Metaswitch Networks

THE BRAINS OF THE NEW GLOBAL NETWORK

SESSION BORDER CONTROLLERS

THE CRUX OF NETWORK SECURITY

JUNE 2015

Some industry pundits called 2014 the Year of the Hacker. Well, permit me to suggest that we ain't seen nothin' yet!

Imagine if what happened at Sony Pictures took place at a large, international network operator. The outcome would be devastating.

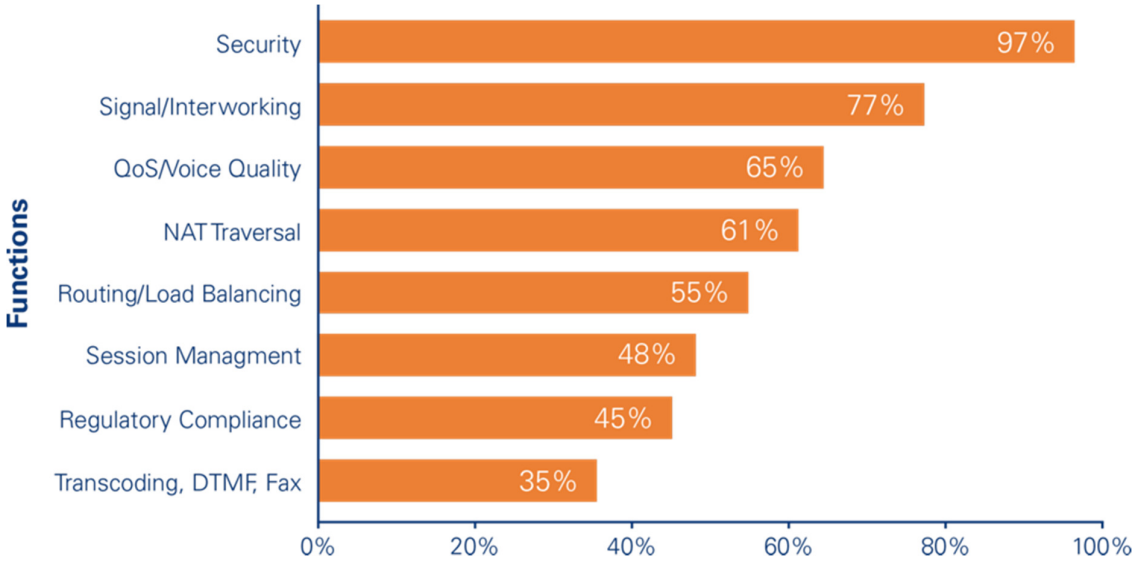
According to a February 2015 report by Gartner, "the Sony Pictures Entertainment (SPE) attack, with the subsequent media frenzy, is a game changer, representing how an aggressive cybersecurity business disruption attack can seriously impact business operations."

Gartner defines aggressive business disruption attacks as targeted attacks that reach deeply into internal digital business operations with the express purpose of widespread business damage. Servers may be taken down completely, data may be wiped and digital intellectual property may be released on the Internet by attackers. Victim organizations could be hounded by media inquiries for response and status, and government reaction and statements may increase the visibility and chaos of the attack. Employees may not be able to function normally in the workplace for months.

These attacks tend to expose embarrassing internal data via social media channels – and could have a longer media cycle than a breach of credit card or personal data. Even though we understand that, and despite the fact that security is the top concern for service providers deploying Voice over IP (VoIP), few service providers have implemented effective measures, and few are monitoring their networks for potential attacks.

As VoIP technology is becoming ubiquitous, so too are the security threats to its users and networks. The need to deploy a next-generation Session Border Controller (SBC) has never been more urgent, as the SBC can protect the VoIP network from attacks and protect the network operator's revenue stream.

According to an Infonetics survey, service providers consider security the number one function of the SBC:



While this need is not a new one, the security issues related to VoIP networks are now compounded by additional ones related to cloud environments and the adoption of NFV (Network Functions Virtualization) networks.

