Next Generation Firewall technical specifications

1. General Requirements

1.1. The proposed system shall Consists of two (Active / passive) appliances.

1.2. The proposed system shall support unlimited IP addresses licenses if exist.

1.3. The solution should be based on modern next generation firewall architecture. Allowing the university to benefit from the design in improving network security by supporting the following functions (please refer to required subscription section):

1.3.1. Application Control

1.3.2. User Identification and control

1.3.3. Content Protection against (network attacks, spyware, viruses, modern malware).

1.3.4. Content filtering (aka URL Filtering & file-blocking)

1.3.5. The application policy controls, firewall policy controls, and threat prevention features all be enabled in a single rule (Policy) in the solution.

1.4. The system must have clear (hardware module) separation of management, control and data plane CPU and memory resources.

1.4.1. The capability to restart the management Plane without need to reboot or impact on ongoing traffic (data plane)

1.4.2. The control plane should be running on dedicated CPU and memory other than the ones used by data plane and the vendor should provide a document showing the resources given to control plane and the connectivity between control and data planes.

2. Hardware Requirements (Physical or Virtual Appliance)

2.1. The proposed system must be able to have minimum support of:

2.1.1. 12 x UTP (10/100/1000 bps)

2.1.2. 8 x SFP/SFP+; Min of 4xSFP+.

2.2. 240 GB dedicated on box logging and reporting storage.

2.3. 1 x Console port.

2.4. 1 x dedicated copper based management port.

2.5. 2x UTP Dedicated ports for High Availability.

2.6. The proposed appliance from factory shall be Rack Mountable.

2.7. The proposed system must use the following power supply:

Dual hot swappable 100-240 VAC, 50-60 Hz power supplies that operate in redundant mode.

3. Operating System and Management Requirements

3.1. The proposed OS must:

3.1.1. Be proprietary OS.

3.1.2. Upgradeable via Secure Web UI or secure file transfer.

3.2. The configurations on the device shall:

3.2.1. Be easily backup or restored via GUI and CLI to/from local PC, remote centralized management.

3.2.2. Provide CLI command configuration file that is readable by Windows Notepad

3.3. The proposed system shall minimally provide management access through:

3.3.1. GUI using HTTPs access.

3.3.2. CLI console using console port & SSHv2.

3.4. The administrator authentication shall be facilitated by local database & remote authentication services such as Radius, LDAP and TACACS+.

3.5. The system shall support profile base login account administration, offering gradual access control such as only to Policy Configuration & Log Data Access

3.6. The system shall be able to provide virtual Entity administration which access is restricted to a particular domain accordingly.

3.7. The proposed system shall be able to limit remote management access from certain trusted network or host.

3.8. The proposed system should be able to facilitate administration audits by logging & Compare Different version of configurations files and detailed activities to event log.

3.9. The proposed system should save minimum 10 configuration profiles on the device storage.

3.10. The proposed system should save automatically last 50 configuration changes on the device storage.

4. System Requirements

4.1. The device shall provide minimally (1) functioning virtual domains.

4.2. The system shall support profiling of the following feature components:

4.2.1. Application Firewall

4.2.2. IPS

4.2.3. Anti-Virus & Anti-Malware

4.2.4. Content filtering

4.2.5. User Group settings

4.2.6. Routing

4.2.7. Log & report Configurations

4.2.8. DNS security

4.3. The proposed system shall be able to operate on either Transparent (bridge) mode, Route (Layer2 and Layer3) mode and span mode simultaneously and within the virtual domains

4.4. The capability to run at least (40) security interface zones.

5. Routing

5.1. The system must be able to support routing protocols including:

5.1.1. OSPF for IPv4 and IPv6.

5.1.2. static routes.

5.1.3. policy based routing: the proposed NGFW should have the capability to perform policy based forwarding based on Source IP/Zone/port, Destination IP/Zone/port and/or Application in use.

