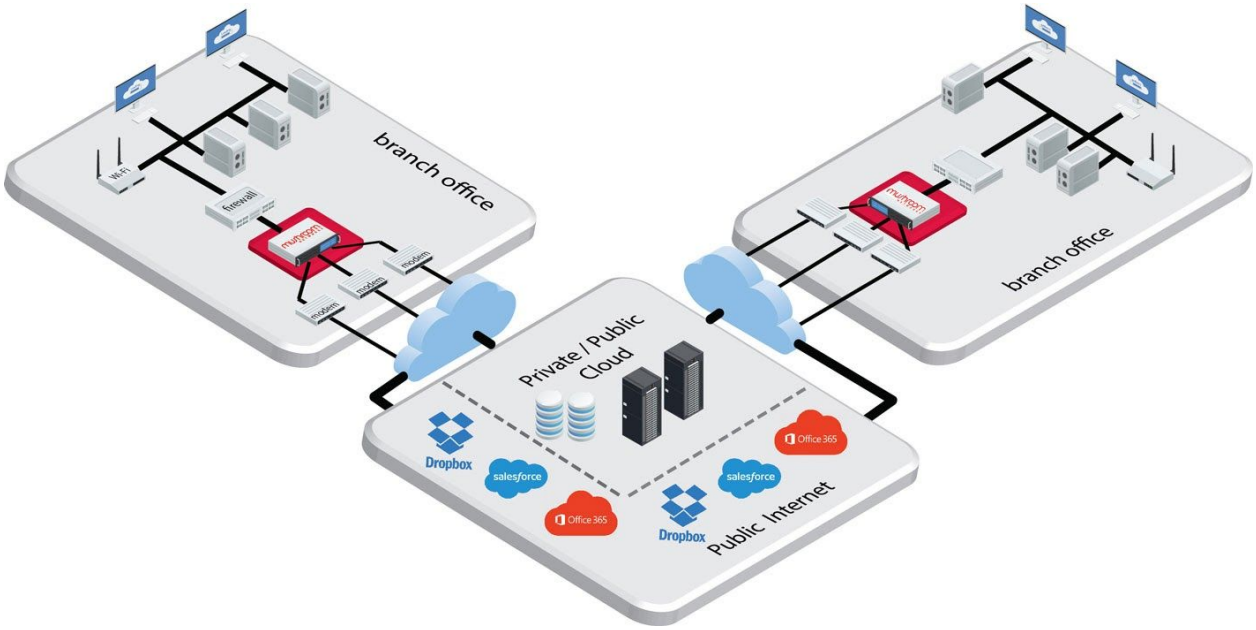
Mushroom Networks Security

Mushroom Networks SD-WAN network architecture leverages overlay tunnels between branch office Mushroom Networks CPE devices and Mushroom Networks cloud-based or premises-based relays. The overlay tunnels facilitate high-performance and fault tolerant inter-office connectivity as well as connectivity to private and/or public clouds. Mushroom Networks uses a variety of cipher suites to maintain the authenticity, integrity and the confidentiality of the data flowing over the overlay tunnels.

