clavister WhitePaper

Clavister DoS and DDoS Protection

How to protect against DoS and DDoS attacks using Clavister

Overview

Denials of Service (DoS) attacks are, as the name suggests, attacks that aim to interrupt or completely suspend access to a service. Many recognize the abbreviation DoS or DDoS from having read about high profile websites made unavailable by an overload attack but the area is much broader than that. DoS and DDoS attacks comes in many forms and shapes and can disrupt the entire business and cost huge amounts of money in lost revenue and productivity.

Unfortunately, becoming a victim of an attack, DoS or DDoS, can now be considered as part of everyday life. As attack tools are becoming more widely available and easy to use, the number of organizations that are attacked has increased dramatically.

Off-the-shelf tools not only make these attacks easier to launch but are also more vicious as they include capabilities to make use of so called Bot-Nets in a coordinated attack (Distributed Denial of Services - DDoS). This form of attack is usually more difficult to combat and leads to more severe consequences.

In this paper, we sort out the concepts around these attacks and explain how different technologies are used, which vulnerabilities and weaknesses hackers most commonly target and how to combat these threats in an effective manner.

DoS and DDoS is a problem that grows exponentially

To understand how the threat of DoS / DDoS attacks evolve, one should look at two key factors: the number of attacks and how complex / extensive these attacks are. The number and complexity translates to the probability of being subjected to an attack and the severity of consequences of an attack. If both factors increase, the problem grows exponentially.

Unfortunately most studies show an increase in both frequency and capacity. In a report by a well known DoS mitigation service company covering quarter 4-2013, the statistics shows a staggering increase of 18% in the number of attacks and an increase of 84% in size (size meaning the average packets-per-second during the peak of an attack).

The exponentially growing problem of DoS and DDoS attacks stress the need for a well thought out strategy for how to respond and handle the crisis situation during an attack.

Opportunity makes the thief - An expression that applies to DoS/DDoS attacks?

DoS and DDoS attacks have existed almost as long as Internet but have been a relatively limited phenomenon as it previously required specialized knowledge to carry out a successful attack.

One factor contributing to the dramatic increase in number of attacks is that the tools to create Denial of Service (DoS) attacks have become more accessible and easy to use even for those who do not possess special knowledge.

The reason why packets per second in an attack has increased includes many factors. One factor is that Internet capacity and computer resources for those creating the attacks have increased. Another and probably most important reason is that tools to create coordinated attacks where multiple systems works together have become more accessible (coordinated attacks are also known as Distributed Denial Of Service attacks). The network of machines used in a DDoS attack are known as bot-nets and can today be rented at low cost and minimal effort.

Unlike many other types of attacks that usually are run by organized criminals with financial interests, DoS and DDoS attacks are more often an expression of dissatisfaction and a form of retaliation.

Organized crime with a financial interest does exist in this context but usually only as the party providing bot-net infrastructure for rent or as part of ransom schemes. The organized criminal groups infect thousands of computers with Trojans. The infected machines, known as Zombies, are often unaffected and unaware of this until the day that the infrastructure is rented out to someone who will then activate and coordinate them to launch a DDoS attack.

Organized crime has a financial interest in infecting large quantities of computers but also to make attack tools as sophisticated and accessible as possible simply because more attacks leads to a greater income.

All this means that people who are dissatisfied with an opinion or how a company has acted against them can more easily and more quickly retaliate. In other words, it is easier to act in the heat of the moment, or as the saying goes: Opportunity makes the thief.

Different types of DoS and DDoS attacks

To effectively protect against these threats one must understand how an attack is designed, what systems are usually targeted and how the attacks will take place. The nature of DoS and DDoS attacks also makes it necessary to understand how the infrastructure can be affected, which network components represent the weakest points and the potential to cripple an entire business as a domino side-effect of someone trying to bring down a public web server.