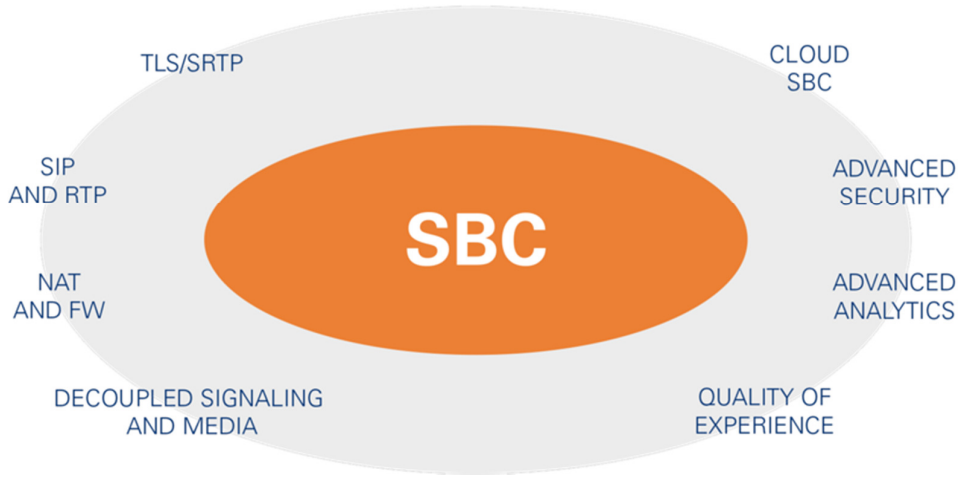
NFV environments introduce new security challenges, such as:

- Perimeter of the network is fluid, with VMs (Virtual Machines) scaling up and down depending on the need for that particular function.
- All VMs are addressable.
- Intra-tenant or multi-tenant traffic is subject to "fate-sharing."
- There is a longer chain of trust due to reliance on other software (hypervisors, orchestration, etc.).
- With SBCs being virtual functions themselves, the ability for a VM to support a DDoS flood decreases, as the number of traffic-processing CPUs also decreases.

VoIP Security Measures Still Haven't Been Widely Implemented

The new breed of Session Border Controllers will need to understand all these threats and be able to distinguish between authorized and malicious traffic.

Today's SBC **New SBC**



There are so many threats, vulnerabilities and attack vectors, it's hard to differentiate between real-life scenarios and merely theoretical or inapplicable issues.

We will try to simplify the matter and group the attacks into a handful of categories:

1. Volumetric attacks
2. Protocol attacks
3. Authentication
4. Encryption, integrity and privacy
5. Fraud

Last, but not least, a somewhat related category is "legal intercept" – the ability to work with different country-specific standards and regulations.

Volumetric Attacks

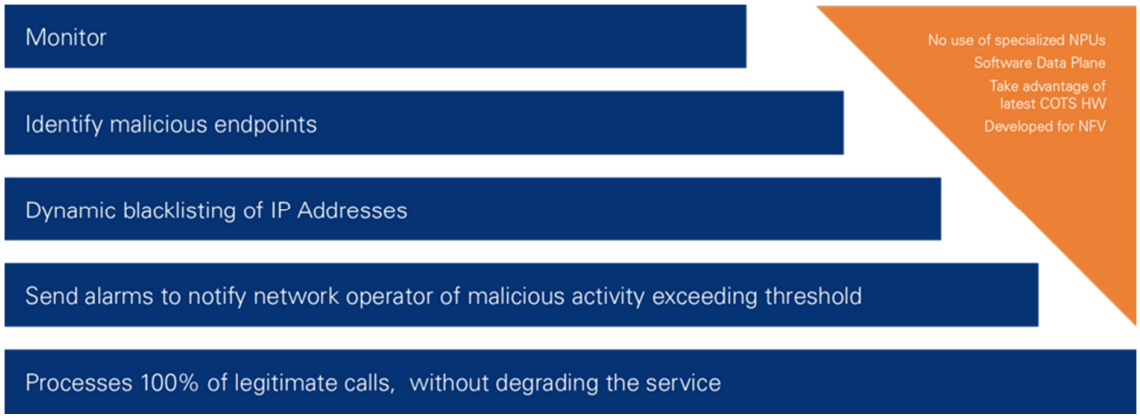
Volumetric DDoS (Distributed Denial of Service) attacks are also known as floods. DDoS attackers seek to overwhelm the target with excessive data, often gained through reflection and amplification techniques. Volumetric attacks seek to make use of as much bandwidth as possible.

These attacks are quite common in the VoIP space, and the most common form is a *crafted* DDoS attack. This attack involves bombarding the SBC with a large quantity of packets. These packets are expertly crafted to force the SBC to devote a large portion of its resources to processing them. Attacks of this type include SIP (Session Initiation Protocol) packets, which require heavy-duty parsing by the control plane CPUs, and TCP (Transmission Control Protocol) SYN packets intended to exhaust all the TCP listen ports on the SBC.

