MANAGED SOLUTIONS

Fact Sheet

CROWN CASTLE

Next-Generation Firewall

Today's fast evolving cyber threat landscape requires comprehensive, advanced protection that legacy firewalls with rigid and reactive architectures can't offer. And though traditional edge firewalls are often anchored to physical sites, you need the same level of robust protection regardless of where you connect from—branch office, headquarters, home office or on the road.

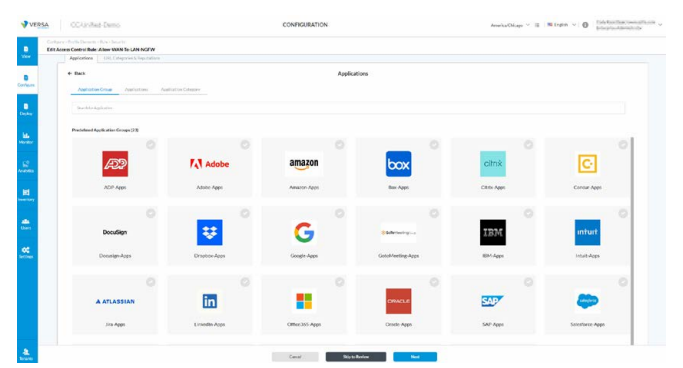
Our next-generation firewall (NGFW) is a value-added feature that can enhance your Managed SD-WAN solution and accelerate your digital transformation by providing comprehensive security in a single, scalable platform to address the most complex needs. It delivers advanced application layer capabilities to protect against the most evasive threats across your entire network, all within a single platform for networking, security, threat prevention and centralized management. NGFW uniquely classifies and protects your inbound and outbound traffic—regardless of user, type of device or location—to enhance security posture, improve application availability and enhance user experience.

Key Service Capabilities

NGFW provides comprehensive network security with zero trust based secure access, IoT/OT security and device fingerprinting, URL filtering, next-generation intrusion prevention and advanced security capabilities. NGFW also offers flexible deployment options including:

- On-premises, on bare-metal appliances
- In private data centers in virtualized form factor
- In popular public cloud environments such as AWS, Azure and Google Cloud Platform

Our NGFW can be added to your Managed SD-WAN solution to securely connect users and devices in enterprise branches to applications in or near any of the outlined deployment options. It provides single pane-of-glass management and visibility, with high availability options—active/active and active/passive modes—to ensure business continuity.



NGFW applications in the Versa Concerto Portal

Application aware, resilient network security

Our NGFW identifies all applications across all ports with features including layer 7 deep packet inspection (DPI), URL, protocol and port numbers, destination IP addresses and more, combined with comprehensive policy-based control. Built-in support for DoS (denial of service) protection, CGNAT (carrier grade NAT) and ALG (application layer gateway) ensures scalability and security.

User authentication and user/group level policies

NGFW provides built-in user and group-based access control capabilities. The operating system can integrate with popular identity providers (IdPs) to authenticate users, perform MFA (multi-factor authentication) and obtain user and group information to apply security and access controls. Conditional access policies can be defined for different classes of users like executives, guests, employees and contractors.

We also provide a centralized broker to help authenticate users in passive or in proactive forms, creating a seamless user experience by eliminating the need for repetitive authentication.

And when inline user authentication capabilities are not deployed, the captive portal can authenticate users and manage access control based on user identity.

DNS proxy and DNS security

DNS proxy

Using the information learned from authoritative DNS servers, as well as through DNS reputation feeds, the DNS proxy secures DNS entries and prevents traffic from getting to untrusted, unknown or malicious sites known to work as command and control (C&C) centers for attackers.