DoS and DDoS attacks are usually divided into different groups (see list “ Common variants of DoS and DDoS attacks” below)

Each type of attack has a different pattern and must be fought in different ways to provide adequate protection and reduce the impact

Common variants of DoS and DDoS attacks are:

Attacks that flood the service

- Attacks which overload internet connections
- Attacks which overload targeted computers or applications/services
- Attacks that overload the weak points in the network infrastructure

Attacks that crash or disrupts the service without having to flood them:

- Attacks that exploits vulnerabilities in applications in order to suspend the service
- Attacks that damage configurations in order to disrupt a service
- Attacks that can disrupt legitimate traffic by sending unsolicited messages to reset connections for real users

Overloading the Internet connection

Attacks where the amount of data exceeds the capacity of the victim’s Internet connection often create devastating consequences, where customers and external users cannot access the organization’s various public services. It also creates problems for internal users who can not use systems located outside of their own network, e.g. cloud based systems such as Office365 or Salesforce.

To generate enough traffic and achieve an overload of the internet connection it is often necessary to have a large amount of computers to participate in a coordinated attack. Depending on the internet bandwidth capacity and type of attack, it might require anything from a few hundred to several thousands of computers. This type of attack is very difficult to stop yet easy to perform if the attacker has access to a Bot-net.

Even if this type of large scale operation might not be the most common type, the severity of the consequences is a good enough reason to revisit mitigation strategies.

The trend for DDoS attacks has recently shifted utilizing Bot-nets with large amounts of hosts to smaller networks but with hosts that are more powerful and that sit on higher bandwidth capacity links. From a hacker's perspective, fewer but more powerful hosts may be preferred, especially for attacks of a more complicated nature.

Overloading weak points in the network infrastructure

Many organizations use, for practical and security reasons, a single layer of firewalls to both manage the public services located in the DMZ (Demilitarized Zone) and the private services located in various internal networks. Additionally the firewall might be used as the core-router for these internal networks. In such architectures it is crucial to review the potential weaknesses and understand how a denial-of-service attack targeted towards the public services can, as a side-affect, cripple the entire network and all its users.

In a scenario where an inadequately dimensioned firewall, router or other central network equipment is overloaded by a DDoS attack from the Internet, traffic on the internal networks will be affected as well. Some examples of how such a situation manifests itself includes the following:

- VPN connections are disconnected.
- VoIP phone calls will suffer from poor quality or be entirely disconnected
- Internal file shares become slow or impossible to use
- Internal applications and services become slow or stop working
- External services will be slow or become inaccessible from the internal or external network
- Access to email becomes extremely slow or is completely suspended
- Backup and log data sent between different segments in the firewall becomes slow or stops working

Firewalls are often wrongfully dimensioned to only manage a scenario with legitimate traffic and a small subset of the security features activated. As new services are brought into use, more functionality enabled and network capacity increased, the conditions change and might not be able to handle the load under an attack.

Are UTM and NGFW firewalls more vulnerable to DoS attacks?

Many organizations choose to upgrade the software on existing hardware and add UTM and NGFW features. Application Control, IPS and similar offers good protection but turning on additional functionality must be done in a controlled and measured way.

When more functionality is enabled, adding more stress on the firewall, you must ensure that capacity is still enough to handle the traffic during a DDoS attack while also providing uninterrupted service for the internal network.

Many UTM and NGFW products have been designed around relatively old-fashioned technology where, for example, application recognition is done using an IPS Engine with hundreds of thousands of application signatures. This technique not only results in a high margin of error, but also in severe performance degradation. Some vendors have a performance degradation of up to 80 % when this type of functionality is enabled. A performance degradation of 80% on the firewall will probably lead to the entire network and all users being affected during an attack.

The firewall is usually not the intended attack vector but because of poor planning and performance it may become the bottle-neck that cause consequences greater than the attacker ever had hoped for.

Attacks targeting specific computers or applications

Instead of overloading the internet connection, attacks can be designed to target specific systems and disrupt critical services with relatively little amount of traffic.

Vulnerabilities in the system can be anything from a bug in the code of the application or operating system, but can also be as simple as a website that requires a relatively large amount of processing power to generate a specific page.

The most classic form of attack targeting a specific application is to generate HTTP requests to a specific page on a website that contains large images or files. A few megabytes of requests from the client(s) will result in the web server responding with several gigabytes of data. This can disrupt both the webserver's operation but also create problems with the internet connection.

Exploitation of vulnerabilities in applications

Exploiting vulnerabilities (bugs) in applications can be potentially more devastating but usually requires much more advanced skills. If applications are often protected by, for example, an IPS system it will force the attacker to write custom made attacks and exploit unknown vulnerabilities rather than running an off-the-shelf attack tool. This is not done by anyone and can be very time consuming even for the savvy hacker.