Volumetric attacks are on the rise, according to Gary Sockrider, solutions architect at Arbor Networks: "Looking back to our first report 10 years ago, 90 percent of respondents saw volumetric DDoS attacks on their networks. This year [2014], 90 percent saw application-layer DDoS attacks, which weren't even being discussed back then." DDoS attacks have also grown in terms of the attack bandwidth volume in recent years. The Arbor report found that the largest DDoS attack in 2014 reached a peak of 400 Gbps. In contrast, the largest attack in 2004 was only 8 Gbps. Large-bandwidth attacks are also becoming more common, with Sockrider noting that 159 DDoS events in 2014 exceeded 100 Gbps.

Most industry analysts agree that the trends toward larger and more frequent attacks will continue, so the need to protect against increasingly powerful attacks should be top priority.

The following graphic depicts the types of features that need to be considered in an SBC:



Protocol Attacks

The most common protocol attacks originate from deliberately manipulated SIP messages. This attack involves the usage of a field name or value in the protocol header that is RFC compliant but deviates from normal use. An example might be using field values that contain hundreds of characters, where fewer than a dozen is expected. These protocol attacks using SIP messages make SIP applications vulnerable to attacks that flood servers with huge quantities of fraudulent data, eventually overwhelming the server. Protocol attacks can also result in buffer overflow conditions, which may result in arbitrary code execution. In cases such as these, it is likely that the VoIP network is being attacked.

These attacks can be handled by an SBC with a high degree of flexibility in message manipulation, when encountering a “fuzzed” message. Most importantly, the degree of flexibility in inspecting and manipulating the messages should not affect the SBC’s ability to process legitimate flows – in fact, the SBC must still be able to achieve its rated load when performing this essential function.

To protect against this type of attack, SBCs need to be able to fix the malformed SIP/SDP (Session Description Protocol). Furthermore, the mechanism to fix the malformed protocol needs to be flexible enough to defend against new attacks, without costly code enhancements.

Authentication

The most common authentication attacks come from not being able to keep up with requests from compromised or malicious IP addresses attempting to penetrate your VoIP network. As an SBC is typically deployed at the network's edge, SBCs are usually the first line of network defense. It expects malicious activity to originate on its untrusted interface.

SIP uses a challenge-and-response mechanism. If a request contains incorrect or no authentication information it will be challenged by a "401: Unauthorized" response. The request must then be re-sent with the correct authentication details.

The IMS (IP Multimedia Subsystem) architecture uses authentication to police access to its services. The initial SIP REGISTER is authenticated to verify the user's identity and establish a bond between that identity and the device the user is employing. The nature of that bond can vary, depending on the capabilities of the device and the IMS network itself.

The gold-standard for IMS authentication is normally taken to be IMS-AKA with IPsec. In this scenario there is a pre-shared key stored on the user's ISIM card (embedded in the phone) and the network's user database (stored in the HSS).

However there are various cases where IMS-AKA+IPsec may not be used, typically when either the network or UEs don't support it. 3GPP TS 33.203 describes the alternative approaches in its annexes.
Simple SIP digest authentication is used in almost all non-IMS SIP deployments today. It provides mutual authentication but very little other security (no integrity, encryption, etc.). Unlike "normal" VoIP deployments, which may authenticate every request, IMS in general only authenticates REGISTERs. To prevent a security hole, the SBC validates that any other requests originating from a subscriber come from the same IP address (and same Via header) that the authenticated REGISTER uses. This requires that the access network prevent IP spoofing. If the access network is not trusted to do this, then the IMS core (S-CSCF) may authenticate other non-REGISTER requests explicitly.

Digest authentication may be improved by the use of TLS (Transport Layer Security) to provide integrity and encryption. If neither TLS nor IPsec is supported (or enabled), and SIP digest is not deemed sufficient, additional options are available for fixed and mobile network access.
These mechanisms can all coexist, and the SBC is expected to be able to support all of these mechanisms concurrently.

Encryption, Integrity and Privacy

Generally, SIP voice data traveling over the Internet is sent as completely open packet streams. Your voice conversation is sent as an RTP stream of data that is not encrypted or protected in any way. Anyone having access to the underlying network can listen in on those conversations without any special hardware or rocket-science skills. Public Wi-Fi, hotel Internet and shared computers are very vulnerable to this type of attack, but almost any corporate IP network can be compromised as well. This is potentially a serious security threat and is

unacceptable for business VoIP service today due to the magnitude of the risk it poses to corporate security. On top of being able to spy on your data, it's also possible for a malicious device to inject additional content into the message or otherwise adjust the message. This could be executable code that is used to gain root access to your system and completely compromise it. It's critical that this not occur.