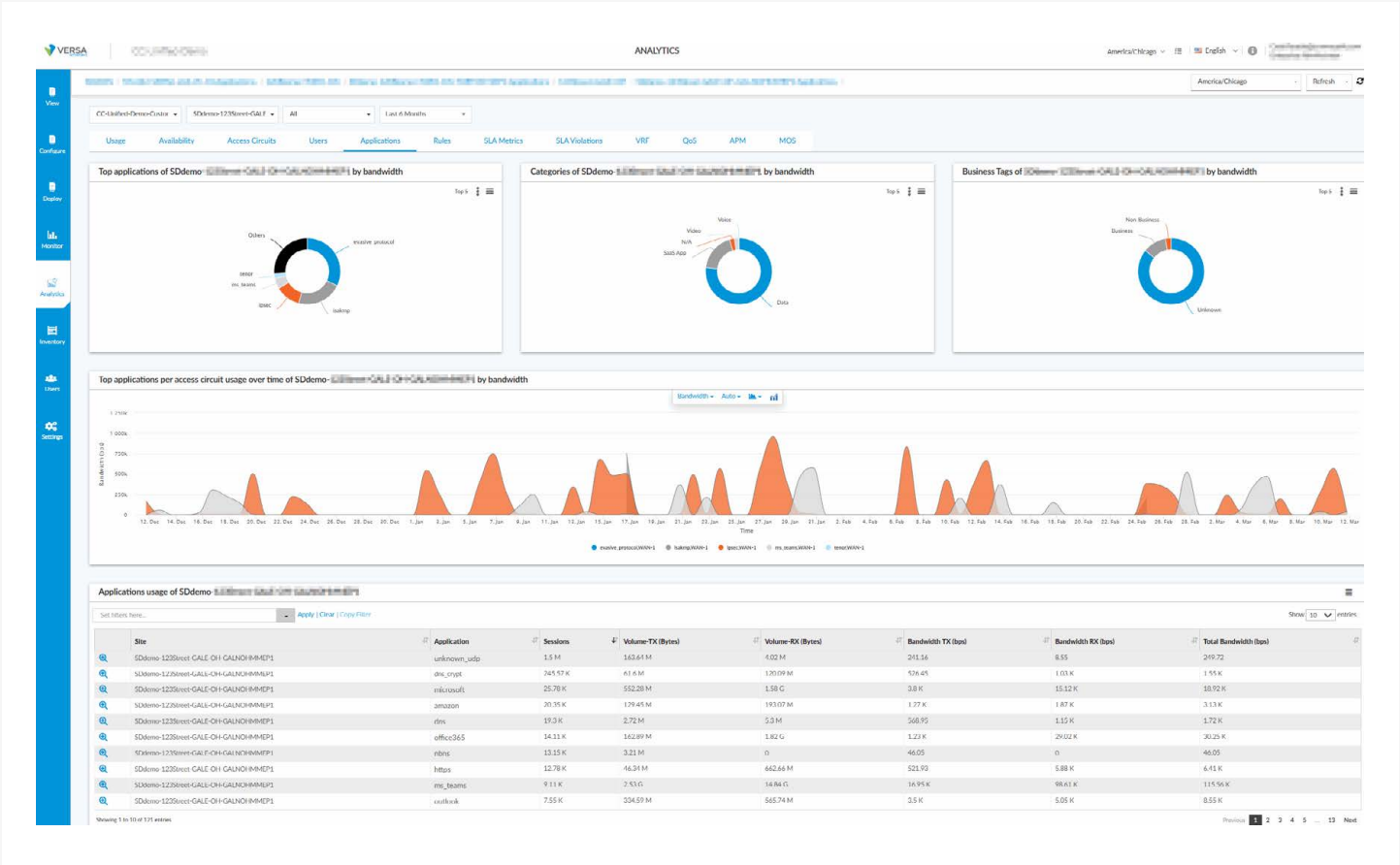
DNS security and filtering

Provided at the DNS layer, we secure the network and users from DNS hijacking, DNS based attacks, DNS reflection attacks, amplification attacks, phishing attacks, malware, ransomware and botnets. We also block access to compromised websites. DNS security uses global DNS threat intelligence gathered from hundreds of sensors across the globe to block resolution of new domains until reputation is updated. DNS reputation feeds are then used to keep this database up to date.

URL and IP reputation, categorization and filtering

NGFW provides a rich set of URL and IP categorization and filtering capabilities in 80+ URL categories to allow safe browsing while blocking malicious sites. The URLs are ranked by reputation, risk and trustworthiness. In addition to predefined classes, we provide support for user-defined and custom classes that can be created and managed as needed. Hundreds of millions of domains and more than 13 billion URLs are scored and classified for maximum threat coverage. Additional features include:

- 80+ predefined URL categories including generative AI, ways to improve employee productivity, inappropriate sites and bandwidth management including voice and video sites
- URL database is updated periodically via security package updates without the need for operating system or software upgrades
- Real-time cloud lookups of URL categories for those uncategorized in the operating system cache
- Custom URL categories based on regular expressions (Regex) and/or fixed string match
- Customizable captive portal screens for policy enforcement and redirection
- Support for block, inform, ask, justify, override and authenticate pages



Analytics showing top applications and URL categories

TLS/SSL proxy

The TLS/SSL proxy protects you from threats hidden in encrypted traffic by breaking open and inspecting TLS/SSL traffic and applying additional security policies for threat and data protection. It directs encrypted traffic based on application signatures and scans encrypted content for malware and exploit prevention all while detecting and preventing data leaks. The proxy also provides support for transparent or split-proxy modes in TLS versions 1.0, 1.1, 1.2 and 1.3.

For organizations requiring higher levels of security, TLS 1.3 provides enhancements that help ensure the confidentiality and integrity of communication. Perfect forward secrecy (PFS) then use specific ephemeral keys to alleviate any confidentiality concerns. By generating a unique key for every session, even the compromise of a single session key will not affect any data other than that exchanged in the specific session protected by that particular key. Knowing the private key of the server no longer allows decrypting of the session.

Parts of the handshake (the server certificate values such as CName and/or SAN) are encrypted. This prevents malicious third parties—that rely on examining server certificates—from eavesdropping on the connection.