If an attacker is successful with an attack of this category, it can result in the entire IT-environment being compromised and lead to complete outage of all services and possibly lost and / or corrupted data.

In addition to the tangible consequences of such an attack, it might also require a very complicated and time consuming process to restore service.

Exploitation of weaknesses in applications

An easier way to disrupt services, as compared to customizing an attack that exploits vulnerabilities (bugs), is to target weak designs. The theory is quite simple, first you analyze the application or website to find features or pages that take a longer time to load (requiring more processing power). Once the weak spots are found, the attack is focused on these features or pages and creates an overload without any custom written attack and with a relatively small amount of traffic.

Common examples of vulnerable pages or features are those that contain large images or make use of complex SQL expressions.

This type of attack is popular because it is so simple to do and does not require access to a large bot-net. A simple tool that analyzes response times and sizes of all pages on a website and a handful of computers is all that it takes to disrupt service.

To protect against this type of attack it is necessary to apply both behavior-based protection and also design the actual applications so that they can not be easily exploited. As an example, a website that provides a phone directory service should implement security features such as:

- The response to any query should not return a response with more than a 100 entries per page
- The search string must be at least 5 characters
- The search string must be validated for irregularities (e.g. alpha numeric values only)
- Captcha 's to be entered if there is more than one search per second from the same IP address

Other weaknesses in application design are often found in the features that may have been implemented in order to compensate for disruptive connections. For instance, FTP applications are normally designed so that in a single session there are several different types of signaling packets that must be sent in a particular order. If this order is broken and packets that do not belong to any existing session pops up, the application should drop and ignore the packet. Unfortunately some applications have been developed to compensate for disruptive connectivity on the client. When a packet that does not match an ongoing session arrives at these applications there are features that will try to match the packet to a session that might have been lost and to re-establish the session as smoothly as possible. This is a great feature in some cases but also easy to exploit. By sending "illegal" packets to the application it will make the application process a lot of information and use extensive CPU and memory resources to process illegal and irrelevant data and will very quickly result in an overload situation.

Reflection attacks

Reflection Attacks utilize a technique that involves attacking the victim indirectly by using an intermediary, a middle-man. The principle behind reflection attacks is based on the perpetrator sending a fake request to the intermediary where the request appears to come from the victim. Response messages from the intermediary will therefore be directed to the victim. This technique greatly complicates efforts to track down the perpetrator and terminate the attack.

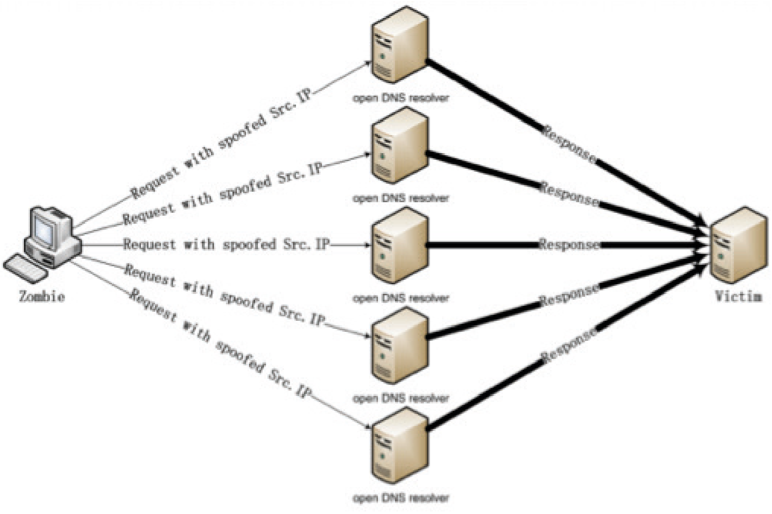
Request with spoofed Src. IP
Request with spoofed Src. IP
Request with spoofed Src. IP
Request with spoofed Src. IP
Request with spoofed Src. IP
open DNS resolver
open DNS resolver
open DNS resolver
open DNS resolver
open DNS resolver
Response
Response
Response
Response
Response
Zombie
Victim

Figure 2: Relection attack

A classic example of a reflection attack is that the perpetrator sends an A record request to a legitimate DNS (Doman Name Server) server. The request is forged (spoofed) to appear as if it was sent from the actual victim instead of from the attacker (this traffic is often referred to as backscatter).