Security experts have tackled these two problems in parallel, with encryption and integrity checks. Encryption ensures that only trusted recipients can read the contents of the message. And integrity checks ensure that the recipient can be confident that the message was sent by the expected sender, without tampering.

However encryption and integrity schemes can't run end-to-end, because the devices in the network core need to be able to inspect and modify the messages. A device is required to interwork between the insecure outside and the secure core of the network. That device is an SBC.

There are various schemes available to operators, although none have seen widespread adoption:

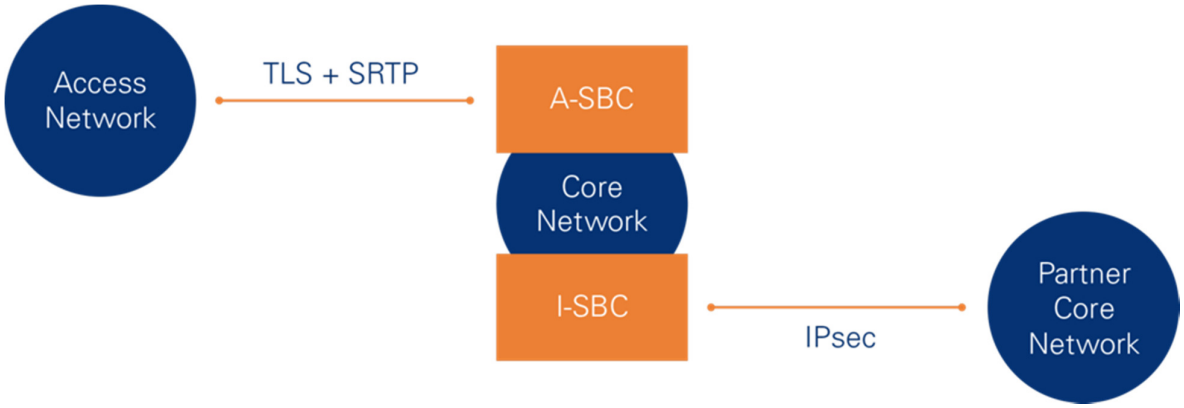
- TLS can be used to encrypt the signaling.
  - It runs over TCP on a per-port basis and is negotiated when the TCP connection is set up.
- IPsec can be used to encrypt signaling or media.
  - It runs at the IP layer, below the transport protocol.
  - It can be negotiated in two ways – IKE and IMS-AKA.
- IPsec is negotiated via IKE during system initialization.
- IMS-AKA negotiates in SIP registration message exchange.
- SRTP is used to encrypt RTP packets.
  - There is a variety of schemes, but the most common is to exchange keys in the TLS of a session set up using TLS.

The correct scheme to use depends on a couple of factors:

- Access or interconnect?
  - Interconnect SBCs have a low number of trunking connections with a high volume of traffic.
  - Access SBCs have a large number of connections to access devices, each of which handles a low volume of traffic.
- Signaling or media?
  - Signaling is used to set up calls. It consist of large, variably sized messages that can be sent at any time.
  - Media comprise a much larger volume of packets, which are often small. They can only be sent when a call is set up.

In interconnect scenarios we expect signaling to use TLS or IPsec, and media to use IPsec. The IPsec encryption is often performed by downstream routers from the SBC, to reduce encryption demands on the SBC.

In access scenarios we usually see TLS/SRTP. Vanilla IPsec doesn't work for NATs, and the extensions that do aren't widely available, so it's not a suitable scheme in a wide range of access networks. IMS-AKA is still not heavily deployed, although this may change as most VoLTE networks are expected to be IPv6 and therefore have no NATs.



Sometimes, people making SIP calls want to hide their identities from the endpoints that they call (or are called from). Much of the time it is not feasible for endpoints to remove personal information at source, since this information is required for routing and billing purposes. In these cases, users can achieve privacy by adding a Privacy header to their SIP messages and routing them through a **SIP privacy service**, as defined in RFC 3323. SBCs should be able to act as a SIP privacy service to provide security to an operator's subscribers.

Topology hiding is another technique of shielding sensitive internal network information from devices outside that network. This helps prevent targeted attacks on the internal devices, and conceals commercially sensitive network architecture information.

