SD-WAN Security Features

3 Tiers of built in SD-WAN Firewall Service
(Stateful Firewall, Next Gen Firewall, and Next Gen Firewall with UTM)

SD-Wan Firewall & Features	Firewall & Feature Tiers		
Features & Functions	**Stateful FW**	**NGFW**	**UTM**
SD-Wan Network Analytics	X	X	X
Network Report Generation	X	X	X
Dynamic Path Control	X	X	X
IPSec Encryption	X	X	X
Application Traffic Load Balancing	X	X	X
Forward Error Correction	X	X	X
Standard Dynamic IGP/BGP & Static Routing Protocols	X	X	X
MPLS Layer-3 VPN with QoS	X	X	X
QoS Settings	X	X	X
Policy-Based Application Forwarding & Routing	X	X	X
Out-of-Box Indentification of 2600+ Applications	X	X	X
Per Flow Application Logs	X	X	X
Built in Stateful Firewall	X	X	X
DDos		X	X
Application Control		X	X
User/Group Definition & Control		X	X
SSL Inspection		X	X
Geo Location & IP Reputation Filtering		X	X
URL Classification with Web Reputation & Filtering		X	X
DNS-Based Protection & Access Control		X	X
Signature-Based File Type Identification & Filtering			X
SSL Decryption			X
Multi-Layered Anti-Virus & Anti-Malware Protection			X
Signature & Anomaly-Based IDS/IPS			X

Standard Firewall Features

(Included as default firewall feature)

Routing & QoS

- IGP: OSPF v2
- BGP: BGP v4, MP-BGP
- Static routing
- BFD for OSPF v2, MP-BGP & Static
- Policy Based Forwarding/Policy Based Routing
- VRRP
- MPLS L3 VPN
- QoS
  - Classification
  - DSCP marking
  - Adaptive rate limiting

CGNAT

- CGNAT Translation Types
  - Static & Dynamic NAT44
  - NAPT44
  - DNAT44
  - NAT Port-Forwarding
- CGNAT Features
  - Endpoint Independent Mapping (EIM)
  - Endpoint Independent Filtering (EIF)
  - Address pooling paired
  - Port parity
  - Port Block Allocation (PBA)
  - Random Port Allocation (RPA)
  - Inter tenant
- ALG support
- IPv6 tunneling
  - 6RD
  - DSLite (Dual-stack lite)

Stateful Firewall

- Zone & endpoint based stateful firewall
- Elastic policy based support
- Policy triggers
  - Based on 5 tuple flows
  - Zone/address/subnet, Geo-IP, blacklisting, domain names
  - Time of day
  - L3/L4 headers
- Triggers can be combined with other match conditions (and, or)
- Actions
  - Allow, Deny, Reject
  - QoS, Log
- Available for all policy types

– Access, QoS, PBF, DDoS, Traffic Monitoring, SD-WAN
• ALG support for various protocols

Ipsec
• Site-to-site IPSec/Concentrator
– IKEv1/v2
– Pre-shared key/PKI authentication
– Dead peer detection
– Diffie-Hellman key negotiation
– AES 128/256 encryption (IKE/IPsec)
– SHA1/SHA256/SHA384/SHA512/Null hashing
– NAT traversal
– Perfect forward secrecy
– IPsec rekey time/volume based
– Anti-replay
– Pre/post fragmentation
– Route based VPN

Application Visibility
• Identification of 2600+ applications & protocols
• Support for user-defined applications & application groups
• Per flow application logs via Syslog, IPFIX
• Support for user-defined application filters via Analytics
– Based on any combination of
– Family, Subfamily (Example, Risk, Productivity & Tag)
• Automatic application signature updates via Versa Security Package

Next-Gen Firewall Features

(Includes all previous Firewall features listed)

Application Control
• Ability to recognize & control traffic for over 2600+ applications
• Policy triggers
– Applications
– Application Groups
– Application Filters (Family/Subfamily)
• Triggers can be combined with other match conditions (and, or)
• Actions
– Allow, Deny, Reject, QoS, Log
– Packet Capture
– Apply Profile (IP Filtering, File Filtering, DNS Filtering, URL Filtering, Vulnerability, Anti-Virus)
• Available for all policy types
– Access, QoS, PBF, Traffic Monitoring, SD-WAN