Reflection attacks are most successful when combined with different techniques such as Amplification. A combined reflection and amplification attack means that the victim is attacked through an intermediate AND that the response messages are larger than the requests made from the attacker to the intermediate. DNS Reflection and Amplification attacks means that DNS requests are made from forged IP source addresses and queries the server for records of the type TXT.

In other words, a simple request to an intermediary results in a greater response message to the real target and is at the same time also difficult to trace back to the one who really is behind the attack.

How to build a robust network and protects against DoS and DDoS attacks

There is no miracle solution to protect against DoS and DDoS attacks. Because there are several different types of attacks there are also several ways to protect against these. Efficient protection can be achieved but requires a combination of a well thought trough plan, robust and resilient network design, hardened applications and firewalls with functionality specifically to address these type of attacks.

Since DoS and DDoS attacks come in so many variations it requires a combination of different features to provide good protection. The table below provides an overview of techniques that are well suited for each category of attack.

	IPS	AC	Rate Limiting	Traffic Shaping	SLB	RLB	Cloud och CDN	Capacity Planning	Multi Layer FW
Overloaded internet connection						X	X		
Blocked or disrupted access to internal systems for external users				X					
Blocked or limited access for both incoming and outgoing traffic for employees / users.				X		X			
Overload of network infrastructure equipment									
Caused by high traffic volume			X	X				X	X
Caused by high volume of sessions			X		X			X	X
Service specific attacks									
Overload caused by:									
...downloading large files		X	X	X	X		X		
...targeting resources and functions that utilize high amount of RAM/CPU		X	X	X	X		X		
...high volume valid traffic			X	X	X		X		
...high amount of encrypted (SSL) sessions		X	X		X				
Crash or hang by exploiting vulnerabilities not related to traffic volume	X	X							
Reflection attacks (DNS)		X	X	X	X		X		

Network Design

Correctly Dimension Central Firewall

It is imperative that you have a properly sized firewall, especially when the same firewall is being used to protect both the internal and public networks. A proper dimensioning of firewalls and other equipment must be made considering the total aggregated capacity from all networks connected. This means that you have to study the aggregated capacity for traffic in both directions for all networks connected to the firewall and make an assessment of what the traffic would be in both a normal and worst-case scenario.

Furthermore, dimensioning must be made with consideration to the firewalls capacity based on the features that will be active. Functions that often require a lot of CPU capacity are those that require a more detailed analysis or encryption / decryption. Examples of such functionality include:

- Establishment of SSL sessions with long encryption keys
- Inspection for SSL traffic that includes both decryption and re- encryption

- Application Control
- Anti-Virus
- IPS
- VPN with high encryption and/or high amount of new tunnel establishments

Many network equipment manufacturers only provide capacity figures for so-called plaintext traffic and with only basic firewall functionality enabled. This might be very different from real world configurations and it is important to study how the device is affected if one intends to use services such as UTM and NGFW functionality. Some products may have a performance penalty of up to 80% when UTM and NGFW functionality is activated. This means that even a relatively small amount of traffic during a DoS or DDoS attack can overwhelm the devices. Overloading such a centrally located unit leads to generally poor response times or even complete suspension of all services across the entire network.

In addition to capacity in terms of bandwidth it is also important to ensure that firewalls and other devices can handle a sufficient number of new connections per second, number of packets per second and the total number of simultaneous connections.

Unlike Clavister, most firewalls are designed in a way that means that when the maximum number of connections has been reached, all new connections are blocked until the old ones reach its timeout value. This weakness is present in most firewalls on the market and results in service suspension for several minutes or, at worst, hours before any new traffic is allowed to pass through the firewall.

Segmented networks with separate firewalls for public and internal services

By segmenting the network and separating public and internal systems from each other the consequences of a DoS/DDoS attack can be contained and disruptions minimized.

Instead of both internal and public services being affected by an attack you can separate these and maintain service for internal services even during a full-blown attack targeting the public systems.

Especially in environments where TCP / IP-based solutions are used for storage purposes (NFS for example) it is important to separate the network so that an overload attack against a high-profile target such as the webserver won’t affect the central data storage and thereby disrupt the entire organization.

