SOLUTION BRIEF

Ekinops: Helping Service Providers deliver Cyber-secure services to enterprises

Cyber-Security is a must

Cyber-security is now a major concern for any business or organization when selecting a service provider. As the gateway to the corporate network, service providers can play an important role in helping enterprises provide the first line of defence in blocking malicious traffic and preventing bad actors from accessing critical areas of the corporate network.

The Ekinops OneOS6 operating system powers its range of network access routers and includes the latest zone-based firewall and Denial of Service (DDoS)technologies that are able to detect and stop the latest cyber-attacks from disrupting normal traffic flow and delivering their malicious payloads.

Why zone-based firewall vs interface-based firewall?

Classic firewalls use access control lists applied to every IP address accessible from the firewall. In complex environments this can prove to be a complicated challenge.

Zone-based firewalls are independent of access lists and use policies that can affect all traffic passing through the network and are more appropriate for multiple interfaces which may have different security requirement and access policies.

Why is a comprehensive DDoS protection needed?

DDoS attacks are designed to overwhelm network resources, slow down and ultimately stop all legitimate traffic gaining network access. To ensure acceptable user communication's response times the router must remain manageable under a variety of different types of DDoS attacks:

Type of DDoS attack	Description	Examples
Volume based	Floods the device with a high volume of packets or connections exhausting the CPU and memory resources of the device	Botnet, reflection, amplification
Application based	Floods the device with protocols, used by the device	HTTP flooding, VoIP call and message flooding and malformed messages, control plane applications like DNS, DHCP, BGP, management plane applications like SNMP, SSH
Network based	Exploits protocol weaknesses mainly on layer 3 and 4 of the OSI model	TCP SYN flood, TCP SYN ACK reflection flood, TCP FIN flood, TCP RST flood, TCP PUSH ACK flood, IP packet fragment, ICMP echo request flood, UDP flood, ping of death, smurf attack

Zone-based firewall

At a glance

In zone-based firewall, policies are no longer configured at the interface but are defined between zones. The user can configure different zones, and interfaces can be attached to a specific zone.

This way the customer organization is able to block traffic between different zones inside the LAN.

In this example, the corporate network is segmented into three zones, LAN, DMZ and Wi-Fi, each requiring different access policies.

The firewall defines boundaries between each zone. The default setting is to block all traffic between zones except explicitly authorized traffic. Of course, traffic between two interfaces in the same zone passes freely, as does all traffic between interfaces attached to any zone.

A firewall can make three decisions: pass, drop and inspect.

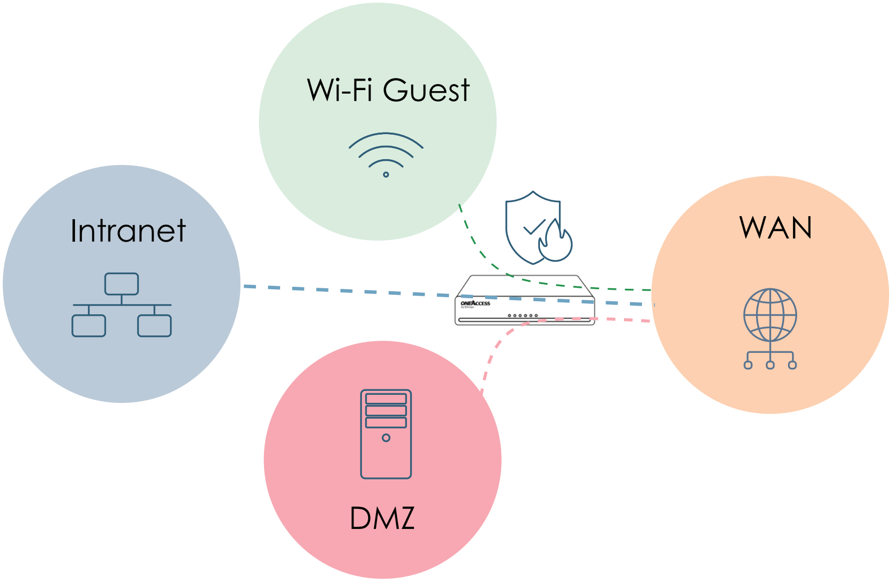

Figure 1 - Zone-based firewall diagram

When the decision is "**pass**" (equivalent to "allow" in the access control list), traffic will be able to pass from one zone to another. When the decision is "**inspect**", return traffic will also be allowed.

