بسم الله الرحمن الرحيم

ތަކެތި ސަޕްލައިކުރުން ބާރުވެ

ގާނޫ،

ދިވެހިރާއްޖެ

ބާރުވެ (IUL)32-A2-PR/1/2020/22 (20 ސެޕްޓެމްބަރ 2020) ތާރީޚުގައި ކުށްވެރިކަން ސާބިތުކުރުމަށް ގާނޫނީ ކަންކަމުގެ ދާއިރާގެ ކަންތައްތަކާ ގުޅޭ ސާފުކުރަންޖެހޭ ކަންތައްތަކަށް ބަލައި ދެ ފަރާތުގެ ހާޒިރުވުން ބޭނުންވާ ކަމަށް ބަލައި ކުށްވެރިކަމުގެ ދާއިރާގެ ކަންތައްތަކާ ގުޅޭ ސާފުކުރަންޖެހޭ ކަންތައްތަކަށް ބަލައި ދެ ފަރާތުގެ ހާޒިރުވުން ބޭނުންވާ ކަމަށް ބަލައި

- ދިވެހިރާއްޖެ ތަކެތި ސަޕްލައިކުރުމުގެ ގާނޫނުގެ 01 ނޮވެމްބަރ 2020 ވ ވަނަ ގާނޫނުގެ ދަށުން 11:00 ގައި.

- ދަނޑުވަޅުގެ ތަފްޞީލް

Base Firewall Features
General Management
Firewall Throughput (Mbps) - 28
IPS Throughput (Mbps) - 4
IPsec VPN (Mbps) - 1.8
NGFW Throughput (Mbps) - 3
Ethernet interfaces - minimum 6 GbE copper
minimum one expansion slot for future requirement
Purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators
Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN
Advanced trouble-shooting tools in GUI (e.g. Packet Capture)
High Availability (HA) support clustering two devices in active-active or active-passive mode.
Full command-line-interface (CLI) accessible from GUI
Role-based administration
Automated firmware update notification with easy automated update process and roll-back features
Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers
Jumbo Frame Support
Self-service user portal
Configuration change tracking
Flexible device access control for services by zones
Email or SNMP trap notification options
SNMPv3 and NetFlow support
Central management support via Signal Management Console
Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
API for 3rd party integration
Interface renaming
Cloud-based license management
Firewall, Networking & Routing
Stateful deep packet inspection firewall
User, group, time, or network-based policies
Access time polices per user/group
Enforce policy across zones, networks, or by service type
Zone isolation and zone-based policy support
Default zones for LAN, WAN, DMZ, LOCAL, VPN and WIFI
Custom zones on LAN or DMZ

Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule
Flood protection: DoS, DDoS and portscan blocking
Country blocking by geo-IP
Routing: static, multicast (PIM-SM), and dynamic (RIP, BGP, OSPF)
Upstream proxy support
Protocol independent multicast routing with IGMP snooping
Bridging with STP support and ARP broadcast forwarding
VLAN DHCP support and tagging
VLAN bridge support
WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules
Wireless WAN support (n/a in virtual deployments)
802.3ad interface link aggregation
Full configuration of DNS, DHCP and NTP
Dynamic DNS (DDNS)
IPv6 Ready Logo Program Approval Certification
IPv6 tunneling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec
Base Traffic Shaping & Quotas
Flexible network or user based traffic shaping (QoS) (enhanced Web and App traffic shaping options included with the Web Protection subscription)
Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical
Real-time VoIP optimization
DSCP marking
Secure Wireless
minimum throughput - 800 Mbps
Simple plug-and-play deployment of wireless access points (APs) — automatically appear on the firewall control center
Central monitoring and management of APs and wireless clients through the built-in wireless controller
Bridge APs to LAN, VLAN, or a separate zone with client isolation options
Multiple SSID support per radio including hidden SSIDs
Support for the latest security and encryption standards including WPA2 Personal and Enterprise
Channel width selection option
Support for IEEE 802.1X (RADIUS authentication) with primary and secondary server support
Support for 802.11r (fast transition)
Hotspot support for (custom) vouchers, password of the day, or T&C acceptance
Wireless guest Internet access with walled garden options
Time-based wireless network access
Wireless repeating and bridging meshed network mode with supported Aps
Automatic channel selection background optimization
Support for HTTPS login
Authentication
Share currently logged in Active Directory user ID between endpoints and the firewall without an agent on the AD server or client
Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
Single sign-on: Active directory, eDirectory, RADIUS Accounting
Client authentication agents for Windows, Mac OS X, Linux 32/64
Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos
Browser Captive Portal
Authentication certificates for iOS and Android
Authentication services for IPSec, SSL, L2TP, PPTP
Google Chromebook authentication support for environments with Active Directory and Google G Suite
API-based authentication
User Self-Service Portal
Download SSL remote access client (Windows) and configuration files (other OS)
Hotspot access information
Change user name and password
View personal internet usage
Access quarantined messages and manage user-based block/allow sender lists (requires Email Protection)