Hardened security stack and operating system

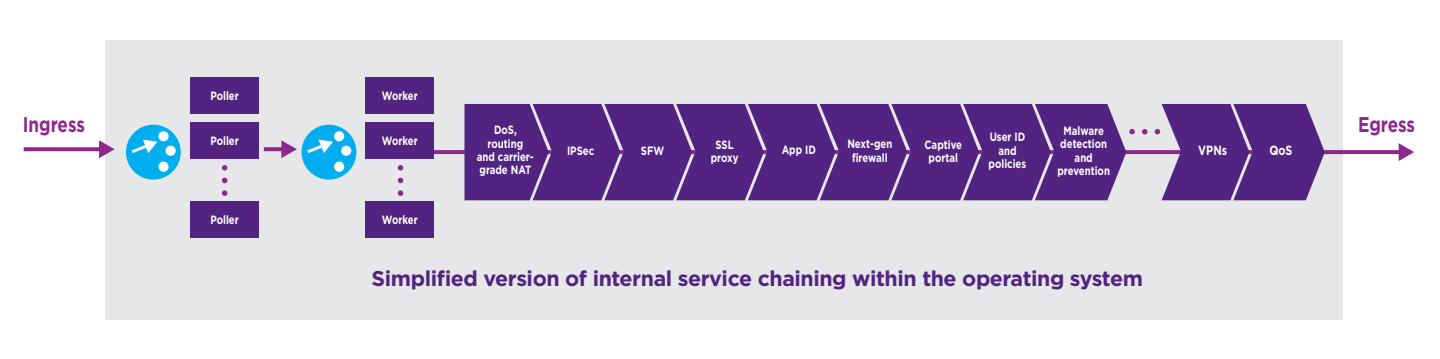
Our operating system is a hardened OS. This includes installation of the required minimal set of packages, use of signed binaries, rules for administrator password, privileged access management, password safe storage and boot loader protection. Our hardened security stack and operating system are verified and audited periodically with release updates.

Genuine multi-tenancy

Our NGFW provides genuine multi-tenancy across our orchestration platforms, control plane and data plane. This level of multi-tenancy isolates the policies, configuration, logs and statistics of every tenant, and keeps them segregated from the other tenants. This ensures enhanced security and high performance for each tenant.

Scalable single-pass architecture

The operating system is based on a single pass, scalable architecture that makes it fast and easy to deploy NGFW from tens to thousands of locations, providing consistent policies across each location. This removes the burdens of limited visibility, high incident response time, manual configuration, troubleshooting and unmanageable alerts.



Our single pass architecture

NGFW Additional Features

User and Group Level Traffic Control for Managed SD-WAN
User and group-based policies with support for active directory and lightweight directory access protocol (LDAP)
Kerberos, captive portal form, OAuth and SAML service provider support
SD-WAN QoS control support by user ID and group
SD-WAN traffic engineering policy control support by user ID and group
SD-WAN L7 SLA policy-based traffic engineering by user ID and group
DNS Proxy and Security
DNS forwarder
DNS split proxy
DNS proxy
DNS proxy for IPv6
DNS filtering
Next-generation (L7) Firewall
L7 application-based policies
Application triggers (family and sub family, risk, productivity, tags)
Network Access Control
User and group-based policies with support for active directory and LDAP
Kerberos, captive portal form, OAuth and SAML service provider support
802.1x with RADIUS back-end
802.1x certificate and MAC-based access control
Policy trigger support by user ID and group

Forward Proxy
DIA/DCA use case coverage
SSL-TLS proxy
Security service chaining
URL, Content Filtering and Captive Portal
Predefined/user defined categories and actions
Whitelist and blacklist
Search patterns and strings
Web reputation feeds
Reputation/category-based actions and captive portal
URL filter based captive portal with a rich set of actions
Intelligent path selection based on URL category
Custom action messages
IPv6 support (URL identification and traffic engineering)
IPv6 support (categorization and reputation)

Why Crown Castle?

Our unique, nationwide portfolio
With approximately 90,000 route miles of fiber, we own and operate one of the largest and densest fiber networks in the country with a presence in 23 of the top 25 US markets.

Our proven track record
In our 30 years of experience owning and operating network assets we've seen it all and we're always ready to adapt to changing network trends.

Our deep expertise
We've worked with nearly every industry so we understand your unique opportunities and challenges and can tailor solutions to meet your goals.

Our solutions
We have your networking and security needs covered. Visit our infrastructure solutions page to learn more about our suite of solutions and how they can solve your toughest challenges.

CROWN CASTLE

Crown Castle owns, operates and leases more than 40,000 cell towers and approximately 90,000 route miles of fiber supporting small cells and fiber solutions across every major US market. This nationwide portfolio of communications infrastructure connects cities and communities to essential data, technology and wireless service—bringing information, ideas and innovations to the people and businesses that need them.

For more information, please contact 1-888-553-1781 or visit **CrownCastle.com**