With a network design based on several layers, or separate islands, it becomes easier to dimension all network elements and reduce excessive “over-capacity” as the number of factors to account for are reduced at each separate point.

This method is recommended for larger and more complex networks where many factors can affect each other and it is more difficult to predict the consequences of an attack.

Cost and administrative complexities are disadvantages of this solution as it requires investment and administration of multiple layers of firewalls and other network equipment. These drawbacks can be limited because the capacity for internet connections and public systems usually are relatively low and therefore do not require the same expensive equipment as the internal system.

In other words, you can size the respective network more closely to the expected limits and with somewhat less excess capacity than that which would be the case when using a central and single layer of firewalls. Depending on the size of the network, this method with multiple smaller firewalls can actually be cheaper in terms of cost/mbps because of the premium that often has to be paid for high-end central firewalls.

Segmented networks and cloud services

Cloud services and so-called Content-Deliver-Networks can be used to distribute the various business critical systems across multiple segments and thus avoid an attack on a single point disrupting the service entirely.

Cloud services also have the advantage that they are usually very scalable and allows temporary increase in capacity for critical services and thereby compensate for the increased traffic resulting from a DoS / DDoS attack.

Clavister provides virtual firewalls, making it possible to apply the same type of firewall technology regardless of the environment to be protected, whether it be the in-house physical network , the internal virtualized data center or even an off-site and hosted cloud environment. All Clavister platforms (physical and virtual) use the same mature and proven core and can be administered with the same central administration tool. Thanks to this, it is easy to make use of existing skills and experiences.

Functions which prevents or helps during DoS and DDoS attacks

Limiting the number of connections

Threshold Rules - Rate Limiting is a feature in Clavister 's products that make it possible to define what is normal or abnormal traffic behavior. By controlling the amount of new connections being set up, in a specific time interval or in total from a single user or network, makes it significantly more difficult for a hacker to overload the protected systems. Since this form of protection does not need to rely on any signatures of known attacks and instead operates based on behavior patterns, it works just as well on known as it does on unknown attacks.

This is one of the most effective ways to prevent and obstruct the attacks based on the number of connections created in a short time and exploit any weaknesses where establishment of new connections is the attack vector.

Intrusion Prevention System (IPS)

Intrusion Prevention System in Clavister 's products can identify both known and unknown attacks by combining several techniques, including signatures. Clavister's IPS functionality looks both for known attacks and unknown attacks that attempt to exploit vulnerabilities. When an attack is identified you can choose to either stop the connection, just log the traffic or even blacklist all traffic from the hosts that has been identified as causing problems.

Bandwidth Management

Traffic Shaping, or bandwidth shaping, is a feature normally used to manage allocation on bandwidth for different users or applications. Applied correctly, this feature can also be highly effective in order to combat overload attacks. This feature can be configured both to prevent a single user overloading the protected systems but it can also be configured in a way to limit the total load that is allowed from all users to a specific server resource. This means that the threat is stopped at the firewall before the protected service crashes or hangs.

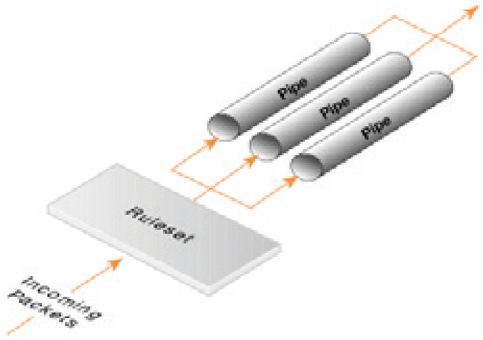

Figure 2: Bandwidth Management

With Clavister products, you can also combine Traffic Shaping with the Intrusion prevention System (IPS) and/or Application Control. This makes it possible to restrict bandwidth for specific users who have been identified as having behavior that deviates from the norm. In this way it is easier to provide a good service to real customers and limit harmful traffic. Many times it is more effective to "trick " the perpetrator and make it appear as if the attack works and bandwidth limit the traffic instead of completely blocking it.