Base VPN Options
Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
L2TP and PPTP
Route-based VPN
Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Android VPN client support
IKEv2 Support
SSL client for Windows and configuration download via user portal
IPSec VPN Client
Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH
Intelligent split-tunneling for optimum traffic routing
NAT-traversal support
Client-monitor for graphical overview of connection status
Mac and Windows Support
Network Protection Subscription
Intrusion Prevention (IPS)
High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection
Top rated by NSS Labs
Thousands of signatures
Granular category selection
Support for custom IPS signatures
IPS Policy Smart Filters enable dynamic policies that automatically update as new patterns are added
ATP
Advanced Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
Lateral Movement Protection further isolates compromised systems by having healthy -managed endpoints reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain
Remote Site Manage Device VPN
minimum throughput - 200 Mbps
Minimum Interface - 4 x 10/100/1000 Base--TX (1 GbE Copper)
USB Port - 2 x USB 3.0
Modular Bay - for use with optional Wi-Fi OR 4G/LTE Card
Optional Wi-Fi Module - 802.11 a/b/g/n/ac Wave 1 (Wi-Fi 5) dual-band capable 2x2 MIMO 2 antennas
Power Redundancy Support
Central management of all remote site devices
No configuration: Automatically connects through a cloud-based provisioning service
Secure encrypted tunnel using digital X.509 certificates and AES 256-bit encryption
Virtual Ethernet for reliable transfer of all traffic between locations
IP address management with centrally defined DHCP and DNS Server configuration
Compression of tunnel traffic
VLAN port configuration options (RED 50)
Clientless VPN
Encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC
Web Protection Subscription
Web Protection and Control
Fully transparent proxy for anti-malware and web-filtering
Enhanced Advanced Threat Protection
URL Filter database with millions of sites across maximum categories backed by OEMLabs
Surfing quota time policies per user/group
Access time polices per user/group
Malware scanning: block all forms of viruses, web malware, trojans and spyware on HTTP/S, FTP and web-based email
Advanced web malware protection with JavaScript emulation
Live Protection real-time in-the-cloud lookups for the latest threat intelligence
Second independent malware detection engine for dual-scanning
Real-time or batch mode scanning
Pharming Protection

HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions
SSL protocol tunneling detection and enforcement
Certificate validation
High performance web content caching
File type filtering by mime-type, extension and active content types (e.g. ActiveX, applets, cookies, etc.)
Safe Search enforcement (DNS-based) for major search engines per policy (user/group)
Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload customs lists
Block Potentially Unwanted Applications (PUAs)
Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users
User/Group policy enforcement on Google Chromebooks
Cloud Application Visibility
Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated
Discover Shadow IT at a glance
Drill down to obtain details on users, traffic, and data
One-click access to traffic shaping policies
Filter cloud application usage by category or volume
Detailed customizable cloud application usage report for full historical reporting
Application Protection and Control
Automatically, identify, classify, and control all unknown Windows and Mac applications on the network
Signature-based application control with patterns for thousands of applications
Cloud Application Visibility and Control to discover Shadow IT
App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added
Micro app discovery and control
Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g. P2P), and risk level
Per-user or network rule application control policy enforcement
Web & App Traffic Shaping
Custom traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared
Central Firewall Reporting
Pre-defined reports with flexible customization options
Reporting for Firewalls (hardware, software, virtual, and cloud)
Intuitive user interface provides graphical representation of data
Report dashboard provides an at-a-glance view of events over the past 24 hours
Easily identify network activities, trends, and potential attacks
Easy backup of logs with quick retrieval for audit needs
Simplified deployment without the need for technical expertise
Warranty and Support – 1 Year
Hardware warranty & RMA
24x7 Support via Telephone & Email with Remote Consultation from STSE (up to 4 hrs)
FREE Security Updates & Patches
FREE Software Features Updates & Upgrades
Security Subscriptions - 1 Year
Base Firewall with VPN, Routing, WAN Link Load Balancing, Traffic Shaping & Quota, Wireless, Authentication, etc
Network Protection Subscriptions (IPS, RED/HTML5, ATP, Anti-malware),
Web Protection Subscriptions (URL, AppCtrl, Web/App Traffic Shaping),
Others

Implementation should be done by Certified Engineers (Please include Certificates)
Project Plan should be provided with the Proposal
History of similar projects undertaken with customer letters should be provided
Should offer Certified Training for 3 Staff

ތަންފީޒުކުރާނެ ގޮތާ ގުޅޭ ލިބޭނެ ގުނަކަށް ލަފާދޭ ގޮތް:

- ތަންފީޒު ކުރުން
- ތަންފީޒު ކުރުމުގެ ދަށްދެނެ ލިބޭ ތަނުގެ ލިސްޓް
- ފެށުމުގެ ތަން ބަލައިގަތުމުގެ ގޮތް
- ނިމުމުގެ ތަން ބަލައިގަތުމުގެ ގޮތް
- ގެނައި ބަދަލުތައް ބަލާ ގޮތް
- ބަދަލު ދިނުމާ ގުޅޭ ގޮތް (ބަދަލުގައި ދެވޭ ތަކެތި)
- ގާތްކަމުގެ ވަރަށް ބަލާ ގޮތް (ތަކެތި ގާތްކަމުގެ ވަރަށް ބަލާ ގޮތް)
- ގާތްކަމުގެ ވަރަށް ބަލާ ގޮތް (ތަކެތި ގާތްކަމުގެ ވަރަށް ބަލާ ގޮތް)
- ދަށުން ކަނޑައަޅާ ގޮތަށް ތަކެތި ގެނައުމުގެ ކުރިން ކުރަންޖެހޭ ކަންތައް (ތަކެތި ގެނައުމުގެ ކުރިން ދަށުން ކަނޑައަޅާ ގޮތަށް ކުރަންޖެހޭ ކަންތައް، ތަކެތި ގެނައުމުގެ ކުރިން ކުރަންޖެހޭ ކަންތައް)
- ދަތުރުގައި ހިނގާ ތަކެތި ތަންފީޒު ކުރުމާ ގުޅޭ ގޮތް ތަކެތި ތަންފީޒު ކުރުމުގެ ދަށްދެނެ ކުރަންޖެހޭ ކަންތައް ކަނޑައަޅާ ގޮތް ތަކެތި ތަންފީޒު ކުރުމުގެ ދަށްދެނެ ކުރަންޖެހޭ ކަންތައް ކަނޑައަޅާ ގޮތް.

ދަށުން ކަނޑައަޅާ ގޮތަށް ތަކެތި ގެނައުމުގެ ކުރިން ކުރަންޖެހޭ ކަންތައް ބަލާ ގޮތް:

ދަށުން ކަނޑައަޅާ ގޮތަށް ތަކެތި ގެނައުމުގެ ކުރިން ކުރަންޖެހޭ ކަންތައް ބަލާ ގޮތް ތަކެތި ގެނައުމުގެ ކުރިން ދަށުން ކަނޑައަޅާ ގޮތަށް ކުރަންޖެހޭ ކަންތައް ކަނޑައަޅާ ގޮތް.