But when the decision is "**drop**" (equivalent to "deny" in the access control list) traffic will be discarded. In this case, a summary will show which traffic has been rejected.

Decisions are made according to an access policy. This consists of a list of rules that apply to individual flows by means of filters. Each rule specifies the action to be taken on the corresponding traffic.

When traffic flows from an interface with a defined zone to the management zone (or vice versa), it is allowed by default. However, this can be over-ridden by defining a specific policy between the corresponding zone and the management zone.

But how does it work?

As mentioned previously, an interface is assigned to each zone.

To enable the exchange of traffic between zones, a zone-pair will be defined. Then, to enable the firewall to make decisions about traffic between zones (pass or drop), policies will be defined and applied to each zone-pair.

A policy uses a collection of rules describing the appropriate actions for different inter-zone traffic. As stated above, the three possible actions are: pass, drop and inspect.

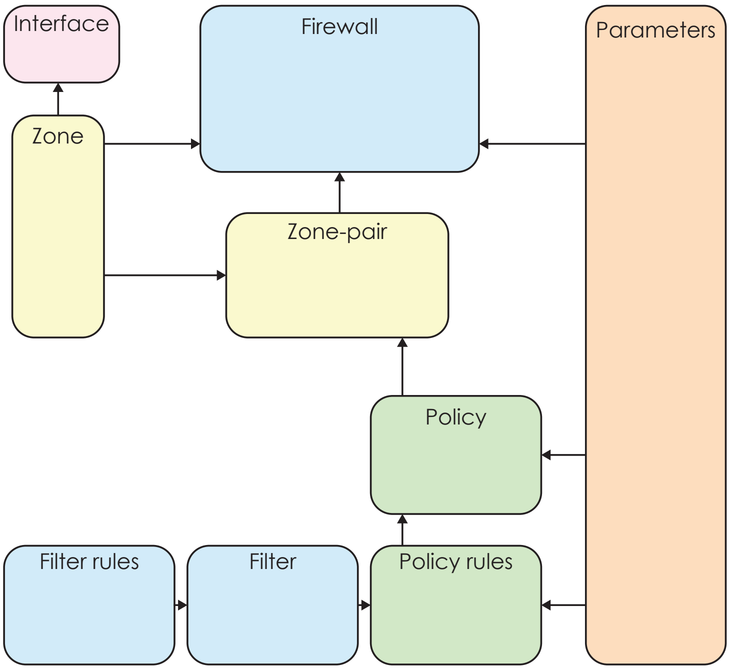

Figure 2 - Zone-based firewall configuration flow

Rules are defined on the basis of filters describing the matching criteria applied to IP packets.

These criteria include source and destination address ranges (IPv4 or IPv6), IPv4 networks and IPv6 prefix delegations. Protocol definitions or port numbers can also be used as criteria.

To complete the firewall configuration, additional parameters can be defined for an application when a new connection is created. These may include time-out values or connection number thresholds.

These parameters can be applied at firewall, policy, or filter rule level.

Zone-based firewall in Ekinops solutions

The OneOS6 operating system includes a powerful embedded zone-based firewall. This can be activated simply via the ACS license (advanced connectivity and security).

All physical data and voice products, as well as their virtualized equivalents (VNF), can use the zone-based firewall.

A WEB UI is available as standard to enable configuration of zone-based firewall by the end customer.

Note: For more information on configuration and usage, please refer to the OneOS6 user manual.

DDoS protection

At a glance

OneOS6 DDoS protection uses a set of mechanisms to protect the router against attacks from malicious actors.