Load Balancing and Server Farming (SLB)

As the name implies, this feature spreads the load or traffic across multiple servers. By using this function it is possible to increase the overall capacity by distributing the load across a cluster of servers providing the same type of service (a server farm). In addition to increased and scalable capacity this feature also improves resilience and fault tolerance resulting in a more robust network. As a nice side effect it also makes daily maintenance work such as server and patch management simpler to manage. Instead of having to plan downtime for upgrading software on a server that is a single point of failure it is possible to conduct maintenance on one server at a time while providing continuous service with reduced capacity.

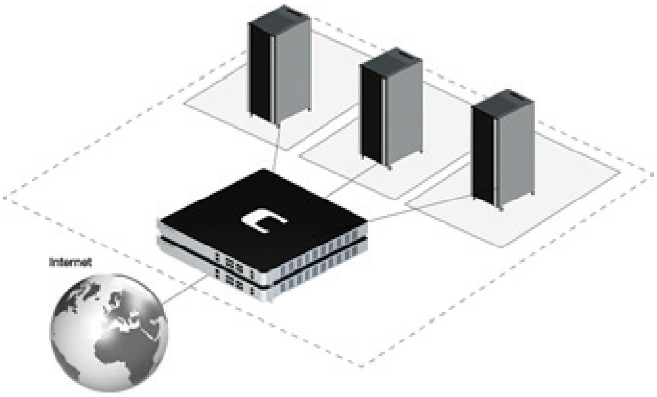

Figure 3: Load Balancing and Server Farming (SLB)

Load balancing - Redundant Internet connections

Through the use of multiple Internet links coordinated by Clavister ‘s Route Load Balancing function, it is possible to ensure that internal users have access to the Internet and services available outside of the organization, even during an ongoing attack where the primary internet link is being flooded.

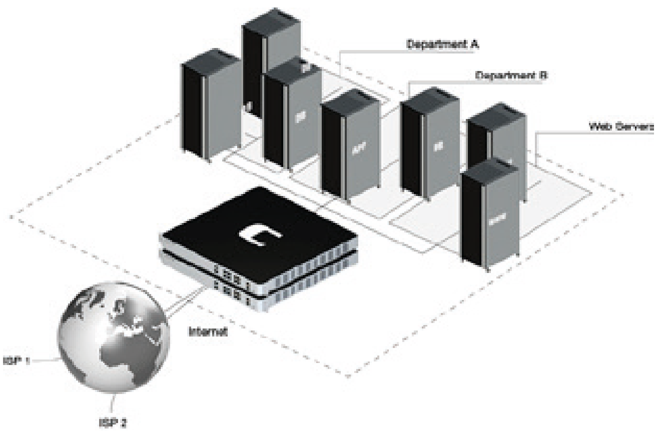

Figure 4: Load balancing - Redundant Internet connections

Instead of a paralyzed organization, critical services may still be available and administrators can work on mitigating the attack with less pressure and risk of human errors.

Clavister ‘s functionality for distributing traffic over multiple parallel links can be configured in several different ways to suit the actual situation. Traffic can be distributed over secondary connectivity either according to a distribution policy for normal operations or as a passive fail over where all traffic is routed over the secondary link only if the primary link is unavailable or shows signs of poor response time.

Active Redundancy - Load Balancing

This means that traffic is distributed over all Internet connections, even in normal operation, thereby resulting in increased capacity and improved response times. This is a good solution when the subscription for the secondary links allows unlimited data transfer at a flat rate/fixed fee.

Passive redundancy - Failover

This means that traffic is only sent over the secondary link if a problem occurs with the primary connection. This is a desirable solution when the secondary links have a limitation in the total amount of data per month (Eg 3G/4G-LTE subscription).

Link Monitoring

In addition to load distribution capabilities, Clavister products also has the capability to monitor each individual link The responses from the integrated link monitoring feature are evaluated and distribution dynamically adapted according to the configured policies. The Clavister link monitoring (Route Monitor) subsystem can measure latency, ping responses and even the responses from application requests. This makes it easy to evaluate the health/performance of the links and not just whether the link is up or down.

With the Clavister Route Load Balancing and Link Monitoring feature it is easy to create a robust and efficient network able to handled DDoS attacks at the same time as it provides benefits during normal operations.

Application Control

Application Control is a feature in Clavister products that identifies and controls traffic based on the type of application used regardless of the port or service used.

Figure 5: Clavister Web Management

Using Application Control, you can prevent the attacker from sending malicious traffic to internal systems by disguising it to look like legit traffic. Regular firewalls without this type of feature will simply allow such malicious traffic to pass through the gateway.