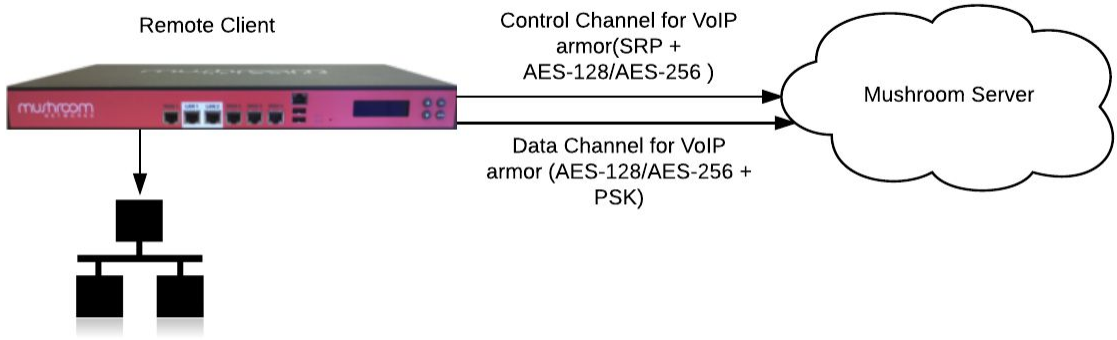


Security of Overlay Tunnels

Mushroom Networks SD-WAN tunnels facilitate the ability to exclusively use the Cloud IP addresses for all traffic. This therefore provides the ability to obfuscate the local IP addresses provided by ISPs (or to freely change/refresh local IP addresses without disrupting any services) adding another level of DDoS protection.

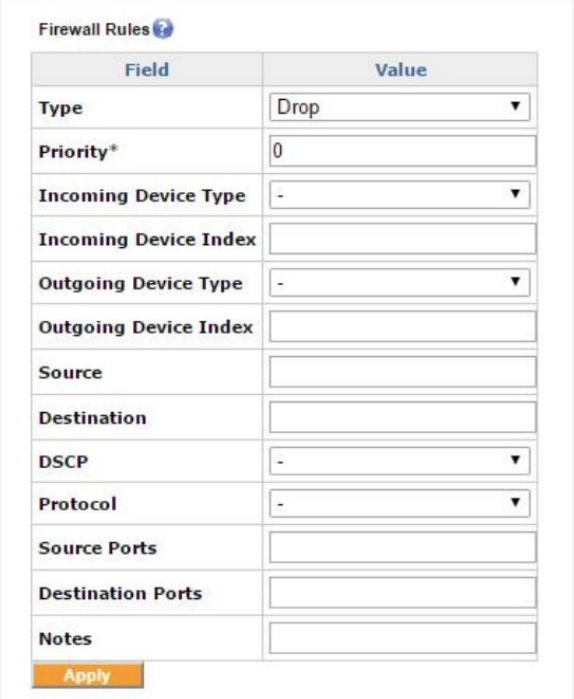
Mushroom Networks appliances connect to the Mushroom Networks operated Cloud Relays using multi-path overlay tunnels that support AES-128 and AES-256 encryption to protect against eavesdropping, tampering and message forgery, and leverage TLS 1.2 with SRP (Secure Remote Password) protocol authentication with protection against dictionary attacks. Similarly, when on-premises relays are used instead of Mushroom Networks operated Cloud Relays, the same TLS 1.2 with SRP protocol authentication is used.

Cloud Relays are based on a secure network architecture with strict traffic flow policies. Comprehensive monitoring of inbound and outbound communications is done to detect threats such as Denial of Service (DoS), Distributed Denial of Service (DDoS), flooding, software/logic attacks, Man in the Middle (MITM) attacks, IP spoofing, port scanning and packet sniffing. Additionally, redundant telecommunication providers as well as additional capacity protect against the possibility of DoS attacks.