5.1.4. BGP ipv4.

6. Firewall Requirements

6.1. The matching Firewall policy should include:

6.1.1. Address Object(s) – IP, IP range, Subnet, FQDN.

6.1.2. Service Object(s)

6.1.3. Scheduling capabilities

6.1.4. In use Applications or group of applications

6.1.5. In use URL category

6.1.6. User-identification (users or group of users based on integration with AD/Group mapping)

6.2. The firewall policy table shall support both IPv4 and IPV6 GUI configurations.

6.3. The firewall policy table shall also allow display of filtered firewall policies based on selected column objects.

6.4. The proposed system shall support the following firewall policy features:

6.4.1. At least (10,000) Address Objects.

6.4.2. At least (1,000) address groups.

6.4.3. Predefined and Customs Service Objects (services/app).

6.5. The proposed Statefull Inspection Firewall should include:

6.5.1. Policy based Network Address Translation (dynamic and static NAT)

6.5.2. Static NAT; one to one address mapping and static NAT groups.

6.5.3. Port Forwarding.

6.5.4. User integration & control.

7. User / Device Authentication Requirements

7.1. The proposed Firewall shall be able to support various form of user Authentication methods simultaneously, including:

7.1.1. Local Database entries.

7.1.2. LDAP server entries.

7.1.3. RADIUS server entries.

7.1.4. Native (agentless integration) Windows AD user napping (Single sign on capability) for at least 64,000 DC objects.

7.2. The administrators shall be able to create user groups which are lists of user identities. An identity can be:

7.2.1. a local user account (user name and password) stored on the unit

7.2.2. A RADIUS, LDAP, or TACACS+ server users (all identities on the server can authenticate).

7.2.3. a user and users group defined on a Microsoft Active Directory server

7.3. When user authentication is enabled on a firewall policy, the authentication challenge is issued for any of the selectable protocols:

7.3.1. HTTP (can also be set to redirect to HTTPS)

7.3.2. HTTPS

7.4. The solution shall be capable of providing Windows AD single sign-on.

7.5. The proposed solution must support user-based policies.

8. Next Generation Threat Prevention (NGTP) Requirements

8.1. NGTP must include:

8.1.1. IPS vulnerability/exploit scan (against all known applications)

8.1.2. Full Anti-Virus scan against below applications:

8.1.2.1. Http

8.1.2.2. SMTP

8.1.2.3. imap

8.1.2.4. pop3

8.1.2.5. smb

8.1.2.6. Ftp

8.1.3. Full scan for Anti malware scan (including spyware, worms, Trojan, botnets, adware, backdoors, keylogger …)

8.1.4. File blocking (FB) by type and application

8.1.5. Data Leakage Prevention (scan for keywords and credit card numbers)

8.1.6. Block buffer overflow attacks

8.1.7. Block DoS/DDoS attacks

8.1.8.Supports attack recognition for IPv6 & IPv4

8.1.9.Built-in Signature and Anomaly based IPS engine

8.1.10. Ability to create custom user-defined signatures

8.1.11. Supports CVE-cross referencing where applicable

8.1.12. Supports automatic security updates directly over a secure connection without rebooting the device.

8.1.13. The platform should be capable to enforce various NGTP profiles on different applications running on same L4 session information

8.1.14. The proposed solution should provide malicious DNS signature blocking (ability to alert and drop) malicious DNS requests.

8.2. NGTP throughput should be measured based on a real-time application mix of traffic including combined services mentioned in 8.1

8.3. NGFW should have the capability to apply different NGTP profiles to every legitimate application passing through the network.

8.4. The NGTP detection methodologies shall consist of:

8.4.1. Signature based detection using real time updated database.

8.4.2. Anomaly based detection that is based on thresholds.

8.5. Administrator shall be able to configure DoS policies that are used to associate DoS settings with traffic that reaches an interface based on defined services, source and destinations IP/Range.

8.6. The proposed system shall identify, set threshold and act on network traffic anomalies of statistical anomaly types (Flooding, Scan, Source session limit, Destination session limit) for the TCP, UDP, and ICMP.

8.7. The device shall allow administrators to create custom NGTP signatures: that includes custom-based IPS signatures, applications and Malware:

8.7.1. Statistical anomaly profiles.

8.7.2. Signatures.

8.8. The NGTP system shall have signatures in a single local DB for all threat types.

8.9. NGTP Signatures can be updated in two different ways:

8.9.1. Manually.

8.9.2. Push or Pull technology.

8.10. When a signature is matched, the following configurable actions can be automatically taken:

8.10.1. Detailed attack logging

8.10.2. Inbuilt email alerts

8.10.3. SNMP traps

8.10.4. Pass, block or reset sessions

8.10.5. Syslog messages (locally in same device and remotely to centralized Syslog server)

8.11. The device shall allow administrators gradual NGTP signature implementation by:

8.11.1. Configurable NGTP filters to selectively implement signatures based on severity, target (client/server), protocol, Application types and optionally OS.