This feature comes as standard in OneOS6. All physical data and voice products, as well as their virtualized equivalents (VNF), can use the DDoS protection against a range of common DDoS types.

Volume attacks:

OneOS6 prevents volume attacks from overwhelming the router's CPU and memory resources to ensure that the router will always be accessible and controllable when subjected to such attacks.

OneOS6 monitors the CPU load and starts dropping low-priority packets when it exceeds a certain threshold.

Protocol attacks:

OneOS6 detects and limits incomplete TCP connections. If not controlled, incomplete TCP connections can lead to router resource saturation

Fragmentation attacks:

OneOS6 detects IP fragmentation attacks that can exploit weaknesses of IP protocol, resulting in resource saturation of the router. Those are typically:

- Overlapping IP fragments (This means that the second fragment is contained in the first)
- Fragment size over 65535 bytes
- Too many too small fragments

How does it work?

The DDoS protection engine is made of 3 basic building blocks.

- A DDoS policer
- A DDoS stateful engine
- A DDoS protocol policer

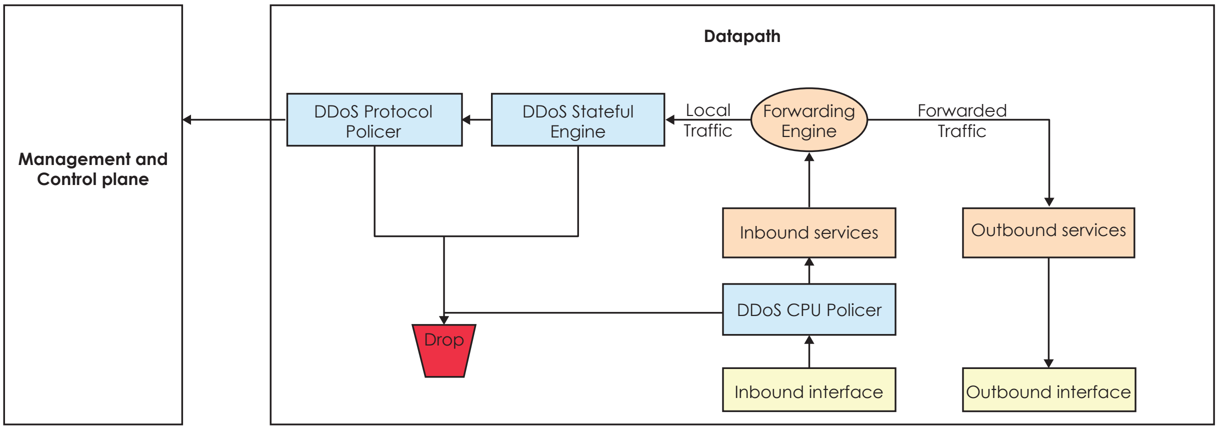

Figure 3 - DDoS protection diagram

DDoS CPU policer:

The DDoS CPU Policer itself consists of 2 parts:

- A CPU Classifier to make the distinction between high and low priority traffic.
- A CPU Policer for the low priority packets.

The classifier and the policer run both at the very entry of a packet into the device before any other processing on all the traffic.

They immediately act at the ingress traffic prior to any other services for a minimum impact on the performance hence it applies both to forwarded and local traffic.

The ingress traffic is defined as high priority or low priority traffic based on the pass/drop policy. Priority can be configured per protocol or/and port number.

DDoS stateful engine:

This keeps track of sessions of local traffic. It controls and limits the number of half open TCP or UDP sessions as well as their lifetime.

DDoS protocol policer:

This prevents the IP protocol stack becoming overloaded with unwanted packets from several DDoS attacks.

The policer can restrict the number of ingress packets per second on the protocol stack.

It defines which ingress packets are counted. It consists of several rules based on protocols, port numbers and interfaces.

If too many packets are matching with the rules during a configured time interval, it is assumed that a DDoS attack is ongoing, and the local policer goes into violation state for a configurable number of seconds. During this violation state, all matching traffic is dropped.

Note: For more information on configuration and usage, please refer to the OneOS6 user manual.