ދަށުން ކަނޑައަޅާ ގޮތް 50 (ފަންސާސް) ޕާސެންޓް:

ދަށުން ކަނޑައަޅާ ގޮތް ޕާސެންޓް ތަކެތި ގެނައުމުގެ ކުރިން ކުރަންޖެހޭ ކަންތައް ކުރަން ފެށުމުގެ ކުރިން ކުރަންޖެހޭ ކަންތައް ކަނޑައަޅާ ގޮތް.

- **ތަކެތި (ކުރަންވާ ތަކެތި ހުރިހާ ތަކެތި / ކުރަންވާ ތަކެތި ގަނެފައި ތަކެތި × 50)**

ދަށުން ކަނޑައަޅާ ގޮތް 20 (ވިހި) ޕާސެންޓް:

ދަށުން ކަނޑައަޅާ ގޮތް ޕާސެންޓް ތަކެތި ގެނައުމުގެ ކުރިން ކުރަންޖެހޭ ކަންތައް ކަނޑައަޅާ ގޮތް ދަށުން ކަނޑައަޅާ ގޮތް ތަކެތި ގެނައުމުގެ ކުރިން ކުރަންޖެހޭ ކަންތައް ކަނޑައަޅާ ގޮތް.

- **ދަށުން ކަނޑައަޅާ ގޮތް (ތަކެތި ގެނައި ގޮތް ކުރަންވާ ތަކެތި ގެނައި ގޮތް / ކުރަންވާ ގޮތް ދަށުން ކަނޑައަޅާ ގޮތް × 20)**

ގަތުމުގެ ގޮތުގެ ޕާސެންޓް 20 (ވިހި) ޕާސެންޓް:

ސަރުވިސް ގެނައުމުގެ ޕާސެންޓް ތަކެތި ގެނައުމުގެ ކުރިން ކުރަންޖެހޭ ގަތުމުގެ ގޮތް ބެލުމުގެ ކުރިން ތަކެތި ގެނައުމުގެ ކުރިން ކުރަންޖެހޭ ކަންތައް ކަނޑައަޅާ ގޮތް ތަކެތި ގެނައުމުގެ ކުރިން ކުރަންޖެހޭ ކަންތައް ކަނޑައަޅާ ގޮތް.

- ދަށުގައި ބަލައިފައި ވާ ގޮތުގެ (ހަމައެކި ގަޑުގެ ދުވަސްތަކުގެ / ތިން ދުވަހުގެ ތެރެ ދުވަސްތަކުގެ × 20)

ކުށުގެ ގޮތުގައި 10 (ދިހަ) ކުރިން:

ކުށުގެ ގޮތުގައި ކުރިން ކުށްވެރިކަމުގެ ބަދަލުގައި ކަނޑައަޅާ ދަށުގައި ބަލައިފައި ވާ ގޮތުގެ ތެރެ ކުރިން ކުށްވެރިކަމުގެ ބަދަލުގައި ދެވޭ ދުވަސްތަކުގެ ތެރެ ކުރިން ކުށްވެރިކަމުގެ ބަދަލުގައި ދެވޭ ދުވަސްތަކުގެ ތެރެ 10 ދުވަހުގެ ތެރެ. (ތ) ފަސާތުގައި ކުށްވެރިކަމުގެ ތާރީޚުގެ (ހ) ދުވަހުގެ ތެރެ 10 ދުވަހުގެ ތެރެ.

- (ހަމައެކި ގަޑުގެ ފަސާތުގެ ތާރީޚުގެ ތެރެ ފަސާތުގެ / ފަސާތުގެ ތާރީޚުގެ ތެރެ ތިން ދުވަހުގެ ތެރެ ހަމައެކި ގަޑު × 10)

ނޯޓް: ދިވެހިރާއްޖެ ތެލިފޯނު ކޯޕަރޭޝަން 7764222 ނަންބަރަށް ތިން ދުވަހުގެ ތެރެ ގުޅުއްވުން ކަނޑައަޅާ.

20 ފެބްރުވަރީ 2020