Application Control can also be used to enforce policies on what browser may be used, what pages may be requested and similar. This gives an enhanced protection and can avoid standard attack tools from being used. Of course, tools can be adjusted by the ones who have sufficient knowledge but it will limit the window of vulnerability and reduce the risk for attacks by cyber vandals lacking such skills.

Protocol validation and consistency checks

Protocol validation is used to ensure that the traffic allowed through the firewall really follows the defined standards that apply to each protocol. Typical checks done through protocol validation includes the right sequence number being used on packets, that the correct flags are set and that the sessions are set up in the proper way. Since many attack tools are based on recorded traffic in which, for example sequence numbers and other values are not correct, it is easy to block those attacks by using protocol validation and consistency checks which are part of the base firewall functionality. Once again, these things can be adjusted by someone with enough knowledge but will make it harder for less skilled hackers who are trying to utilize off-the-shelf tools.

Even for the ones who have the necessary knowledge, it still is effective as it will require a more complicated procedure and will require more capacity and power from the host that is attacking the network.

Monitoring and Alarms

Best-practice in the field of monitoring for security purposes is to monitor all equipment and services in the network. Reason for such extensive monitoring is that you should get a good and comprehensive understanding of the normal state and thereby make it easier to detect anomalies. Different tools can then be used to visualize abnormalities or to send alarms when deviations occur. Some things can be automated while others are more effectively handled in a manual way. There are many different tools to monitor network equipment. For monitoring and alarm management with Clavister products, we recommend the following:

- **Clavister InControl**
  Central Management for Clavister products. Contains functions for both management, monitoring and log analysis. Clavister InControl can manage hundreds of firewalls and concurrent administrators and is included in the maintenance agreement for firewall products and requires no additional licensing fee.
- **Multi Router Traffic Grapher - MRTG**
  A free and well-known tool for monitoring the status and traffic from many network devices using SNMP is MRTG. MRTG provides an excellent overview of how traffic flows across the whole network, thus making it easier to detect if there is a problem and where in the network it might be causing issues.
- **OSsec**
  OSsec is a well-known and free tool that can be used to analyze log data from many different sources, This includes log data from firewalls, VPN devices, operating systems, applications and more. OSsec can be used to identify potential breaches by correlating log data from different systems and generate alerts when a specific pattern is identified.
- **SIEM Tools (Splunk and other brands)**
  During an attack, it is more a rule than an exception that several devices are affected in one way or another. It can be a difficult and cumbersome task to identify and understand an attack if looking at the data from each single device at a time as it might require digging through hundreds of thousands if not millions of log records. To assist in finding the needle in a giant haystack, one can make use of automated and policy based log correlation. This is a central and key component in Security Information Event Management (SIEM) tools. These SIEM tools can also be setup to trigger alarms that requires several different events to occur on multiple devices and thereby alert the IT operation staff in an early stage of an attack.

Preparedness plan and Exercise

No security solution is 100% perfect, and even if there were such a solution the internet connection can still be overloaded.

In order to quickly and effectively stop an attack and limit the damage it is crucial to have a contingency plan. A good plan should include who is responsible for the work, how to identify the type of attack you are exposed to, the description of how the attack affects the organization and how to act in the short, medium and long term to mitigate the attack.

An effective plan should include detailed descriptions on how to act and should be updated at least every three months to reflect the current environment.

Many administrators avoid exercises and practice these plans in a production environment, which is perfectly understandable given the potential disruption it can have on the business. However, the limited disruption caused by an exercise in the production network can avoid future disasters.

It is strongly advised to contact a specialist to help conduct a survey and give advice if there is any hesitation or reason to suspect that there are gaps and holes that could jeopardize a smooth and continuous.

Recommendations

DoS and DDoS attacks is a broad concept covering many different techniques of attacks and related risks, it is difficult to make short and simple advice without being too general. Good protection against DoS and DDoS attacks must be tailored to suit each individual organization and network in an optimal way, but there are some general principles that help no matter what environment and situation is involved.

