack surface is expanded considerably with attacks looking at exploiting any vulnerability present within the OS, applications, and even the people using these devices.
The Rise of Apps

The many business solutions being adopted by SOHO-SMBs are today accessible through apps on their mobile devices. With cloud-based apps, the office is wherever the employee is, facilitating telecommuters and road warriors and increasing employee productivity. Executives can monitor functions within the organization and the network, helping them stay organized and efficient, enabling quick inspection and customer response.

The presence of the same app on different devices which executives use interchangeably, depending on whether they are in the office, on the road, or with client raises the need to keep the session alive and to synchronize the status with the cloud and the other devices. All this traffic is taking its toll on the network and security.

Further, these apps work on the web protocols, HTTP, HTTPS and are always on, keeping executives updated on a continuous basis. So the port-protocol thumb rules of olden times become irrelevant in meeting current security needs.

The Rise of Application Threats

Whereas earlier, the vectors of attack were floppies, pen drive or emails, today, applications have become an important vector. The rise in personal and business applications on devices has led to a rise in application threats. About 80-96% of web applications contain high risk vulnerabilities detected during detailed manual and automated assessment by white box method, according to the Web Application Security Consortium. While malicious applications whose sole objective is to gain access to data or to perpetrate other threats gain attention, genuine business and personal applications are of critical security concern too. Many of them carry security lacunae, leaving devices vulnerable to new forms of application threats. Business and personal applications co-exist on the same devices, exposing organizations to higher levels of risk.

Threats can easily trick an application into doing what they are not supposed to do, gaining access to devices and data stored on the device, including user credentials to a range of personal and business applications. Further, given the always-on nature of devices and constant access to the network, it is with little delay that attackers gain access to the network and the cloud through compromised data.

The fact that these apps travel through the HTTP, HTTPS protocols makes it practically impossible to detect them without deep packet inspection.

Shift in Security Fundamentals

The basic security need of the organization today is to prevent the gigabit network and cloud traffic generated by multiple devices and multiple applications from compromising network security. Cloud security might well offer multi-layered security, but the network and mobile devices themselves can become the weak link if network security devices are not geared to handle the high-volume, complex traffic.

Security devices geared towards generic traffic assessment and monitoring fail to understand, assess or meet the traffic and filtering requirements of this single-user, multiple-device, multiple-application traffic scenario. It is as if a single user with a lone car on the expressway has metamorphosed into a range of vehicles, some of them gigantic trucks rumbling at blazing fast speeds on the expressway.
Shift in Security Fundamentals

The ability to meet these challenging security requirements requires an urgent shift in security fundamentals. Three factors represent the shift and hold the key to effective SOHO-SMB security – gigabit speeds, deep inspection and multiple intelligence.

Gigabit Security for Gigabit Networks

Although the Internet traffic they are meant to filter travels at blazing fast speeds and the infrastructure itself, including switches and laptops carry gigabit ports, current security devices and next-generation firewalls meant for SOHO-SMBs still function with 10/100 ports.

When such security devices capable of filtering traffic along single digit broadband pipes attempt to filter traffic that runs at five to a hundred times the current MBPS, the effect is evident. It is the equivalent of trying to drive 12-lane traffic through a 2-lane check point along the expressway.

These inline security devices then become the bottleneck, queues form, packets begin to drop and productivity suffers. Given the choice of productivity vs security, it is productivity that gains the upper hand, security rules are bypassed or completely discarded and the organization is open to threats from the unfiltered traffic that begins to move through the network.

It becomes critical for the security device to carry gigabit capability to match the volume of traffic generated by multiple devices with no traffic slow down.

Deep Inspection – Converging on HTTP/HTTPS

Traditionally, port-based scanning and filtering simplified the task of security devices wherein they had to identify the application based on the port-protocol.

In contrast, today, with all applications tunneling through port 80 and port 443, the ubiquitous HTTP and HTTPS ports, or by port-hopping, the application architecture itself has undergone a sea change. The task of security devices has just become more complicated. Firstly, in addition to the surge in traffic volume, they need to perform deep inspection of traffic without the simplicity afforded by port identification.

The second level of complexity is that HTTPS protocol being an encrypted port designed for data security in transmission, it is also actively used to hide threats. Decryption to identify this traffic places a higher burden on the security device. Performing deep packet inspection in case of SSL-encrypted traffic is unavoidable in the interests of identifying and filtering malicious traffic arriving through compromised devices with malicious or compromised applications.

The third level of complexity is the fact that each app, for example, Facebook can potentially carry hundreds of apps related to photos, messenger, games, surveys and many more, requiring identification. Considering that organizations want selective access to these applications, the demand is for granular policy enforcement.

This takes the number of applications to be scanned, identified and filtered into the thousands – a task that requires application-awareness with context and content intelligence in addition to identity and device intelligence and can only be performed by a gigabit-port, next-generation unified threat management (UTM) device.

Multiple Intelligence

There is no question any longer that identity forms the foundation of intelligent security. Generic security no longer holds good. With multiple devices accessing the network, the question of identity becomes one of multiple intelligence.

Security performance was traditionally assessed and predicted based on the number of users within the network since a user equaled a device. Today, the user is no longer synonymous with the device. With the same user handling multiple devices with applications that are always on, multiple simultaneous streams of traffic are created.

Security devices that are capable of identifying the user and the device become necessary to secure the organization, its data and network. In addition to Layer 7 application security, Layer 8 human security becomes critical.

This scenario demands multiple intelligence comprising user, device and application identity in addition to context and content intelligence. Such intelligence holds the key to next generation security.
Conclusion – Next Generation UTM is the Future

With gigabit Internet speeds, multiple devices and multiplying applications expanding the current volume of threats and introducing a whole new range of threats to SOHO-SMBs, a quantum shift in security fundamentals has become critical.

The high speed networks of SOHO-SMBs require network security devices that function at gigabit speeds with deep packet inspection. These capabilities are necessary to prevent these in-line security appliances from becoming choke points rather than high-speed check points.

The critical fact is that generic security or single intelligence based on application or user is no longer enough to retain security as well as work flexibility. Only security devices with multiple intelligence can ensure high levels of secure flexibility at work.

Failure to incorporate these security fundamentals can lead to compromised data and networks, loss of trust and credibility in the industry, slowing down organizational growth.

Gigabit Security for SOHO-SMBs – Cyberoam Next Generation UTM Appliances

Cyberoam Next Generation UTM appliances bring enterprise-grade gigabit security to SOHO-SMB organizations for the first time, offering network and crypto acceleration through radical software enhancements that help these appliances get the best out of their state-of-the-art hardware.

The hardware comes with gigabit ports, gigahertz processor and high-memory gigabyte RAM along with gigabyte compact flash and hard disk drive which help the appliances deliver nano-second security processing for high speed networks.

Cyberoam next-generation UTM appliances provide wirespeed, intelligent security geared to meet the requirements of high-speed complex networks where the user-device-application ratio is expanding beyond measure. These appliances carry multiple intelligence with the capability of user and device identification, granular application identification, content and context-aware intelligence to perform the high-rigor security with deep inspection required in today’s flexible and highly complex work environments.

By providing such critical security, they enable SOHO-SMBs to leverage high-speed Internet and the numerous business applications to enhance productivity, gain customer trust and build expanding businesses.