• Geo Location
– IP Address database spanning multiple countries

– Enforce actions based on Geo Location
– Match based on Source IP, Destination IP or combination of both
• IP Reputation
– Protection against 12 million + malicious IP Addresses
– Both IPv4 and IPv6 Addresses
– Supports user-defined black & white lists
– Updates in near real time
– Match based on Source IP, Destination IP or combination of both
– Threat types include Windows exploits, Web attacks, Phishing, Botnets, DoS, Scanners, Anonomyzers, Spam sources & Mobile threats
• Automatic Geo & IP reputation updates via Versa Security Package

• URL Classification
– 460+ million domains and 13+ billion URLs scored & classified
• 83 predefined categories, custom & Cloud app category support
• Supports user-defined black & white lists
• Web reputation
• Real-time Cloud lookups of URL categories & URL reputation
• Policy triggers
– URL, URL category
• Triggers can be combined with other match conditions (and, or)
• Actions
– Allow, Deny, Reject, Log, QoS
– Inform, Ask, Notify, Override, Block
– Apply Profile (IP Filtering, File Filtering, DNS Filtering, URL Filtering, Vulnerability)
• Available for all policy types
– Access, QoS, PBF, Monitoring, Authentication, Decryption, SD-WAN
• Automatic URL category updates via Versa Security Package
URL Reputation & Filtering

DNS Reputation & Filtering
• DNS-based protection & access control
– Policy triggers from DNS query data
– Combined with Zones, IP Addresses, Geo-Location, User/Group, Category, Reputation
– Supports user-defined black & white lists
– Actions include Allow, Deny, Reject, Log, QoS
• Global DNS Intelligence for zero-day threats
– Passive DNS database
– Block resolution of new domains until reputation is updated
– Internal names, brand spoofing
– Recognizes potentially suspect sites
– DNS configuration errors
– Provides enhanced phishing protection
• Integration with URL Category and IP Reputation Feeds

• Directory support
– Active Directory

– LDAP
• Authentication support
– Kerberos
– Forms based via captive portal using LDAP
• Policy triggers
– User
– Group
– Attribute
• Triggers can be combined with other match conditions (and, or)
• Actions
– Allow, Deny, Reject, QoS, Log
– Apply Profile (IP Filtering, File Filtering, DNS Filtering, URL Filtering, Vulnerability, Anti-Virus)
• Available for all policy types
– Access, QoS, PBF, Monitoring, SDWAN
User/Group Control

• Security Checks
– Expired certificates
– Untrusted issuers
– Unsupported
o Ciphers
o Key Lengths
o Versions
– Restrict certificate extensions
• Actions
– Allow, Deny, Reject, Alert (allow & log)
SSL Inspection

DDoS
• Provides zone based & endpoint based protection
• Zone & DDoS profile provides protection against:
− Reconnaissance attacks
o ICMP sweep, port scanning, aggressive session aging
− Common floods
o UDP, SYN, ICMP, ICMPv6
− Packet-based attacks
o Fragmented packets, spoof protection, malformed packets, Invalid IP options
− Volume Based attacks
o Rrate and burst profile definition
o Planned evolution to support heuristics
• Support for both aggregate profiles & classified profiles
• Corresponding measures can include
– Generation of alert log,
– Exclusion of incoming packets
– Activation of flood protection mechanism

Next-Gen Firewall with UTM

(Includes all previous Firewall features listed)

•IDS/IPS Signature & anomaly-based detection/prevention
• Extensive coverage over the last 10 years
• Vulnerability signatures & anomaly detection engine
– Provides real-time protection
• Additional coverage for vulnerabilities disclosed
– Part of Microsoft Tuesday
• Support for PCN/SCADA signatures (modbus, dnp3)
• Support for Snort rule format
• Support for custom/user-defined vulnerability signatures
• Automatic signatures updates via Versa Security Package

• Anti-Virus/Anit-Malware
– Heuristics
– Emulation
– Signatures
• Detection on HTTP, FTP, SMTP, POP3, IMAP, MAPI
• Cloud detection integration
• Automatic engine & signature updates via Versa Security Package
Anti-Virus

SSL Decryption
• End-to-end SSL security
– Decrypt
– Inspect
– Encrypt
• Traffic Visibility
– Decrypt outbound & inbound SSL traffic transparently
– Inspect the decrypted traffic for threats
– Re-encrypt to both client & server
• Decrypt policy based by IP/Zone, User/Group, URL host or URL host category

File Filtering
• Signature-based file type identification
• Application, file type, direction & size-based filtering
• Reputation based filtering support
• Supports user-defined black & white lists
• File transfer detection on HTTP, FTP, SMTP, POP3, IMAP, MAPI
• Automatic file type updates via Versa Security Package