More security features

To complement the zone-based firewall and DDoS protection features, the Ekinops OneOS6 offers a range of additional security features to help Service Providers to deliver enhanced secure services to enterprises

Secure boot

All physical data and voice products feature a secure boot by default. Combined with assigned software it enables protection against installation of malicious software that could take control of the product during boot process.

Secure boot is a factory installed in the product.

TPM (Trusted Platform Module)

The TPM (Trusted Platform Module) is a secure, isolated, cryptographic processor that is typically built into the hardware. The TPM is used to securely store cryptographic keys, preventing unauthorized access.

The TPM is the latest feature in the Ekinops product range. It is available as a default feature for all mid-range routers and as a factory option for the branch office product range.

Secure management protocols

OneOS6 supports a wide variety of secure management protocols such as SSH server and client, SCP server, SFTP and HTTPS client, HTTPS server for web GUI, SNMPv3, CWMP (TR-069) over HTTPS, Zero Touch Provisioning over HTTPS, Netconf over SSH and mTLS, telnet over mTLS.

User password policies

In OneOS6, different password policies can be created for different user accesses.

The password policy defines restrictions on passwords, (minimum password length, the type of characters that must be included in the password).

The password policies are applicable to the different server access possibilities including UI (console/telnet/SSH), NETCONF, SNMP, or web UI.

Certificate management

The certificate is a way to securely authenticate the peer contact in many secure applications. IPsec, HTTPS for web GUI, NETCONF over mTLS, SYSLOG over mTLS, NetFlow over mTLS, CWMP over HTTPS, SIP-TLS are all applications that may use certificates.

OneOS6 uses X.509 certificates to authenticate the OneOS6 device to a peer application.

Enrollment using SCEP, renewal and revocation lists are all supported in the complete Public Key Infrastructure (PKI) ecosystem.

Certificate can also be installed in the product at factory.

Conclusion

OneOS6 provides a comprehensive range of security features that enable service providers to offer their corporate customers connectivity packages a high level of protection against cyber-attacks aimed at breaking into the customer's network or blocking its use.

In addition to these features, Ekinops offers a range of professional services to support service providers in deploying and using our solutions including:

- Proactive monitoring of CVE's (Common Vulnerabilities and Exposure), their re-scoring, communication towards customers, and where necessary remediation.
- SABs (Security Alert Bulletins) publishing which are accessible to Customers via a private portal and e-mail.
- Personalized security penetration tests for Customer's specific requirements and service configurations (port scanning, OWASP Top 10 penetration testing, DAST testing, resistance to external DDoS attacks).

About Ekinops

Ekinops is a leading provider of open and fully interoperable Layer 1, 2 and 3 solutions to service providers around the world. Our programmable and highly scalable solutions enable the fast, flexible and cost-effective deployment of new services for both high-speed, high-capacity optical transport networks and virtualization-enabled managed enterprise services

Our product portfolio consists of three highly complementary product and service sets: Ekinops360, OneAccess and Compose.

- Ekinops360 provides optical transport solutions for metro, regional and long-distance networks with WDM for high-capacity point-to-point, ring and optical mesh architectures, and OTN for improved bandwidth utilization and efficient multi-service aggregation.
- OneAccess offers a wide choice of physical and virtualized deployment options for Layer 2 and Layer 3 access network functions.
- Compose supports service providers in making their networks software-defined with a variety of software management tools and services, including the scalable SD-WAN Xpress and SixSq Edge-to-Cloud solutions.

As service providers embrace SDN and NFV deployment models, Ekinops enables future-proofed deployment today, enabling operators to seamlessly migrate to an open, virtualized delivery model at a time of their choosing.

A global organization, Ekinops (EKI) - a public company traded on the Euronext Paris exchange operates on four continents.

EKINOPS360
Dynamic Optical Transport

ONEACCESS
Fast Network Virtualization

COMPOSE

© 2023 Ekinops « all rights reserved » - Ekinops reserves the right to change the technical characteristics described in this document without prior notice - Security_1123