- **Analysis & Network Mapping**

  Analyze your environment and map out what systems are public facing, internal only and the dependencies between all of them. Analyze consequences and impact on other systems if one point fails, including network equipment such as routers and firewalls.
- **Planning**

  Establish a practical and hands-on plan of action in which it is clear who is responsible for what and who makes the decisions in a crisis situation.
- **Documentation**

  Make sure to keep system documentation up to date and that everyone knows where documentation is being stored. Pay special attention to documentation on how backups are stored and how complete servers can be restored.
- **Monitoring**

  Monitor all services and place extra importance on monitoring all services that are public and can be seen as a target for malicious users, customers or other groups that constitute threats.
- **Redundancy**

  A robust network with redundancy helps in case of attack but also contributes to a more efficient network during normal operation. This applies especially to redundant Internet connections and server farms.
- **Virtualization and virtual firewalls**

  Offload and simplify configuration of the central firewall by using a virtual firewall for the more complex and resource-intensive functions (UTM / NGFW) used to secure the virtual environment. Be observant of how the dynamic resource allocation works for your virtual machines. Always configure both the minimum and maximum resource capacity for critical functions running in the virtual datacenter, specially the virtual security products.
- **Capacity Planning**

  A good basic principle is to calculate for having more excess capacity if services and servers are centralized than if they are segregated and isolated. If you use a single layer of firewalls to manage both internal and public networks you should review the capacity of these when all functions are enabled, and compare it with the aggregate capacity of all networks under a worst-case scenario. If you have already made an investment in a central firewall and want to expand security with UTM and NGFW functionality then you should be extra careful and consider upgrading to larger hardware or consider segmenting the public and internal networks with another layer of firewalls.
- **Report & Analysis**

  Use so-called SIEM - Security Information Event Management tools to analyze information from multiple applications and systems. By correlating information from multiple systems, an attack is identified at an earlier stage. SIEM tools also help to recreate and understand how the attack took place and what happened which is of great importance in avoiding the same problems in the future.
- **Prioritize**

  Get the big picture clear and prioritize what is critical for your organization and focus on making sure that prioritized functions and services are secured properly before trying to secure every function and getting held up in too many details. Perhaps it is acceptable that the website has a poor response time for the period under attack but it is critical that employees can continue to operate and use email, CRM, office tools in the Cloud and so on. For other customers it might be the exact reverse situation where internal staff productivity may be impacted but the e-commerce portal must maintain operations at all costs.

Summary

With IT being an integrated part of business any disruption means money lost.

DoS and DDoS attacks are on the rise and the consequences of an attack can be devastating.

Inadequate protection, monitoring and action plan may be the difference between minor disturbances and a complete halt in production, disgruntled employees, lost revenue and potentially lost customers.

There is no bullet proof protection but simple things such as a properly dimensioned and configured firewall, action plans and low-cost redundancy capabilities can fend off most attacks, especially attacks from those who lack specialized skills and might only be acting in the heat of the moment.

Clavister 's products have comprehensive protection against DoS and DDoS and can either be deployed as a central protection or retro-fitted into an existing network as a separate layer. Instead of costly niche products Clavister adds good protection without significantly increasing administration and cost.

Cloud, Content Delivery Networks and virtualization are effective ways to spread risk and create a more robust and tolerant environment. The security of these environments may not be waived and protection equivalent to the physical network should be applied without compromise. Clavister VSG is a virtual firewall with the same functionality as the hardware based version and can be used both in the cloud and the virtual network to protect these environments against DoS / DDoS attacks and other security issues.

A good recommendation is to start simple and improve the security solution in small steps.

It is strongly advised to consider managed services or help from specialized consultants if skills and experiences are not available in-house.

Wait and see is a strategy often applied but can result in major and irreparable damage. Acting before it is too late may sound like a cliché but is very real and applicable to any network security strategy.

Contact Clavister

Visit us at www.clavister.com for more information, or contact us or one of our certified partners for advice.

About Clavister
Clavister is a leading security provider for fixed, mobile and virtual network environments. Its award-winning solutions give enterprises, cloud service providers and telecoms operators the highest levels of protection against current and new threats, with unmatched reliability. Clavister's performance in the security sector was recognized with the 2012 Product Quality Leadership Award from Frost & Sullivan. The company was founded in Sweden in 1997, with its solutions available globally through its network of channel partners. To learn more, visit www.clavister.com.

Where to Buy
www.clavister.com/partners

Contact
www.clavister.com/contact

WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com