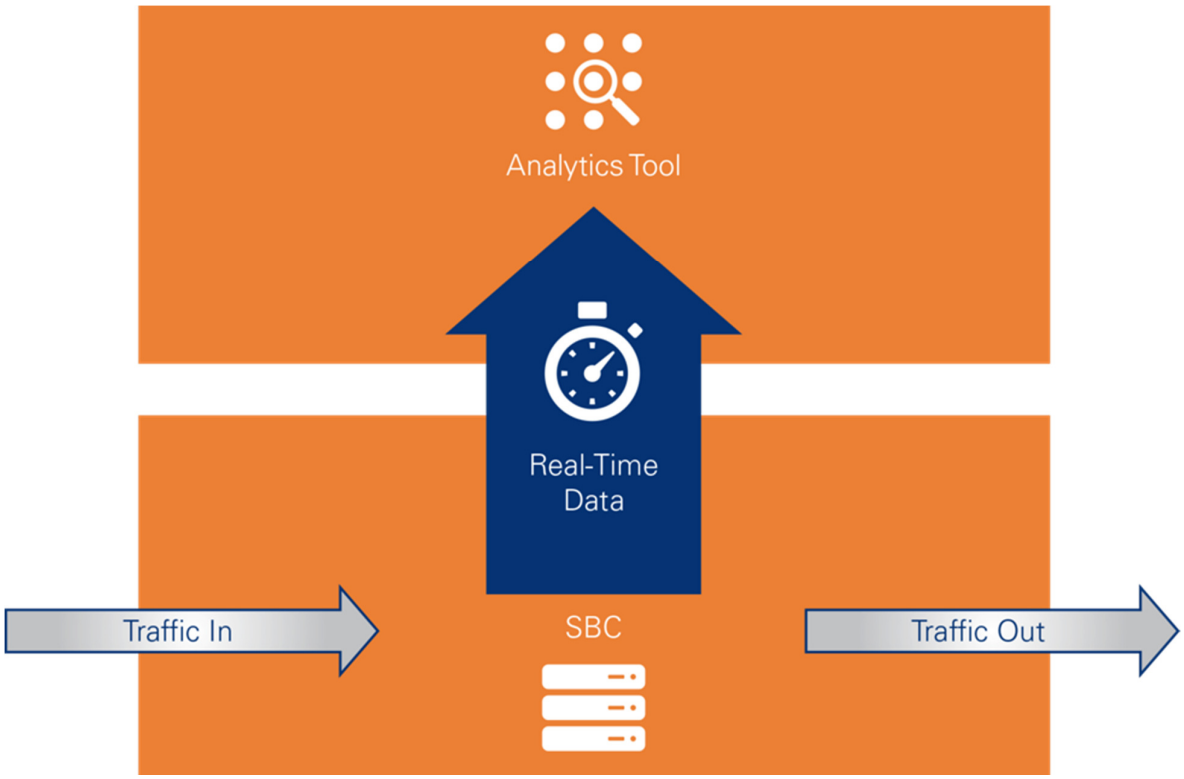
Most SBCs support topology hiding by automatically removing and rewriting certain parts of protocol messages that can expose topology information. These features should be easy to configure. A powerful set of message manipulation features can enable you to configure customized topology hiding based on the requirements of your deployment – for example, by stripping specific SIP headers or by applying search-and-replace rules to remove IP addresses from the body of SIP messages.

Fraud

Serious, sustained and widespread "theft of service" attacks continue across the service provider community. This has resulted in hundreds of thousands of high-value (e.g., international) calls being made fraudulently, totaling tens of thousands of call hours in the last couple of years.

VoIP fraud can affect any organization that uses or sells VoIP services. In most cases, the fraud target is an enterprise. Most enterprises never realize they have been hacked, refuse to pay the fraudulent charges and threaten to switch to a different service provider. The SIP service provider has little leverage over its international long-distance vendors and is left to cover the bill.

SBCs should have a mechanism that is able to detect subscribers' call behavior and alert the operator when it detects an anomalous pattern of usage that may indicate fraudulent activity on a subscriber's line.



Legal Intercept

While legal intercept is not a security issue in its self, it is a required feature in most countries, allowing the government to intercept calls for the purpose of analysis or evidence

Almost all countries have LI capability requirements and have implemented them using global LI standards developed by the European Telecommunications Standards Institute (ETSI), 3rd Generation Partnership Project (3GPP) or CableLabs – for wireline/Internet, wireless and cable systems, respectively. In the USA, comparable requirements are enabled by the Communications Assistance for Law Enforcement Act (CALEA), with the specific capabilities promulgated jointly by the Federal Communications Commission and the Department of Justice.

SBCs need to provide this capability for VoIP networks and make sure they comply with different countries' regulatory requirements.

Conclusion

While security issues can be classified and analyzed in many ways, one thing remains certain: It's just a matter of when, not if, a major attack happens against a large service provider network.

The burden is therefore on the service providers' shoulders, and SBC manufacturers should help carry this burden and protect the networks in which Session Border Controllers are deployed.