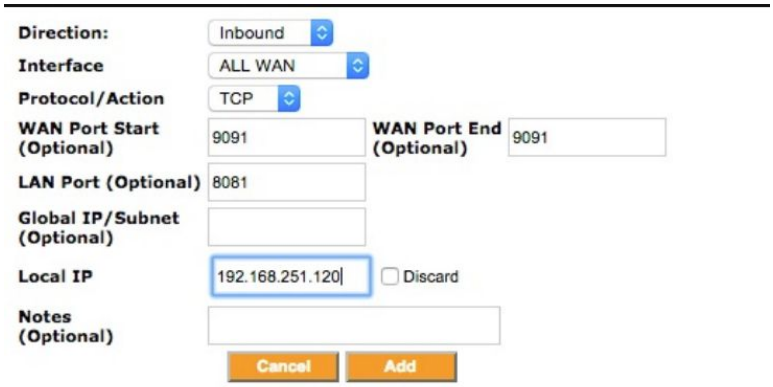
Stateful Firewall with Packet Filtering

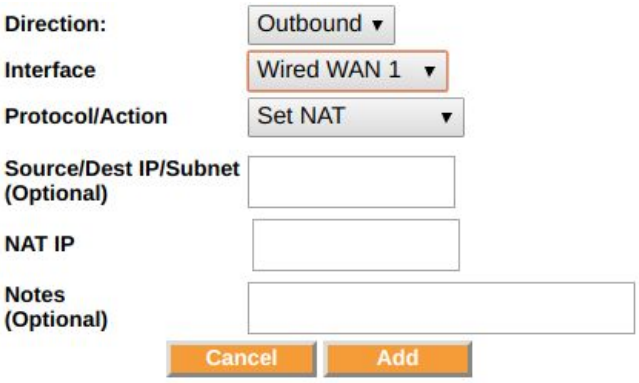
Traffic can be allowed or denied based on filters based on layer3 to layer7 traffic characteristics and the state of the sessions.



Port forwarding and NAT functionality

Inbound port forwarding and outbound NAT (one-to-one and many-to-one) is supported. By default all inbound ports are blocked and any outgoing traffic from the device is allowed.





Device Management and Authentication Options

Device Management is done by using a web-based HTTPS connection authenticated with password credentials. Additionally, TACACS+ authentication can also be used for remote user access authentication and management. Multiple user access profiles can be created to manage the device with different privileges.

Alerts and Reporting Capabilities

Mushroom Networks supports Syslog/SNMP and traps/Netflow/email for alerting and reporting. Additionally, Mushroom Networks monitoring portal facilitates a web-based dashboard of real-time and

historic data collected from various Mushroom Networks CPE devices. Email alerts can be configured with various threshold triggers.

Netflow is also supported. Attached below is the Netflow configuration user interface:

Built-in Troubleshooting and Analysis Tools

Mushroom Networks devices support various diagnostics and packet-capture tools such as ping, traceroute, tcpdump, iperf3, etc. Here are a few examples of using these tools from the command line interface:

ping - send ICMP ECHO_REQUEST to network hosts
for quick command summary or full documentation:
ping -h or man ping
to ping a device over a specific interface:
ping <IP address> -I <interface>
ping 10.10.2.2 -I eth2

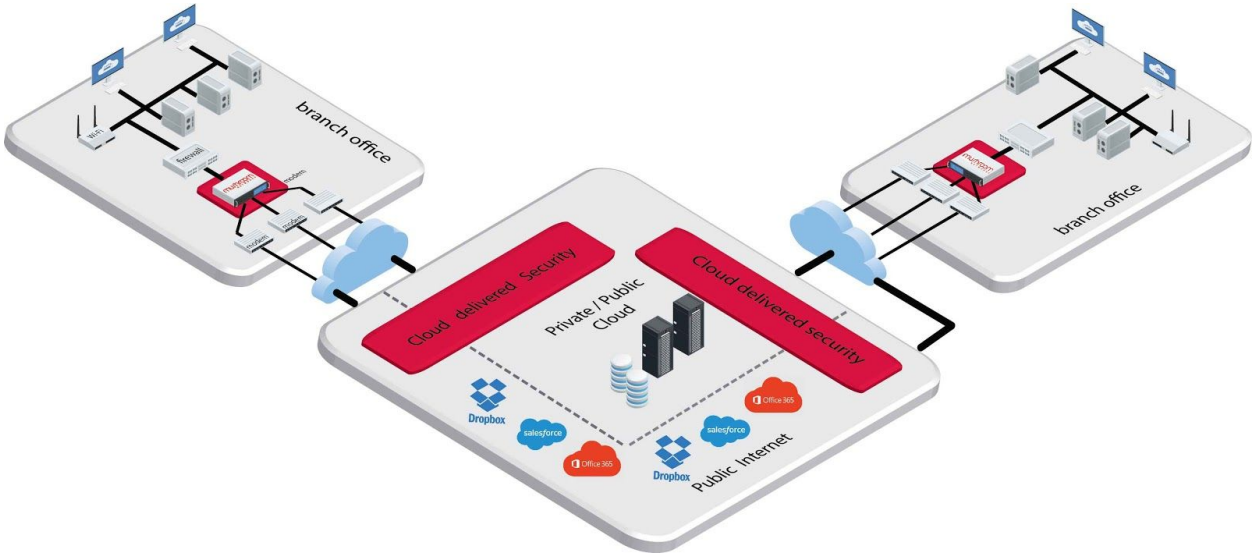
tcpdump - dump traffic on a network
for quick command summary or full documentation:
tcpdump --help or man tcpdump
to see all available interfaces that tcpdump can monitor:
tcpdump -D
for example, to monitor SIP traffic on default port 5060 using eth0:
tcpdump -i eth0 port 5060
to monitor telnet traffic on default port 23 using eth0:
tcpdump -i eth0 port 23
typical full command to monitor traffic to/from given host, suppress DNS resolution, only view a specific interface, and only capture 50 packets and then exit::
tcpdump -n -i eth2 host 10.10.2.2 -c 50

