REDES DEFINIDAS POR SOFTWARE

iQuila Ltd

Explicación del Protocolo iQuila VEN

IQ22100r1

Este documento hace referencia a:

iQuila Cloud
iQuila Enterprise

Protocolo iQuila VEN con IA Incorporada

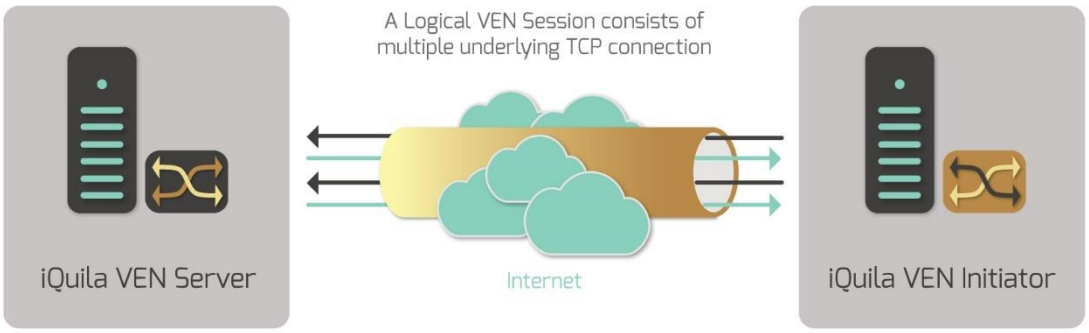
Protocolo iQuila VEN

iQuila VEN es una plataforma avanzada de comunicaciones de Capa 2 que intercambia tramas ethernet virtuales y se comunica utilizando el protocolo VEN. El protocolo iQuila VEN encapsula, encripta y transmite tramas ethernet virtuales en una red IP física, a través de Internet vía Capa 3, a otra red IP física, extendiendo el segmento completo de Capa 2 de una LAN a otra LAN.

El diseño único del Protocolo VEN utiliza múltiples conexiones TCP/IP paralelas para formar su conexión con el servidor iQuila. Debido a los múltiples flujos de conexiones TCP, cuando una o más conexiones TCP se pierden, las conexiones TCP restantes mantienen la conexión viva y activa mientras que las conexiones perdidas se reconstruyen utilizando su rápido sistema de reconexión automática. Esto permite una conexión segura, rápida y estable incluso cuando se despliega en entornos que implican un movimiento de alta velocidad (automóviles, aviones, trenes, etc.)

Inteligencia Artificial (IA) de iQuila

La IA integrada controla todas las comunicaciones en el Protocolo VEN, optimizando y haciendo más eficientes las comunicaciones. Esto permite mejorar el rendimiento y reducir la latencia, logrando así una mayor velocidad y una menor latencia. Un usuario nunca sabrá si una comunicación se realiza a través del Protocolo VEN o directamente en una red física.



Conmutadores Virtuales

El Protocolo VEN de iQuila se basa en la tecnología de virtualización. Al virtualizar la conmutación de Capa 2, el protocolo VEN puede unir estos conmutadores virtuales sin problemas con los conmutadores físicos de Capa 2 existentes. Dentro del software iQuila, se pueden crear múltiples conmutadores virtuales de Capa 2 sobre la marcha. Cada conmutador soporta IEEE 802.1Q VLANs.

Filtrado de Paquetes de Priorización de Datos

iQuila Enterprise Packet Filtering y Data Prioritisation le permite asegurar su red mientras prioriza sus datos importantes, Packet Filtering es una función que pasa o descarta los paquetes IP que pasan a través de los dispositivos de la red de acuerdo con las reglas designadas comúnmente conocidas como reglas de filtrado de paquetes, las reglas son procesadas en el número de prioridad asignado a cada regla, cuanto más bajo sea el número de prioridad establecido más importante es la regla y mayor prioridad tendrán los datos a través de la red. Se pueden crear múltiples reglas, lo que permite un control detallado de los datos que circulan por la red.

Encriptación y Seguridad

Las comunicaciones y los datos del protocolo VEN de Iquila están encriptados por medio de la encriptación Secure Socket Layer (SSL).

iQuila soporta, TLS 1.2. con SHAR2

La Autenticación de Certificados RSA soporta hasta 4096bits.

Algoritmos de encriptación actualmente soportados.Encryption algorithms currently supported.

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305

Verificación de Certificados de Servidor de iQuila

iQuila soporta la Verificación de Certificados de Servidor "man-in-the-middle" (MITM) Prevención de ataques.

Los certificados pueden ser generados y almacenados en el repositorio de certificados de seguridad para cada conmutador virtual, estos certificados pueden ser emitidos a los clientes para la verificación del servidor cuando el certificado no es auténtico, la conexión se interrumpe, y una advertencia será mostrada al usuario y la conexión al Servidor iQuila se detiene, esto protege contra ataques de enmascaramiento o MITM.

iQuila soporta la autenticación de usuarios de servidores externos

Autenticación por Contraseña

Cada conmutador virtual tiene una base de datos separada y segura para la autenticación de contraseñas. Las contraseñas se almacenan y se codifican con algoritmos SHA2 para mayor seguridad.

Autenticación con Radius y Active Directory

iQuila VEN soporta la integración de RADIUS y Active Directory para la autenticación de usuarios. Esto puede ser definido por cada Switch Virtual; también es posible tener una mezcla de diferentes tipos de autenticación en un Switch Virtual en operación al mismo tiempo.