8.11.2. Configurable NGTP filter-overrides that provides specific signature exclusions or variations based on source and destination addresses

8.12. The device shall allow administrators gradual NGTP anomaly implementation by:

8.12.1. Multiple Anomaly profiles based on source and destination IPs.

8.12.2. Each profile allow administrator to configure variable thresholds and actions.

8.13. NGTP profiles should be configurable on normal and heavy traffic load, NGTP should be applied per policy basis to facilitate the addition and removal of profiles.

8.14. The proposed system shall provide option to detect Gray-ware includes adware, dial, downloader, hacker tool, key-logger, RAT and spyware.

8.15. NGTP should be measured against logging being enabled for all traffic and threats.

8.16. NGTP must include a mechanism to block submitting user credentials (Username/Domain Name/Username-password) via http post messages.

8.17. NGFW must have Machine-Learning driven engine to prevent unknown files in real-time without need to perform additional dynamic analysis (aka Sanboxing)

9. High Availability Requirements

9.1. The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component

9.2. The device shall support statefull session maintenance in the event of a fail-over to a standby unit.

9.3. The device shall event log, send SNMP traps and send alert email when fail-over occurs.

9.4. High Availability feature must be supported for either Transparent (bridge) mode, Route mode or span mode.

9.5. The proposed system shall provide high availability clustering features, enables enhanced reliability and load sharing (Provides Active-Passive redundancy).

9.6. The proposed system shall support interface link monitoring failover.

9.7. The HA solutions should support automated firmware upgrade process that provides minimum downtime.

10. Log & Report Requirements

10.1 . The device shall be capable of logging with the following options:

10.1.1. memory (buffer).

10.1.2. syslog server.

10.1.3. local hard disk.

10.2 . To facilitate investigations, the logging & reporting shall be able to:

10.1.4. Provide a web based real time attack log viewer.

10.1.5. Log searching and filtering capabilities.

10.1.6. Correlate attacks logs and display top attacks information on various periods of time.

10.1.7. Collect packet logs from the NGTP device and display them real time.

10.1.8. Can operate on the box with no extra solutions or devices.

11. Application Control Requirements

11.3. The proposed system can detect, log and take actions against network traffic based on at least (2000+) application signatures.

11.4. The application signatures shall be manual or automatically updated

11.5. The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions

11.6. The administrator shall be able to set the Session TTL, apply traffic shaping of the selected application/group.

11.7. The proposed system shall maintain statistics on any application that is already defined in the application DB.

12. SSL content scanning and inspection Requirements

12.3. The solution should be able to detect and classify evasive and encrypted applications traffic whether by decryption; decoding and signature based, and take actions based on this classification.

12.4. The solution should have dedicated module for decryption with dedicated physical resources like ram and processor socket, not Virtual CPU like core (X), as a clear hardware separation not by OS, software or any commands

12.5. The proposed system shall perform SSL Inspection

12.6. The proposed system shall support SSL 3.0, TLS 1.0, and TLS 1.2.

12.7. The proposed system shall support certificate key size of 1024, 2048 bits.

12.8. The proposed system shall support Inbound and outbound inspection

12.9. The proposed system shall support SSH decryption

12.10. The proposed system shall have the ability intercept and inspect content of SSL encrypted traffic of the following protocols:

12.10.1. HTTPS

12.10.2. IMAPS

12.10.3. POP3S

12.10.4. SMTPS

12.10.5. SSH

12.11. The proposed system shall be able to perform the following tasks over SSL encrypted traffic:

12.11.1. AV Scanning

12.11.2. Web content Filtering

12.11.3. IPS

12.11.4. Anti-spyware

13. Throughput and licenses

14.1. The appliance must be able to handle traffic of at least (2.0) Gbps of NGTP throughput described in section 8.

شروط خاصة:

1- تلتزم الشركة الموردة بتدريب 3 موظفين مختصين من مركز الحاسوب وتكنولوجيا المعلومات تدريباً فنياً حسب الاصول.