traceroute - print the route packets trace to network host
for quick command summary or full documentation:
traceroute --help or man traceroute

typical full command to find the route taken to an internet host, suppressing DNS resolution, over a specific interface, using ICMP:
traceroute -n -I -i eth2 google.com

Cloud-delivered Security

Cloud delivered Next Generation FireWall (NGFW) and Unified Threat Management (UTM) services are available as VNF (Virtual Network Function) services that can be service-chained to the Mushroom Networks Cloud Relay. With Mushroom Networks cloud delivered NGFW and UTM services, all the work is done in the cloud. Office networks are connected to Mushroom Networks Cloud Relays with the secure encrypted tunnels and the security functions are delivered from the cloud. The Core Security Suite and Advanced Security Suites described below are available as additional add-ons.



CORE SECURITY SUITE

- **Intrusion Prevention**: IPS (Intrusion Prevention System) inspects your packets in real-time to identify known threats and malicious activities including SQL injection, spyware, buffer overflows and cross-site scripting from hourly updated new threat signatures.
- **Reputation based Threat Mitigation**: Botnets and bad reputation URLs that are on various reputation lists that are dynamically updated on an on-going basis are instantly blocked, before they can become a threat to your network.
- **Web Content Filtering**: With more than 100 types of content groups for http and https, allow or restrict URLs to block unwanted traffic in the cloud before it reaches your local network.
- **Gateway AntiVirus**: Protects against known viruses, trojans, spyware, rogueware and worms with multi-layered signature-based and behavioral-based scanning. The signature set is dynamically updated and it leverages Machine Learning models.

COMPLETE SECURITY SUITE ADDS

- **Persistent Threat Blocker**: Provides cloud based sandboxing of advanced persistent threats such as ransomware, zero-day threats and evolving malware that are designed to bypass traditional network security.
- **Data Loss Prevention**: Protects confidential data transmission over email, web and FTP for over 30 file types with the built-in library of over 200 rules and compliance mandates such as PCI DSS and HIPAA and others for 18 countries.
- **Network Mapping**: Detect all unauthorized hosts connected to your network with information such as OS version, open ports and protocols.
- **DNS Inspector**: Scans DNS requests and filters against a list of known malicious DNS Sites. If the site is malicious, blocks access and warns users.
- **Application Control**: Ability to block, allow or restrict over 1,700 applications with granular policies such as bandwidth throttles and per user/group/schedule policies in the cloud before it reaches your local network.
- **AntiSpam**: State of the art real-time protection against spam and phishing attempts.
- **Intelligent AntiVirus**: Protects against evolving zero day malware without requiring signatures but instead leverages Machine Learning based algorithms.
- **Threat Detect & Respond**: Advanced algorithms correlate network and endpoint security events to detect and stop malware attacks.

Mushroom Networks Software Security

Mushroom Networks firmware is based on Debian Linux operating system and has a customized kernel and modules. The Mushroom Networks firmware releases use semantic versioning where upgradability, downgradability, and bug fixes are provided. The ability to upgrade and downgrade to newer or older versions is maintained for around a decade. Any major operating system security updates are monitored and are patched immediately with a maintenance release.