Autenticación de Certificados RSA como PKI hasta 4096bits

iQuila VEN soporta la Autenticación de Certificados RSA, los usuarios pueden ser configurados con un certificado autofirmado o comprado, este certificado se utiliza en el cliente para la autenticación.

Otra solución alternativa es utilizar PKI (Infraestructuras de Clave Pública). Si se especifica que un usuario utilice PKI, no necesita introducir ninguna contraseña. El usuario pasa la clave privada para autenticarse. La clave privada puede mantenerse tanto en discos duros como en tokens de seguridad para mayor seguridad.

iQuila Enterprise también admite tanto la autenticación mediante contraseña como la basada en certificados PKI a través de tokens para la autenticación de dos factores.

Soporte de Tarjetas Inteligentes y Tokens USB para PKI

iQuila Enterprise soporta PKI con tarjetas inteligentes o tokens USB. Las tarjetas inteligentes y los tokens USB evitan la fuga de la clave privada de los usuarios, la clave privada se almacena en un token USB o tarjeta inteligente, estos dispositivos requieren un número PIN para acceder a la clave privada interna para mayor seguridad.

Aceleración UDP

iQuila VEN utiliza puertos UDP para la aceleración UDP. Si una conexión VEN formada por dos o más conexiones TCP/IP detecta que se pueden establecer canales UDP, el sistema utilizará automáticamente la aceleración UDP. Esto aumentará drásticamente el rendimiento y reducirá la latencia en la conexión VEN. La IA intentará establecer un canal UDP directo con los sistemas. Si se puede establecer un canal directo, la IA enviará y recibirá paquetes de datos UDP directamente con estos sistemas, evitando la necesidad de comunicarse con el conmutador VEN. Sin embargo, los paquetes TCP seguirán fluyendo a través del conmutador VEN para su autenticación. Dependiendo de la topología de la red, UDP puede estar restringido por cortafuegos o NATs, y la aceleración UDP puede no ser posible.

La aceleración UDP puede deshabilitarse en cualquier momento en los ajustes del lado del cliente VEN o en la configuración avanzada del servidor.

Comunicaciones VEN sobre DNS o ICMP

iQuila VEN admite una comunicación de reserva a través del puerto 53 UDP de DNS y del protocolo ICMP. Todos los paquetes VEN se encapsulan en paquetes DNS o ICMP y se transmiten a través del cortafuegos. El punto final del Servidor iQuila VEN del lado del receptor, extrae el paquete interno del paquete encapsulado y los entrega a la dirección de destino.

VEN sobre DNS e ICMP se ha implementado basándose en las especificaciones de los protocolos ICMP y DNS. Esta función puede activarse o desactivarse a través de la configuración del iQuila VEN Server.

Uso de la Compresión de Datos

El protocolo VEN de iQuila puede comprimir, enviar y recibir todas las tramas Ethernet internamente y transmitirlas. Se utiliza el algoritmo de iQuila como algoritmo de compresión de datos. El parámetro de compresión se ajusta para que el procesamiento se ejecute a la velocidad más rápida.

Al utilizar la compresión de datos para las comunicaciones VEN, se puede reducir un máximo del 80% del volumen de las comunicaciones (depende del protocol utilizado). Si se utiliza la compresión, la carga de la CPU tanto del cliente como del servidor es mayor y, en muchos casos, dependiendo de la velocidad de la línea (por ejemplo, si supera unos 10 Mbps), no comprimir los datos mejora la velocidad de comunicación.

Paquetes Multicast

iQuila VEN soporta las capacidades de conversión de tramas Ethernet de la misma forma que un switch físico de capa 2 y soporta paquetes IP Multicast sobre una conexión VEN.

VLANS

El protocolo iQuila VEN soporta IEEE 802.1Q. El estándar define un sistema de etiquetado VLAN para las tramas Ethernet y los procedimientos adjuntos que deben utilizar los Puentes de Red y los Conmutadores de Red para manejar dichas tramas.

Limitación de la VLAN

Según IEEE 802.1Q, el número máximo de VLANs en una red Ethernet determinada es de 4.094 (4.096 valores proporcionados por el campo VID de 12 bits menos los valores reservados en cada extremo del rango, 0 y 4.095). VEN puede superar esta limitación utilizando varios Switches Virtuales, cada uno de los cuales puede albergar un máximo de 4.095 VLANs.

Seguridad del Protocolo VEN

El protocolo VEN de iQuila lleva incorporado un sistema de Detección y Protección de Ataques DDoS (SYN Flood) que protege contra los ataques al sistema. Esta función puede desactivarse en la configuración del servidor.

MTU

Los ordenadores utilizan 1.514 bytes como MTU (Unidad de Transmisión Máxima) por defecto, este es un estándar de tamaño de paquete Ethernet sin FCS. No es posible determinar el tamaño optimizado de MTU incluso cuando un paquete se transmite a través de VPN.

El Protocolo VEN de iQuila utiliza un avanzado sistema de tunelización AI. El Protocolo iQuila VEN optimizará los paquetes de envío de ráfagas a 1.514 bytes y los transmitirá a través del túnel VEN. Los paquetes se unirán como una especie de cola de paquetes y se considerarán como un único bloque entero. El Protocolo VEN de iQuila encapsulará entonces el bloque entero por HTTPS y SSL, estos paquetes se pasarán a la red física. Esto genera un menor número de paquetes en general y resuelve cualquier problema de MTU dando un mejor rendimiento general y un mejor desempeño.